Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Cybercrime

Van herkenning tot aangifte

Cybercrime

Van herkenning tot aangifte

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Januari 2012

VOORWOORD

Geachte lezer,

ICT vervult een prominente rol in het dagelijks leven, voor het ondersteunen van bedrijfsprocessen en bij het bedienen van allerlei complexe processen in vitale infrastructuren. ICT is diep ingebed in de samenleving. Vandaag de dag bewaren we al onze gegevens en kennis ergens elektronisch en zijn we aangewezen op de beschikbaarheid en integriteit van computersystemen en telecommunicatienetwerken. Helaas kennen we ook een andere kant, waarbij ICT-middelen worden misbruikt of ingezet voor illegale activiteiten.

Ik ben verheugd om de voorliggende nieuwe versie van de handleiding over *Cybercrime, van herkenning tot aangifte* te mogen presenteren. Deze handleiding biedt ondersteuning aan bedrijven, overheidsinstanties, opsporingsambtenaren en burgers bij het herkennen en het doen van aangifte van criminele activiteiten in de digitale wereld.
Waar moet men op letten? Wat is eigenlijk strafbaar? Welke acties moet men ondernemen als een incident wordt gemeld? Dit zijn een paar vragen die opkomen bij vermoeden van misbruik of als er door cybercrime slachtoffers worden gemaakt. Deze handleiding geeft hiervoor de richtlijnen en uitleg.

Ik hoop dat deze handleiding uw vragen beantwoordt en daardoor een bijdrage levert aan de bestrijding van cybercrime en het beperken van de gevolgen ervan.

Elly van den Heuvel

Waarnemend Hoofd Nationaal Cyber Security Centrum

INHOUDSOPGAVE

TEN GELEIDE

De verwevenheid van ICT met bedrijfsprocessen en het maatschappelijk leven neemt toe. ICT-voorzieningen en telecommunicatiediensten zijn een vanzelfsprekendheid geworden. De elkaar steeds sneller opvolgende technologische trends en toenemende complexiteit en afhankelijkheid van ICT stellen ons voor extra uitdagingen. Ernstige verstoringen, schendingen van de persoonlijke levenssfeer en cybercriminaliteit maken daar deel van uit.

De vorige versie van de handleiding over Cybercrime (v2.0) dateert van augustus 2006. Vanwege alle technische en juridische ontwikkelingen is een herziene versie hard nodig. Gebruikers van de vorige versie zullen constateren dat grote delen van versie 2.0 nog steeds actueel zijn.

Deze nieuwe versie heeft ook betrekking op cybercrime in enge zin. Dit zijn handelingen gepleegd in de digitale wereld, waarvan het klassieke *hacken*, een vorm van computervredebreuk, het meest aansprekende voorbeeld is. Dergelijke vormen van cybercrime zijn anders dan de vormen van criminaliteit waarbij de digitale wereld slechts een nieuw middel vormt om een bestaande praktijk uit de fysieke wereld voort te zetten. Zo wordt kinderporno tegenwoordig vaak verspreid via het internet, maar daarmee is het nog geen cybercrime in enge zin.

Waarom deze handleiding?

De handleiding over *Cybercrime, van herkenning tot aangifte* is bedoeld om vormen van computermisbruik te leren herkennen en om daar in een juridische context mee om te gaan. Deze handleiding vormt hiermee een brug tussen de technische en juridische aspecten van cybercrime.

Om te voorkomen dat men slachtoffer wordt moeten de verschillende vormen van cybercrime inzichtelijk zijn. Het is daarom noodzaak dat organisaties cybercrime herkennen, zowel in relatie tot de wettelijk vastgestelde strafbare feiten als in technische zin. Of een bepaalde verschijningsvorm van ICT-misbruik strafbaar is moet via de beschreven strafrechtelijke criteria duidelijk worden.

Ook de technische aspecten van cybercrime moeten herkenbaar zijn, zodat met het oog op een eventuele aangifte de juiste gegevens vast worden gelegd. Als laatste moet voor het doen van aangifte bij de juiste instantie en het aanleveren van de daartoe benodigde informatie duidelijk zijn waarom het gaat.

Voor het Nationaal Cyber Security Centrum is deze handleiding over Cybercrime een belangrijke bijdrage aan het bewustzijn over en de preventie van cybercrime.

Doelgroep

De handleiding over *Cybercrime, van herkenning tot aangifte* is vooral bestemd voor personen bij Nederlandse organisaties en bedrijven, belast met het gebruik, beheer en de beveiliging van informatie en ICT-voorzieningen, die niet dagelijks cybercrimezaken behandelen.

De handleiding biedt praktische handvatten aan de Chief Information Officer (CIO), de ICT-manager, de Chief Information Security Officer (CISO) en de beveiligingsmanager. Daarnaast biedt de handleiding ook (juridische) achtergrondinformatie aan de technische expert en de systeembeheerder. Voor directieleden, personeelmanagers, juristen en functionarissen van de met opsporing en vervolging belaste instanties kan de handleiding gebruikt worden om incidenten te onderzoeken. Daarnaast is de handleiding zeker interessant en bruikbaar voor een breder publiek dat zoekt naar welke activiteiten op computersystemen nu eigenlijk strafbaar zijn.

Voor het lezen en gebruiken van de handleiding is geen bijzondere kennis vereist. De handleiding is geen lesboek over ICT-beveiliging of computernetwerktechniek noch een juridisch handboek. Enige basiskennis over computerbesturingssystemen, communicatieprotocollen zoals TCP/IP en HTTP, en beveiligingsmethodieken maken het begrijpen van de consequenties wel makkelijker.

Afbakening

Verstoringen van de ICT-voorzieningen, lekken van informatie en vernietigen van gegevens kan op vele manieren plaatsvinden. Deze handleiding zoomt in op de herkenning van moedwillig menselijk handelen door kwaadwillenden. Andere dreigingen en oorzaken, zoals technisch en menselijk falen (onbewust handelen), organisatorische kwetsbaarheden of externe omgevingsfactoren (zoals weer, overstromingen, ongevallen), zijn niet meegenomen.

Moedwillig menselijk handelen omvat onder meer diefstal van gegevens, identiteitsdiefstal, onbevoegde beïnvloeding, verstoringen veroorzaakt door kwaadwillenden en manipulatie gericht op het belemmeren, aanpassen of verstoren van een (bedrijfs-)proces. Drijfveren zijn bijvoorbeeld financieel gewin, wrok, activisme, (bedrijfs-)spionage of misbruik met een terroristisch oogmerk.

De handleiding beperkt zich tot cybercrime in enge zin. Dat wil zeggen tot criminaliteit waarbij ICT-middelen (hard- en software) het voornaamste doelwit zijn of waarbij de daad niet zonder het misbruik van ICT-voorzieningen kan worden uitgevoerd. Deze handleiding gaat dus niet over criminaliteit waarbij ICT-middelen op normale wijze (legitiem) worden gebruikt voor anderszins 'normale' vormen van criminaliteit.

Vaak worden het verlies van (persoons)gegevens of andere incidenten ten aanzien van gevoelige informatie beschouwd als cyber-security-incidenten. In de definitie van deze handleiding vormen informatiebeveiligingsincidenten in algemene zin echter geen onderdeel van cybercrime, in enge noch in ruime zin.

De handleiding beschrijft technische aspecten van de verschillende verschijningsvormen van cybercrime en geeft hierbij de toepasselijke juridische bepalingen. De nadruk wordt gelegd op incidenten die kunnen worden gepleegd via een openbaar elektronisch communicatienetwerk zoals het internet, of die zich voordoen bij bedrijfsnetwerken. De handleiding is geen handboek over informatiebeveiliging of een receptenboek om maatregelen te treffen.

Het is van belang te realiseren dat het hier een handleiding betreft die achtergrondinformatie en aanwijzingen geeft voor de herkenbaarheid, de gegevensverwerking, de juridische aspecten en het doen van aangifte van cybercrime in enge zin. Gezien de ontwikkelingen omtrent cybercrime - op zowel het technische als het juridische vlak - is deze handleiding een levend document en niet uitputtend.

Wat is nieuw?

Het belangrijkste doel van deze handleiding blijft het herkennen van computercriminaliteit in enge zin. Deze gereviseerde versie legt dan ook de focus op het beschrijven van de vormen van cybercrime en de daaraan verbonden strafbare gedragingen.

Een groot verschil met de situatie in 2005 is dat de Wet computercriminaliteit II inmiddels van kracht is. Ook dienen nieuwe uitbreidingen zich aan. Ontwikkelingen op technologisch gebied, bijvoorbeeld op het terrein van het gebruik (en misbruik) van draadloze communicatiemiddelen, spelen nu een belangrijke rol en de internationale dimensie wordt steeds belangrijker.

In het proces van herkenning tot aangifte ontbraken nog handvatten voor het opvolgen en afhandelen van incidenten, de (on)mogelijkheden bij het doorzoeken van computersystemen en inzetten van elektronische bewijsmiddelen. Deze richtlijnen zijn aan deze nieuwe handleiding toegevoegd.

Tips voor maatregelen ter voorkoming van misbruik en bescherming tegen cybercrime zijn komen te vervallen. Zulke informatie is uitvoerig beschreven in de documentatie over informatiebeveiliging en cyber-security, bijvoorbeeld in andere publicaties van GOVCERT.NL.
De handleiding is wél uitgebreid met praktische informatie die van toepassing kan zijn bij het aangifteproces.

Totstandkoming van de handleiding

Deze handleiding is tot stand gekomen door bundeling van technische en juridische kennis op het gebied van ICT-gerelateerde veiligheidsincidenten, cybercrime en de opsporing hiervan. Om er voor te zorgen dat de handleiding enerzijds aansluit bij de praktijk en anderzijds wetenschappelijk wordt gedragen, zijn sinds het uitkomen van de eerste versie deskundigen vanuit diverse organisaties en disciplines geconsulteerd. Daarnaast heeft GOVCERT.NL samengewerkt met het National High Tech Crime Unit (NHTCU) van het Korps Landelijke Politie Diensten (KLPD) en het Openbaar Ministerie. Met ingang van 1 januari is GOVCERT.NL opgegaan in het Nationaal Cyber Security Centrum.

Over het Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) is opgericht in januari 2012, met GOVCERT.NL aan de basis. Het NCSC is een onderdeel van het ministerie van Veiligheid en Justitie. Tot december 2011 was GOVCERT.NL het Computer Emergency Response Team (CERT) van de Nederlandse overheid. Die taak is overgenomen door het NCSC. Het centrum biedt ondersteuning aan overheidsorganisaties en bedrijven in vitale sectoren bij het voorkomen en afhandelen van ICT-gerelateerde veiligheidsincidenten, zoals computervirussen, hackingactiviteiten en fouten in applicaties en hardware. Het NCSC is voor de overheid hét centrale meld- en coördinatiepunt voor ICT-gerelateerde veiligheidsincidenten, 24 uur per dag, zeven dagen per week. Advies en preventie, waarschuwing, incident response en kennisdeling zijn hierbij sleutelwoorden.

Het NCSC beschikt over specifieke kennis en ervaring aangaande herkenning van verschillende vormen van cybercrime maar heeft géén opsporingsbevoegdheden. Het NCSC streeft naar goede advisering over de afhandeling en eventuele aangifte van ICT-gerelateerde veiligheidsincidenten en/of cybercrime. De focus van het NCSC ligt bij cybercrime in enge zin.

Essentieel voor de dienstverlening is de samenwerking en informatie-uitwisseling met andere CERTs, zowel in nationaal als internationaal verband, en met rijksdiensten die een relatie hebben met ICT-beveiliging, zoals het KLPD, de AIVD, de NCTb en het Nationaal Coördinatie Centrum. Het NCSC speelt een belangrijke rol in de informatievoorziening aan deelnemende en buitenlandse organisaties en in de opsporing van ICT-gerelateerde veiligheidsincidenten of vormen van cybercrime.

LEESWIJZER

Er is voor deze handleiding over *Cybercrime, van herkenning tot aangifte* gekozen om te beginnen met het duiden van cybercrime. Daarna doorloopt het semi-chronologisch het proces van juridisch en technisch herkennen van cybercrime, het omgaan met een incident en het doen van aangifte.

Deze aanpak is als volgt opgebouwd:

1. Introductie en duiden van cybercrime
2. Juridische en strafrechtelijke context
3. Vormen van cybercrime
4. Incidentopvolging en -afhandeling
5. Onderzoeken van incidenten
6. Het doen van melding of aangifte

Hoofdstukindeling

In Hoofdstuk 1 wordt de definitie van cybercrime in enge zin gegeven. Daarna wordt achtergrondinformatie gegeven over informatiebeveiliging en een overzicht van de meest relevante wet- en regelgeving.

Hoofdstuk 2 gaat uitgebreid in op de juridische context, achtergronden en strafrechtelijke bepalingen die van toepassingen zijn op cybercrime in enge zin, eigenlijk de maatschappelijke spelregels. Ook worden enkele strafbare gedragingen beschreven die niet tot cybercrime in enge zin worden gerekend, maar wél als computercriminaliteit worden gezien.

Hoofdstuk 3 beschrijft verschijningsvormen van cybercrime in enge zin en de technische aspecten. De strafbare gedragingen volgens de juridische implicaties worden daarbij toegelicht. Bij iedere verschijningsvorm wordt aandacht besteed aan de volgende onderwerpen:

- wat wordt er onder de verschijningsvorm verstaan;
- wat is de technische verschijningsvorm en hoe herken je deze;
- welke gegevens voor vaststelling heb je nodig;
- wanneer is de verschijningsvorm strafbaar.

Hoofdstuk 4 besteedt aandacht aan het afhandelen van cyberincidenten. Het hoofdstuk gaat in op de organisatie van incidentopvolging en afhandeling en geeft aanwijzingen voor het omgaan met en reageren op beveiligingsincidenten.

Hoofdstuk 5 beschrijft verschillende juridische en forensische aspecten bij het onderzoeken van incidenten. Er wordt ingegaan op de bevoegdheid van de rechtsmacht, het gebruik van elektronisch materiaal als bewijsmiddel en aandachtspunten bij het (forensisch) rechercheonderzoek.

Hoofdstuk 6 besteedt aandacht aan de verschillende stappen die een organisatie kan ondernemen als zij vermoedt of constateert dat een bepaalde vorm van cybercrime is voorgevallen waarvan men aangifte wil doen.

Gebruik jargon

Veel woorden in de ICT-sector zijn oorspronkelijk Engelstalig en worden als zodanig gebruikt. De eerste vermelding van het woord is *schuingedrukt*.
Bijlage D bevat een begrippenlijst van de gebruikte terminologie.

HOOFDSTUK 1

Introductie cybercrime

De focus van deze handleiding ligt op *cybercrime in enge zin*, waarvan in dit hoofdstuk een definitie wordt gegeven. Het verband met *cyber security* en informatiebeveiliging wordt uitgelegd. Ook is een overzicht opgenomen van relevante wetgeving, achtergronden en verschillende organisaties betrokken bij de aanpak van cybercrime. Uitgebreide lijsten van veel gebruikte afkortingen en begrippen staan in bijlagen D en E.

1.1 Wat is cybercrime?

Cybercrime is een containerbegrip, voor veel mensen is het een onduidelijk fenomeen. Cybercrime wordt wel omschreven als "criminaliteit op of via het internet". In deze beperkte omschrijving wordt geen rekening gehouden met misbruik dat ook van binnenuit plaatsvindt of betrekking kan hebben op ICT-voorzieningen die *niet* op het internet zijn aangesloten.
Daarnaast zijn er ook vormen van misbruik waarbij nadrukkelijk op bepaalde (psychologische) zwakheid van mensen wordt ingespeeld; dit noemt men *social engineering*. Bovendien krijgen vormen van criminaliteit in de fysieke wereld dankzij de digitalisering nieuwe verschijningsvormen.

Een bredere definitie omvat vormen van criminaliteit die betrekking hebben op, of gepleegd zijn met, computersystemen, inclusief telecommunicatienetwerken. De criminele activiteiten kunnen zijn gericht tegen personen, eigendommen en/of organisaties of elektronische telecommunicatienetwerken en computersystemen.
Een eensluidende (internationale) definitie van cybercrime ontbreekt.

In deze handleiding wordt een definitie gehanteerd in overeenstemming met die van het KLPD (KLPD Dienst Nationale Recherche, 2009):

Cybercrime omvat elke strafbare gedraging waarbij voor de uitvoering het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.

De Nederlandse wetgever gebruikt overigens niet de term cybercrime maar *computercriminaliteit*. Elke vorm van criminaliteit met betrekking tot computers valt hieronder. Daarnaast wordt als containerbegrip voor alle vormen het moedwillig misbruiken van ICT of technisch geavanceerde middelen ook de term *hightech crime* gebruikt.[1]
Deze handleiding gaat uit van het bredere begrip computercriminaliteit, maar omdat cybercrime in literatuur en spraakgebruik inmiddels vaker wordt gebruikt dan de term computercriminaliteit, hanteren we de term cybercrime.

Hierin onderscheiden we twee categorieën:
- cybercrime in enge zin;
- cybercrime in ruime zin.

Cybercrime in enge zin

Onder cybercrime in enge zin verstaan we strafbare gedragingen die niet zonder tussenkomst of gebruik van ICT gepleegd hadden kunnen worden. Kenmerkend is dat de hardware, software of apparatuur en de daarin of daarmee opgeslagen gegevens het doel van de actie zijn. Daarnaast kan het gaan om acties gepleegd via een (openbaar) telecommunicatienetwerk.
Om te spreken over cybercrime in enge zin moeten ICT-middelen dus het voornaamste doelwit zijn of moet de daad niet zonder het misbruiken van ICT-voorzieningen kunnen worden uitgevoerd.

Voorbeelden van cybercrime in enge zin zijn:
- het ongeoorloofd toegang verschaffen tot een geautomatiseerd systeem;[2]
- het ongeoorloofd verwijderen of aanpassen van computergegevens;[3]
- het ongeoorloofd uitschakelen of onbruikbaar maken van systemen;
- het versturen van computervirussen;
- het onderscheppen en/of veranderen van computerberichten.[4]

Overigens komt cybercrime in enge zin vaak voor in combinatie met andere vormen van (computer)criminaliteit.
Zo is bijvoorbeeld het verspreiden van *malware* bedoeld om een *botnet* op te bouwen of om gegevens te verzamelen *(phishing)*, met als uiteindelijk doel geld te verdienen door te stelen van bankrekeningen van slachtoffers.

Cybercrime in ruime zin

Onder *cybercrime in ruime zin* worden strafbare gedragingen verstaan die met behulp van of via ICT worden uitgevoerd. ICT-middelen of digitale technieken worden dus op normale (legitieme) wijze of als ondersteuning gebruikt bij het plegen van anderszins traditionele criminaliteit. ICT speelt een belangrijke rol als hulpmiddel of als onderdeel van de plaats delict.

Voorbeelden van cybercrime in ruime zin zijn het valselijk beschuldigen of bedreigen via een sociaal netwerk of per e-mail, fraude, oplichting, heling via verkoopsites, witwassen, (bedrijfs)spionage, relschoppen, verspreiding van kinderporno of publiceren van discriminerende leuzen.
Vaak hebben deze vormen van criminaliteit hun eigen benaming zoals *cyberstalking*, *cyberfraude*, *cyberhate* of *cyber espionage* (Engelfriet, De Wet Computercriminaliteit, 2007).

1. Het KLPD hanteert aanvullend het criterium dat voor hightech-crime sprake moet zijn van vormen van zware en georganiseerde misdaad (KLPD Dienst Nationale Recherche, 2009).
2. De Nederlandse wet gebruikt de term geautomatiseerd werk voor een computer. Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen (art. 80sexies, Sr.). Hieronder vallen dus computer- en netwerkapparatuur of systemen, elektronische gegevensdragers of telecommunicatienetwerken.
3. Onder gegevens wordt verstaan iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken (art. 80quinquies, Sr.). Hieronder vallen dus alle op een elektronische gegevensdrager, computer of ander geautomatiseerd werk verwerkte of opgeslagen informatie.
4. Onder elektronisch bericht wordt verstaan een tekst-, spraak-, geluids- of beeldbericht dat over een elektronisch communicatienetwerk wordt verzonden en in het netwerk of in de randapparatuur van de ontvanger kan worden opgeslagen tot het door de ontvanger wordt opgehaald (vgl. art. 11.1i, Tw). Hieronder vallen dus alle gegevens die tussen computersystemen op elektronische wijze worden uitgewisseld.

1.2 Wet- en regelgeving

Deze paragraaf geeft een beknopt overzicht van de meest relevante wet- en regelgeving op basis waarvan activiteiten als strafbare gedragingen onder de vlag van cybercrime in enge zin worden gerekend. Daarnaast zijn enkele bepalingen uit het bestuursrecht opgenomen, omdat deze veelal worden geassocieerd met misbruik van ICT-voorzieningen.

Dit overzicht haalt voor de volledigheid ook enkele wetten aan waarmee rekening moet worden gehouden bij het herkennen en opsporen van cybercrime. Deze handleiding gaat niet uitgebreid in op bevoegdheden van opsporingsinstanties of de wijze van strafvervolging.

1.2.1 Cybercrime-verdrag (CCV)

Omdat cybercrime zich niet tot landsgrenzen beperkt, doen zich vaak vragen voor over de toepasselijkheid van nationale wetgeving en de omvang van de bevoegdheden van nationale opsporingsinstanties[5]. De landen aangesloten bij de Raad van Europa hebben in een Cybercrime-verdrag afgesproken tot een gemeenschappelijk strafrechtelijk beleid te komen, gericht op de bescherming van de samenleving tegen strafbare feiten verbonden met elektronische netwerken. Vooral het tot stand brengen van passende geharmoniseerde wetgeving en het versterken van de internationale samenwerking zijn speerpunten (Council of Europe, 2001).

Het verdrag geeft aan welke gedragingen van cybercrime in enge zin ten minste strafbaar moeten worden gesteld (art. 1 t/m 6 CCV). De meeste van deze gedragingen waren al strafbaar in Nederland onder de Wet computercriminaliteit uit 1993. Deze Wet computercriminaliteit had tot gevolg dat in het Wetboek van Strafrecht en het Wetboek van Strafvordering wijzigingen werden doorgevoerd om de nodige strafbepalingen omtrent en bevoegdheden voor computercriminaliteit te regelen. Naar aanleiding van het verdrag is deze wetgeving in 2006 verder geactualiseerd.

Het verdrag beperkt zich niet alleen tot cybercrime in enge zin, maar stelt ook dat het invoeren, aanpassen, verwijderen of andere vormen van interfereren met een computersysteem met als doel valsheid in geschrifte (art. 7 CCV) of fraude (art. 8 CCV) met nadelige gevolgen voor anderen, strafbaar is.

Het verdrag stelt ook dat alle vormen van produceren, bezitten of verspreiden van kinderporno strafbaar moet zijn (art. 9 CCV). In een additioneel protocol bij het Cybercrime-verdrag van 1 maart 2006 is ook het doen van racistische en xenofobe uitingen via computersystemen strafbaar gesteld.[6]

Het verdrag strekt zich ook uit naar de bescherming van het auteursrecht en de naburige rechten voor zover de inbreuken moedwillig, op commerciële schaal en met behulp van een computer(systeem) plaatsvinden (art. 10 CCV). Nederland heeft dit vastgelegd in de Auteurswet 1912 en in de Wet op de naburige rechten.

Het tweede gedeelte van het verdrag bevat bepalingen over formeel strafrecht, die toezien op het onderzoek van computers en computergegevens, en het onderzoek van telecommunicatie. De bepalingen zijn relevant voor alle vormen van criminaliteit (Koops, 2003).

Door de Nederlandse implementatie van het Cybercrime-verdrag vallen de meeste vormen van computercriminaliteit ook onder de Nederlandse strafwet wanneer een Nederlander ze in het buitenland begaat.

1.2.2 Grondwet

De belangrijkste borging van de rechten van personen is uiteraard de Grondwet (Grondwet, 1815). Deze legt onder meer in artikel 10 het klassieke grondrecht vast op privacy en eerbiediging van de persoonlijke levenssfeer. Artikel 13 legt de onschendbaarheid van brief-, telefoon en telegraafgeheim vast en, op basis van later jurisprudentie, tot op zekere hoogte ook de onschendbaarheid van de vertrouwelijkheid van e-mail (Kamerstukken 2004/05, 26671, 2005). De onschendbaarheid van e-mail als zodanig is echter nog niet expliciet vastgelegd in wetgeving.

1.2.3 Wetboek van Strafrecht (Sr)

Sinds 1 september 2006 is de Wet computercriminaliteit II van kracht. Hiermee zijn strafbare gedragingen verankerd in het Nederlandse Wetboek van Strafrecht (Sr) en de opsporingsbevoegdheden in het Wetboek van Strafvordering (Sv). Het Wetboek van Strafrecht bepaalt in welke gevallen er aan mensen of rechtspersonen een straf kan worden opgelegd.

Het Wetboek van Strafrecht stelt onder andere de volgende gedragingen strafbaar die tot cybercrime in enge zin worden gerekend:

- het binnendringen in een geautomatiseerd werk *(computervredebreuk)* (art. 138ab, lid 1);
- het binnendringen in een geautomatiseerd werk en vervolgens kopiëren van gegevens (art. 138ab, lid 2);
- het binnendringen in een geautomatiseerd werk via een openbaar telecommunicatienetwerk en vervolgens verder *hacken* (art. 138ab, lid 3);
- het belemmeren van toegang tot een geautomatiseerd werk (art. 138b);
- het aftappen of opnemen van gegevens *(afluisteren)* (art. 139c);

5. Zie ook 'Internationale bestrijding cybercrime brengt wetswijzigingen met zich mee' persbericht ministerie van Justitie 28.11.2000.
6. http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CL=ENG

- het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen bedoeld om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen (art. 139d, lid 2a);
- het ter beschikking stellen of voorhanden hebben van toegangscodes of middelen met als doel om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen (art. 139d, lid 2b);
- het vernielen of een stoornis teweeg brengen in de gang van enig geautomatiseerd werk of enig werk voor telecommunicatie (art. 161sexies en 161septies);
- het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen (art. 326c);
- het wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens (art. 350a, lid1);
- het ter beschikking stellen of verspreiden van gegevens die schade aanrichten door zichzelf te vermenigvuldigen *(computervirussen)* (art. 350a, lid 3).

Daarnaast stelt het Wetboek van Strafrecht de volgende gedragingen strafbaar die tot cybercrime in ruime zin worden gerekend:
- het bezit van gegevens of een voorwerp waarop gegevens staan die door wederrechtelijk aftappen zijn verkregen (art. 139e);
- het plaatsen van afluistermiddelen (art. 139d, lid 1).

Elke vorm van opzettelijk en wederrechtelijk binnendringen is strafbaar gesteld, ook als daarbij geen beveiliging wordt doorbroken. Bovendien is het ter beschikking stellen of anderszins voorhanden hebben van de technische hulpmiddelen of de wederrechtelijke verkregen gegevens mogelijk strafbaar.

Naast de Wet computercriminaliteit en Wet computercriminaliteit II kunnen misdrijven ook op basis van overige wetgeving worden aangepakt, zoals de strafbaarstelling van vernieling, beschadiging of onbruikbaar maken van de waterhuishouding (art. 161), elektriciteit (art. 161bis/ter), luchtvaart (art. 162-163/168-169), spoorwegen (art. 164-165), scheepsvaart (art. 166-167) en drinkwater (art. 172-173).

Cybercrime in ruime zin, zoals valsheid in geschrifte of fraude, is op verschillende plaatsen in de wet vastgelegd onder de traditionele wetsartikelen. Artikel 232 Sr stelt bijvoorbeeld het valselijk opmaken of vervalsen van een betaalpas, waardekaart of een drager van identiteitsgegevens, bestemd voor het verrichten of verkrijgen van betalingen langs geautomatiseerde weg, strafbaar.

1.2.4 Wetboek van Strafvordering (Sv)

Het Wetboek van Strafvordering bepaalt hoe strafbare feiten opgespoord en vervolgd kunnen worden (formeel strafrecht). Wat de strafbare feiten zijn en welke straffen ervoor uitgesproken kunnen worden, is te vinden in het Wetboek van Strafrecht (materieel strafrecht).

Het Wetboek van Strafvordering stelt o.a. de volgende regels vast voor het doorzoeken om gegevens vast te kunnen leggen:
- de rechter-commissaris, officier van justitie, hulpofficier van justitie en opsporingsambtenaar komt de bevoegdheid toe tot het doorzoeken van plaatsen om gegevens vast te leggen (te kopiëren) die op een gegevensdrager zijn opgeslagen (art. 125i);
- het doorzoeken van een geautomatiseerd werk dat met een netwerk verbonden is, mag op afstand plaatsvinden als dit redelijkerwijs nodig is om de waarheid aan de dag te brengen (art. 125j, lid 1);
- het onderzoek moet zich beperken tot geautomatiseerde werken (netwerklocaties) waar de normale gebruikers van de doorzochte computer rechtmatig toegang toe hebben, vanaf de plaats (computer) waar de doorzoeking plaatsvindt (art. 125j, lid 2);
- een persoon (maar niet de verdachte) die kennis draagt van de wijze van beveiliging van een geautomatiseerd werk of (versleutelde) gegevens, kan het bevel krijgen toegang te verschaffen tot de geautomatiseerde werken of (versleutelde) gegevens (art. 125k).

Belangrijk is dat ook bij de normale doorzoekingbevoegdheden computers kunnen worden onderzocht en gegevens kunnen worden gekopieerd, zoals is vastgelegd in de Wet computercriminaliteit van 1993.

Door de vermelding van bijna alle computerdelicten in het Wetboek van strafvordering kunnen verdachten in voorlopige hechtenis worden genomen, ook als er minder dan vier jaar gevangenisstraf als maximum voor het feit geldt (art. 67 lid 1 Sv). Hierdoor zijn ook de meeste opsporingsbevoegdheden van toepassing.

1.2.5 Telecommunicatiewet (Tw)

Op basis van de Europese Richtlijn privacy en elektronische communicatie dienen aanbieders van elektronische communicatienetwerken en -diensten waarborgen te bieden tegen inbreuken op de persoonlijke levenssfeer van abonnees of gebruikers van hun netwerken of diensten (Europese Commissie, 31 juli 2002). In de Europese Richtlijn wordt onder meer aandacht besteed aan de schending van de persoonlijke levenssfeer als gevolg van de ontvangst van ongevraagde commerciële communicatie (spam), cookies en spyware. Deze bepalingen zijn geborgd in de Nederlandse Telecommunicatiewet (Tw, 19 oktober 1998) en het Besluit universele dienstverlening en eindgebruikersbelangen 2004.

Spam is niet strafbaar volgens de strafwet in Nederland, het valt onder het bestuursrecht. Er zijn alleen bestuurlijke boetes mogelijk. Overtredingen van het spamverbod vallen strikt genomen dan ook niet onder de noemer cybercrime. Toch wordt het gebruiken van e-mail en *cookies* in deze handleiding aangehaald om een volledig beeld van het misbruik van ICT-systemen te geven.

De Telecommunicatiewet en het Besluit universele dienstverlening en eindgebruikersbelangen stelt onder andere de volgende regels vast voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer:

- de aanbieder van een openbaar elektronisch communicatienetwerk of -dienst zorgt voor de bescherming van persoonsgegevens en de persoonlijke levenssfeer van abonnees en gebruikers van zijn netwerk of dienst (zorgplicht en goed huisvaderschap) (art. 11.2);
- het gebruik van automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is uitsluitend toegestaan met daarvoor voorafgaand toestemming (spam) (art. 11.7);
- voor het toegang verkrijgen tot, of opslaan van gegevens, in de randapparatuur van een abonnee of gebruiker, dient voorafgaand de abonnee of gebruiker te worden geïnformeerd en de gelegenheid te worden geboden de handeling te weigeren (cookies) (art. 4.1, Besluit universele dienstverlening en eindgebruikersbelangen).

1.2.6 Auteursrecht

Auteursrecht (of *copyright*) is het recht van de maker of een eventuele rechtverkrijgende van een werk van literatuur, wetenschap of kunst om te bepalen hoe, waar en wanneer zijn werk wordt openbaar gemaakt of verveelvoudigd (Auteurswet, 23-09-1912). Het auteursrecht ontstaat van rechtswege. Men hoeft niets te deponeren of te registreren. Aanvankelijk was het auteursrecht bedoeld voor de tekst van geschriften van literaire of wetenschappelijke aard, maar door een geleidelijke uitbreiding van het werkingsgebied is het tegenwoordig ook op veel andere zaken van toepassing, zoals toespraken, software, foto's, films, opgenomen muziek, beeldende kunstwerken, bouwwerken en journalistiek werk. Ook de schrijver van een e-mail kan soms via zijn auteursrecht optreden tegen ongewenste publicatie (Engelfriet, Elektronisch briefgeheim: de stand van zaken, 2008).

Opzettelijke schending van het auteursrecht, waaronder wordt verstaan een verveelvoudiging en verspreiding zonder de vereiste voorafgaande toestemming van de rechthebbende, geldt in Nederland als een misdrijf en kan met gevangenisstraf worden bestraft.

De Auteurswet stelt in artikelen 31 t/m 36b onder andere de volgende gedragingen strafbaar die tot cybercrime in ruime zin kunnen worden gerekend:

- inbreuk op auteursrechten (art. 31 Auteurswet);
- verspreiden van auteursrechtelijk beschermde werken;
- verspreiden of commercieel voorhanden hebben van middelen om technische beveiligingen van computerprogrammatuur te omzeilen (art. 32a Auteurswet).

1.2.7 Wet bescherming persoonsgegevens (Wbp)

De rechten en verplichtingen voor de omgang met persoonlijke gegevens zijn vastgelegd in de Wet bescherming persoonsgegevens (Wbp, 06-07-2000). De Wbp verplicht organisaties die persoonsgegevens verwerken - dit betekent elke activiteit rondom persoonsgegevens - bepaalde voorzorgsmaatregelen te nemen, zodat de opgeslagen gegevens niet ten nadele van de desbetreffende personen gebruikt kunnen worden. De Wbp en aanvullende besluiten zijn uitgewerkt in drie risicoklassen met bijbehorende te nemen maatregelen in de adviezen van het College Bescherming Persoonsgegevens (CBP).

Als een organisatie vermoedt of constateert dat zich een bepaalde verschijningsvorm van cybercrime heeft voorgedaan, verzamelt zijn gegevens voor (eventueel) aangifte wordt gedaan. Bij het verzamelen en verwerken van gegevens die kunnen worden herleid tot een bepaald persoon moet rekening worden gehouden met de Wbp. De wet staat dit in het algemeen toe, mits het zorgvuldig gebeurt Dat betekent onder andere dat alleen de gegevens die nodig zijn om aangifte te doen, mogen worden verzameld en doorgegeven. Deze gegevens moeten goed worden beveiligd. Het belang van de aangifte dient zwaarder te wegen dan het privacybelang van degene over wie de gegevens gaan.

1.2.8 Wet particuliere beveiligingsorganisaties en recherchebureaus

Soms kan het noodzakelijk zijn om onderzoek te verrichten naar (vermoeden van) cybercrime. Er gelden echter strikte regels voor het bewaken of monitoren van computersystemen en telecommunicatienetwerken, het opsporen van cybercrime en het verzamelen van mogelijk bewijsmateriaal. Zo mag een medewerker, een systeembeheerder of de directeur van een bedrijf niet zonder meer in (zakelijke of privé-) computerbestanden of e-mail kijken.
Het Wetboek van Strafrecht verbiedt beheerders van een (openbaar of bedrijfs)communicatienetwerk om opzettelijk en wederrechtelijk kennis te nemen van vertrouwelijke communicatie van hun gebruikers (art. 273d Sr).
Werkgevers mogen communicatie of internetgebruik van werknemers monitoren, maar moeten dat volgens het goed werkgeverschap wel volgens zorgvuldige procedures doen (art. 7:611 Burgerlijk Wetboek). Een organisatie kan daarom een onafhankelijk particulier onderzoeksbureau inschakelen om objectief aan waarheidsvinding te doen.

Particuliere onderzoeksbureaus houden zich op commerciële basis bezig met het verrichten van feitenonderzoek in zaken met een privaatrechtelijke, bestuursrechtelijke of strafrechtelijke achtergrond. Het verrichten of aanbieden van recherchewerkzaamheden zonder vergunning van de minister van Veiligheid en Justitie is verboden. Zowel het betreffende beveiligingsbedrijf als de ingezette particuliere onderzoekers moeten beschikken over een vergunning. Zij vallen onder de Wet particuliere beveiligingsorganisaties en recherchebureaus (Wpbr, 24-10-1997) en de aanvullende Regeling particuliere beveiligingsorganisaties en recherchebureaus (Regeling pbr, 03-03-1999). Een particulier onderzoeker of rechercheur heeft echter geen extra bevoegdheden, wel verplichtingen.

1.3 Wat is informatiebeveiliging?

Informatiebeveiliging (IB) wordt gezien als het overkoepelende vakgebied dat zich bezighoudt met de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Omdat vrijwel alle informatie digitaal wordt opgeslagen en verwerkt, is het IB-werkveld nauw verbonden met cyber security en cybercrime. Deze handleiding over cybercrime gaat niet uitgebreid in op informatiebeveiliging of cyber security. Daarvoor kan men terecht bij diverse handboeken en de Code voor Informatiebeveiliging (NEN-ISO/IEC 17799 and NEN 7799-2). Een juridische aanvulling op deze Code is te vinden in Koops, 2003/5. Vanwege de context van deze handleiding en de beveiligingsaspecten van informatie- en communicatietechnologie worden deze twee begrippen kort toegelicht.

Informatiebeveiliging

Informatiebeveiliging is het geheel van maatregelen, richtlijnen en procedures voor informatie- en computersystemen, gericht op het waarborgen van het in bedrijf zijn van de computersystemen en het minimaliseren van schade. Het begrip informatie heeft betrekking op alle verschijningsvormen zoals fysieke documenten, digitale computerbestanden of mondelinge overdracht. Informatiebeveiliging spitst zich toe op drie kernbegrippen:

- *beschikbaarheid*: de mate waarin informatie en systemen op het gewenste moment toegankelijk zijn voor gebruikers;
- *vertrouwelijkheid*: de mate waarin de toegang tot informatie en systemen beperkt is tot een vastgestelde groep van gebruikers;
- *integriteit*: de mate waarin informatie en systemen geen fouten bevatten.

Informatiebeveiliging is een continu, complex proces en een vast onderdeel van de dagelijkse bedrijfsvoering. Informatiebeveiliging beweegt zich in een cyclus van risicoafweging, nemen van maatregelen en eventuele aanpassingen aan beleid en uitvoering. Belangrijke vragen zijn: wat moet er precies worden beveiligd en tegen wie of wat? Wat is het mogelijk doel voor de kwaadwillende, hoe gaan ze te werk?

Cyber security

Cyber security is het geheel aan (technische) ICT-maatregelen met als doel om vrij te zijn van gevaar of schade veroorzaakt door misbruik, verstoring of uitval van ICT. Het gevaar of de schade kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT-voorzieningen opgeslagen informatie of schade aan de integriteit van die informatie. Hiertoe worden beschermende, detecterende en herstellende maatregelen gerekend. Cyber security kan als zodanig als uitwerking van de technische aspecten van informatiebeveiliging worden gezien.

1.4 Kwetsbaarheden

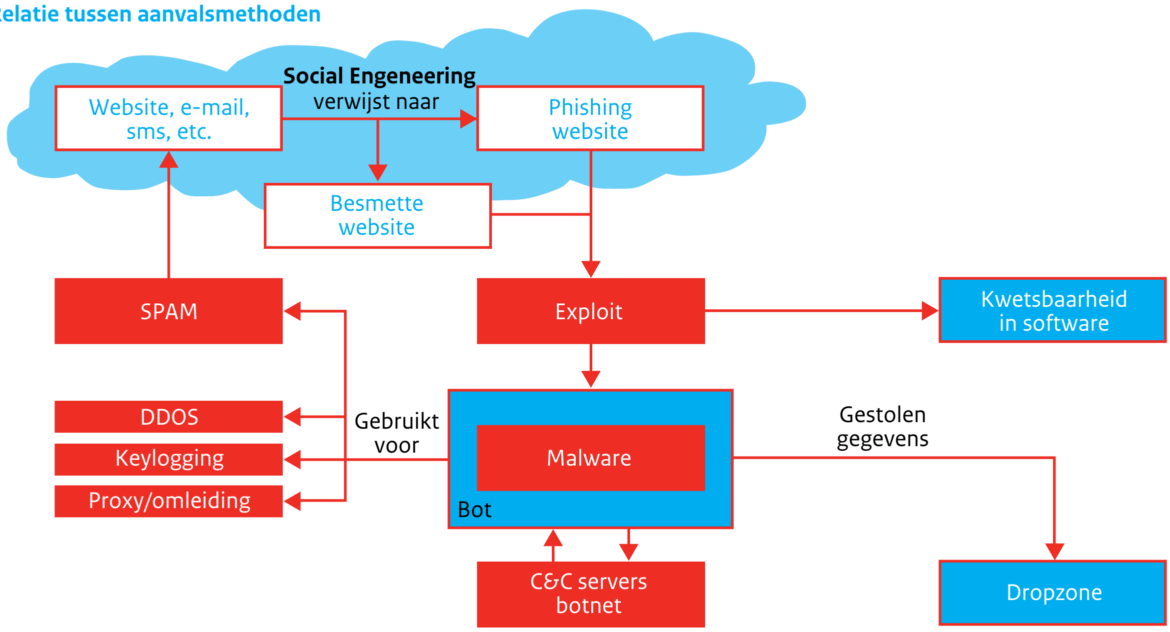
Misbruik van ICT-systemen kan alleen plaatsvinden als er kwetsbaarheden zijn die kunnen worden uitgebuit. Kwetsbaarheden zijn de zwakke plekken in bijvoorbeeld de organisatie, installaties of ICT-voorzieningen waardoor misbruik een kans heeft om ook daadwerkelijk op te treden. Misbruik van ICT-voorzieningen wordt mede mogelijk gemaakt doordat er zwakke plekken bestaan in de computersystemen, netwerkcomponenten of software. Andere oorzaken zijn gelegen in bijvoorbeeld kwetsbaarheden in de procedures of menselijke gedragingen.

Bij veel verschijningsvormen van cybercrime vindt besmetting met malware plaats, worden kwetsbaarheden misbruikt om binnen te dringen of om ongeautoriseerde handelingen uit te voeren. Een besmetting met malware kan bijvoorbeeld plaatsvinden door mensen te verleiden (social engineering) of door in te breken op een computersysteem (hacken). Veel voorkomende groepen van (technische) kwetsbaarheden zijn *buffer overflows*, injectie van code (onverwachte combinaties van codes aanbieden), configuratiefouten, zwakke wachtwoorden, onbeveiligde data- en netwerkprotocollen, en *zero-day*-kwetsbaarheden.

Deze handleiding gaat niet uitgebreid in op de verschillende kwetsbaarheden die aanleiding geven tot het daadwerkelijk laten slagen van een bepaalde vorm van cybercrime. Hoofdstuk 3 geeft bij verschillende verschijningsvormen een korte toelichting op enkele veel misbruikte klassen van kwetsbaarheden.

Een omvangrijk overzicht van kwetsbaarheden en mogelijke beschermende maatregelen voor webapplicaties wordt gegeven in de *Whitepaper Raamwerk Beveiliging Webapplicaties* (GOVCERT.NL, 11-11-2009) of op de website van het *Open Web Application Security Project* (OWASP, 2010). Een achtergrondstudie over veel voorkomende kwetsbaarheden in het bedrijfsleven en bij vitale infrastructuur is te vinden in verschillende publicaties en artikelen, zoals in *Security of Industrial Control Systems: What to Look for?* (Zwan, 2010).

Relatie tussen aanvalsmethoden



1.5 Vormen van cybercrime

Deze handleiding deelt de verschijningsvormen in naar de belangrijkste herkenbare wijzen waarop de handelingen plaatsvinden. Deze indeling is:

- Malware
- Computerinbraak (hacking)
- Websiteaanvallen
- Botnets
- *Denial of Service*-aanvallen
- Social engineering
- E-mailgerelateerde verschijningsvormen

Vaak komen de verschillende vormen voor in combinatie met andere technieken. Zo kan een computervirus dienen om een Trojaans paard te verspreiden, dat gegevens steelt tijdens een criminele activiteit. Ook kan eerst een netwerk worden afgeluisterd om vervolgens met de verkregen gegevens een ander computersysteem binnen te dringen. Een ander onderscheid wordt gemaakt tussen gerichte en ongerichte cyberaanvallen. Ongerichte cyberaanvallen hebben geen specifiek bedrijf of computersysteem als doelwit. Bij ongerichte aanvallen wordt getest op het bestaan van specifieke kwetsbaarheden waarna wordt getracht de kwetsbaarheid van het computersysteem te misbruiken, bijvoorbeeld door malware te installeren.

Bij gerichte cyberaanvallen wordt een specifiek bedrijf of computersysteem op de korrel genomen. De gebruikte aanvalsmethode zal bestaan uit maatwerk om de kans van slagen te vergroten en de kans op detectie te verkleinen. Deze handleiding schaart het uitvoeren van zowel gerichte als ongerichte aanvallen onder *hacking*, met uitzondering van specifieke activiteiten als malware, aanvallen op websites en *denial of service*, die apart zijn beschreven.

1.6 Omgaan met cybercrime

De wijze waarop een organisatie omgaat met cybercrime is altijd de verantwoordelijkheid van de organisatie zelf. Wordt een organisatie slachtoffer van cybercrime, dan moet de organisatie besluiten hoe hiermee wordt omgegaan. Aangifte doen is slechts één van de mogelijke acties. Afhankelijk van de situatie volstaat bijvoorbeeld het doen van alleen een melding of het starten van een civiele procedure. Veelal kiezen organisaties ervoor om eerst de schade als gevolg van cybercrime te herstellen en om de beveiligingsmaatregelen aan te scherpen.

Deze handleiding biedt praktische handvatten ten behoeve van de herkenning van cybercrime in technische en juridische zin. De handvatten staan los van de keuze van de organisatie hoe om te gaan met een cyberincident. Hoofdstuk 6 gaat dieper in op de stappen bij het doen van aangifte.

1.7 Organisatie van opsporing en bestrijding van cybercrime

ICT-veiligheid is een beleidsterrein dat niet onder één ministerie valt en waarin meerdere ministeries rollen, taken en verantwoordelijkheden hebben. De voornaamste betrokken departementen zijn het ministerie van Economische Zaken, Landbouw & Innovatie (EL&I), het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en het ministerie van Veiligheid en Justitie.

Bijlage E geeft een selectie van verschillende organisaties die een rol spelen bij de bescherming van informatie en de opsporing en vervolging van cybercrime.

HOOFDSTUK 2

Juridische en strafrechtelijke bepalingen

Onvoorzichtige gedragingen kunnen zowel door een handelen als door een nalaten worden begaan. Wanneer moet een dader weten dat zijn handelen vernieling of verandering van bijvoorbeeld een geautomatiseerd werk tot gevolg heeft?

In dit hoofdstuk worden juridische begrippen besproken die in zijn algemeenheid van belang zijn voor het omgaan met en eventueel strafrechtelijk aanpakken van cybercrime. Ook geeft dit hoofdstuk een toelichting op de strafrechtelijke bepalingen voor verschillende verschijningsvormen van cybercrime. Per strafbepaling wordt uitgelegd volgens welke criteria en aandachtspunten de strafwetgeving wordt toegepast.

2.1 Strafrechtelijke begrippen

Een aantal stafrechtelijke begrippen loopt als een rode draad door het strafrecht:

- Misdrijf versus overtreding
- Opzet versus schuld
- Wederrechtelijkheid
- Poging
- Deelnemingsvormen

2.1.1 Misdrijf versus overtreding

De Nederlandse strafwetgeving kent een onderverdeling in misdrijven en overtredingen. Het belangrijkste onderscheid is dat bij een overtreding nooit hoeft te worden aangetoond dat er sprake is van opzet of verwijtbare nalatigheid; het bewijs van de gedraging volstaat. Bovendien wordt een misdrijf aangetekend in het strafblad van de veroordeelde.

Een ander onderscheid is de mogelijkheid om poging of medeplichtigheid ten laste te leggen. Volgens de Nederlandse strafwetgeving kunnen de poging tot en de medeplichtigheid aan een strafbaar feit alleen in relatie tot misdrijven ten laste worden gelegd. Voor cybercrime is er altijd sprake van misdrijven.

Misdrijf	Overtreding
'Gaat in tegen rechtsgevoel'	'Niet houden aan afspraak'
Rechtsdelict	Wetsdelict
Opzet of schuld moet worden bewezen door het OM	Opzet of schuld verondersteld aanwezig te zijn
Poging is strafbaar	Poging is niet strafbaar
Medeplichtigheid is strafbaar	Medeplichtigheid is niet strafbaar
Behandeld door arrondissements-rechtbank	Behandeld door kantonrechter
Vrijheidsstraf is gevangenisstraf	Vrijheidsstraf is hechtenis
Verjaring na zes jaar of langer	Verjaring na drie jaar (art. 70 Sr)

De strafbaarstellingen met betrekking tot de misdrijven staan in Boek II van het Wetboek van Strafrecht. Overtredingen staan in Boek III van het Wetboek van Strafrecht.

2.1.2 Opzet versus schuld

In een aantal wetsartikelen komt het woord *opzet* of *schuld* voor.

Opzet

- *Oogmerk, opzet en voornemen*
  Komt één van deze woorden voor in een strafbepaling, dan wordt daarmee een vorm van opzet bedoeld waarbij de dader de bewuste wil heeft om op een bepaalde wijze te handelen of iets na te laten. De gedraging moet voortvloeien uit een wilsbesluit. Deze vorm van opzet wordt ook wel samengevat als *willens en wetens*: de dader wist zeker dat zijn handelen of nalaten een bepaald gevolg zou doen intreden en heeft dat gevolg ook gewild. Ongewild of ongeweten handelen is geen opzet in de zwaarste vorm.
- Een lichtere variant van opzet is het zogenoemde *voorwaardelijke opzet*.
  Dit houdt in dat een dader weliswaar er niet bewust voor kiest om de gevolgen van zijn handelen of nalaten te doen intreden, maar dat hij zich wel willens en wetens blootstelt aan de aanmerkelijke kans dat een bepaald gevolg zal intreden. Het 'op de koop toe nemen' van een bepaald gevolg wordt dus ook als opzet beschouwd. Daarnaast kent de wet ook het *noodzakelijkheidsbewustzijn*: de dader had zich moeten beseffen dat bepaalde consequenties eigenlijk onvermijdelijk waren als gevolg van een door hem verrichte handeling of nalaten.

Schuld

Onvoorzichtige gedragingen kunnen zowel door een handelen als door een nalaten worden begaan. Naast de onachtzaamheid die aanwezig moet zijn is het voor de beantwoording van de schuldvraag ook van belang dat deze onachtzaamheid - die ligt besloten in de schuld - ook verwijtbaar is. Met andere woorden: kon de dader weten dat zijn handelen vernieling of verandering van bijvoorbeeld een geautomatiseerd werk tot gevolg had?

Ook bij schuld bestaan er verschillende gradaties. De zwaarste vorm van schuld omvat bewuste en onbewuste schuld. In dit geval kan iemand geacht worden om te weten dat iets zou kunnen gebeuren. Schuld bestaat in dit geval uit het begaan hebben van een strafbare gedraging of onachtzaamheid van de dader (Jörg, 1994).

Er bestaan verschillende gradaties in opzet (dolus) (Jörg, 1994).

Artikel 161sexies Sr betreft de *opzettelijke* vernieling van een publiek geautomatiseerd werk of werk voor telecommunicatie. Artikel 161septies Sr echter beschrijft de vernieling van een publiek geautomatiseerd werk of werk voor telecommunicatie door *schuld* (culpose variant). Ook voor de vernieling, het veranderen of onbruikbaar maken van gegevens wordt dit onderscheid gemaakt. In artikel 350a Sr is opzet vereist, in artikel 350b Sr dient er sprake te zijn van het veranderen, vernielen of onbruikbaar maken door schuld.

De kern van de schuld (culpa) wordt gevormd door onvoorzichtigheid, onachtzaamheid of nalatigheid (Kamerstukken 1989/90, 21551, 1989-1990).

2.1.3 Wederrechtelijkheid

In diverse wetsartikelen is het begrip *wederrechtelijk* opgenomen. In artikel 138ab Sr moet er bijvoorbeeld sprake zijn van "opzettelijk en wederrechtelijk binnendringen".

Wederrechtelijkheid betekent in strijd met het geschreven of ongeschreven recht, of zonder daartoe gerechtigd te zijn. De wederrechtelijkheid ontbreekt wanneer men

- (legitieme) toestemming had om de gedraging te verrichten,
- handelde in noodweer of noodtoestand,
- handelde op grond van een wettelijk voorschrift of een bevoegd gegeven ambtelijk bevel.

Als het begrip opzet vóór het begrip wederrechtelijk in een wetsartikel staat, betekent dit dat het opzet zowel op de wederrechtelijkheid als op de strafbare gedraging slaat. Staat het woordje *en* tussen het begrip opzet en wederrechtelijk, dan hoeft niet te worden bewezen dat de dader ook wist dat de gedraging wederrechtelijk was. Het opzet slaat in dit geval niet op de wederrechtelijkheid.

2.1.4 Poging

Bij misdrijven is ook een *poging* tot die misdrijven strafbaar (art. 45, lid 1 Sr.). Bij poging moet er sprake zijn van een voornemen van de dader en een begin van uitvoering van de daad. Het voornemen mag gelijkgesteld worden aan (voorwaardelijk) opzet. Er is sprake van een begin van uitvoering als de gedragingen, objectief bekeken, bedoeld zijn het misdrijf te voltooien.

Voor een poging moeten het middel en het object wel enigszins deugdelijk zijn, anders is er sprake van een *ondeugdelijke* poging. De poging kan daarbij *relatief* of *absoluut* ondeugdelijk zijn:

- Bij een *relatief* ondeugdelijke poging deugt het gebruikte middel en het object, maar de manier waarop beide tot elkaar worden gebracht niet.
- Bij een *absoluut* ondeugdelijke poging is hetzij het middel, hetzij het object op zichzelf geheel ondeugdelijk.
- Slechts de *absoluut ondeugdelijke* pogingen zijn niet strafbaar.

Als maximumstraf bij poging geldt de hoofdstraf die op het misdrijf gesteld is, verminderd met een derde (art. 45, lid 2 Sr).

2.1.5 Deelnemingsvormen

Bij cybercrime kan sprake zijn van strafrechtelijk beschreven deelnemingsvorm aan strafbare feiten. Er is onderscheid tussen daderschap en medeplichtigheid.

Artikel 47 Sr omschrijft de verschillende categorieën *daders*, te weten zij die het feit (misdrijf of overtreding):

- plegen: de materiële dader, ofwel degene die het strafbare feit zelf pleegt;
- doen plegen: de intellectuele dader die iemand anders (dwingend) doet plegen;
- medeplegen: twee of meer personen plegen gezamenlijk een strafbaar feit door bewuste samenwerking of gezamenlijke uitvoering;
- uitlokken: degene die door giften, beloften, misbruik van gezag, geweld, bedreiging, of misleiding of door het verschaffen van gelegenheid, middelen of inlichtingen het feit opzettelijk uitlokt.

Van *medeplichtigheid* is sprake als iemand opzettelijk direct behulpzaam is bij het plegen van het misdrijf, of indirect door opzettelijk gelegenheid, middelen of inlichtingen te verschaffen tot het plegen van het misdrijf (art.48 Sr). Iemand verleent dus opzettelijk hulp bij een misdrijf dat door een ander wordt gepleegd zonder zelf als dader (medepleger) te worden beschouwd.

Bij de verschillende vormen van daderschap (art. 47 Sr) geldt de maximumstraf voor het misdrijf. Als maximumstraf bij medeplichtigheid geldt de hoofdstraf die op het misdrijf gesteld is, verminderd met een derde (art. 49, lid 2 Sr).

Medeplichtigheid aan een overtreding is niet strafbaar, medeplegen of uitlokken wel.

2.1.6 Strafmaat

Bij een artikel in het Wetboek van Strafrecht is de strafmaat een gevangenisstraf en/of een geldboete. De hoogte van de geldboete is vermeld als een categorie, waarvan de hoogte in artikel 23 Sr zijn opgenomen, te weten:[7]

- de eerste categorie, € 380,-
- de tweede categorie, € 3.800,-
- de derde categorie, € 7.600,-
- de vierde categorie, € 19.000,-
- de vijfde categorie, € 76.000,-
- de zesde categorie, € 760.000,-

2.1.7 Verhalen van schade

Als gevolg van handelingen van een dader kan (financiële) schade ontstaan. Deze kan volgens het Burgerlijk wetboek worden verhaald. Dan moet worden aangetoond dat er ook echt schade is ontstaan. Bijvoorbeeld de financiële schade als gevolg van inbraak op een draadloze netwerkverbinding en deze gebruiken om het internet op te gaan is lastig aan te tonen. Want welke schade is er voor de eigenaar ontstaan? Een verlies aan bandbreedte is niet kwantificeerbaar.

Kan de schade als gevolg van een onrechtmatige daad wel worden aangetoond, dan kan dit in een civiele procedure worden verhaald (art. 6:162 Bw). Ook kan een zogenoemd “verzoek tot voeging” worden ingediend bij de Officier van Justitie om de civiele zaak toe te voegen aan een lopende strafzaak (art. 51a Sv).

7. Bedragen geldend per 1 januari 2010.

2.1.8 Aansprakelijkheid en schuld van de eigenaar

Eigenaren van computersystemen of netwerken zijn in beginsel aansprakelijk voor alles wat vanaf zijn computer of (draadloze) netwerk gebeurt. Onder artikel 6:162 van het Burgerlijk Wetboek geldt een drietal gronden waarop een bepaalde schadeveroorzakende gedraging als onrechtmatig kan worden aangemerkt:

- inbreuk op een recht;
- of een doen of nalaten in strijd met een wettelijke plicht;
- of een doen of nalaten in strijd met hetgeen volgens ongeschreven recht in het maatschappelijk verkeer betaamt. In dit laatste geval wordt ook wel gesproken van betamelijkheids- of zorgvuldigheidsnormen.[8]

De eigenaar die de voordeur van zijn draadloze netwerk wagenwijd open laat staan, kan beticht worden van onvoorzichtig handelen. De eigenaar had moeten weten dat er tegenwoordig gemakkelijk misbruik van gemaakt kan worden. Individuele omstandigheden, zoals de expertise van de eigenaar, instellingen ter voorkoming van en normaal gebruik van WiFi, spelen hierbij een rol.
Als aan deze voorwaarden voldaan wordt en de eigenaar kan het slachtoffer op geen enkele manier op de daadwerkelijke dader wijzen, kan de eigenaar eventueel zelf aansprakelijk worden gesteld.

Een eigenaar van een systeem kan ook strafbaar zijn voor het veroorzaken van stoornis in de gang of werking van een geautomatiseerd werk van een ander door schuld. Op grond van artikel 161septies Sr. WvS kan bijvoorbeeld degene die het mogelijk maakt dat er sprake is van een *open web proxy* of *mail relay* strafbaar zijn.

Schuld kan ontstaan door onachtzaamheid. Van onachtzaamheid is sprake als men een netwerk open laat staan. Daarmee heeft een ander toegang tot het netwerk. In het geval van onachtzaamheid moet voor de beantwoording van de schuldvraag nog wel worden bewezen dat deze onachtzaamheid ook verwijtbaar is. Kon de rechthebbende weten dat het feit dat hij zijn netwerk heeft laten openstaan, geleid heeft tot stoornis in de gang of werking van het (computer)systeem.

2.2 Cybercrime in enge zin

Strafrechtelijke bepalingen uit het Wetboek van Strafrecht bij cybercrime in enge zin bevat de categorieën:

- Binnendringen in een geautomatiseerd werk;
- Stoornis in de gang of werking van een (publiek) geautomatiseerd werk;
- Onbruikbaar maken, veranderen of aantasten van gegevens;
- Afluisteren.

Ieder onderwerp in deze paragraaf bevat het integrale artikel uit het Wetboek van Strafrecht en een toelichting op de criteria waaraan moet worden voldaan om van een strafbaar feit te kunnen spreken.

2.2.1 Binnendringen in een geautomatiseerd werk

Het binnendringen in een geautomatiseerd werk[9] is strafbaar gesteld in artikel 138ab Sr (ingevoerd in 1993 als art. 138a Sr; bij wet van 24 juli 2010 is dit opnieuw genummerd in art. 138ab):

Artikel 138ab Sr

1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:
   a. door het doorbreken van een beveiliging,
   b. door een technische ingreep,
   c. met behulp van valse signalen of een valse sleutel, of
   d. door het aannemen van een valse hoedanigheid.
2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.
3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens
   a. met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk;
   b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.

Toelichting

Het binnendringen in een computer is vergelijkbaar met het binnendringen in een woning. Er is sprake van opzettelijk binnendringen in een computer als de dader *wil* binnendringen. Van huisvredebreuk is sprake als men binnengaat *tegen* de wil van de bewoner. De wil kan blijken uit woorden of uit daden.

8. Zie ook http://www.iusmentis.com/aansprakelijkheid/onrechtmatigedaad/
9. Zie de begrippenlijst voor een toelichting bij 'geautomatiseerd werk'.

Met dit artikel is elke vorm van opzettelijk en wederrechtelijk binnendringen strafbaar gesteld, ook als daarbij geen beveiliging wordt doorbroken. De opsomming onder lid 1, met de woorden 'in ieder geval', is niet-limitatief. Het doorbreken van een beveiliging of het gebruik van een technische ingreep, valse signalen of hoedanigheid is dus geen noodzakelijke voorwaarde. Het is wel een voldoende voorwaarde: het enkel doorbreken van een beveiliging is voldoende om van binnendringen te spreken.

Bij het toegang verwerven tot een computer door het gebruik van een valse hoedanigheid kan worden gedacht aan het gebruik van het wachtwoord en de gebruikersnaam van een ander. Een veelgebruikte manier om deze gegevens te ontfutselen is het zogenoemde *social engineering*. Via een listige manier worden gegevens van een ander verkregen, bijvoorbeeld door zich voor te doen als systeembeheerder die deze gegevens van de gebruiker nodig heeft voor onderhoud aan het systeem.

Van een technische ingreep is sprake als er bijvoorbeeld wordt binnengedrongen via een speciaal daarvoor geschreven programma. Valse signalen of een valse sleutel is bijvoorbeeld een zelf gegenereerde toegangscode die het computersysteem activeert, of een (geldig) wachtwoord dat de persoon in kwestie niet behoort te hebben.

Strafmaat
Wordt aan bovengenoemde criteria voldaan, dan kan de rechter ten hoogste een jaar gevangenisstraf of een geldboete van maximaal € 19.000,- opleggen.

Is iemand binnengedrongen en neemt vervolgens gegevens op of over of tapt men het systeem af, dan wordt de straf verhoogd. De rechter kan dan vier jaar gevangenisstraf of een geldboete van maximaal € 19.000,- opleggen. Overnemen of vastleggen van gegevens is bijvoorbeeld als iemand gegevens van de binnengedrongen computer naar een eigen medium kopieert.
Deze strafverzwarende omstandigheid is vaak aan de orde. Meestal wordt in een geautomatiseerd werk ingebroken om gegevens over te nemen, vast te leggen of te wissen. In dit laatste geval is ook sprake van het misdrijf aantasting van gegevens (artikel 350a en 350b Sr).

Als iemand via een openbaar telecommunicatienetwerk - dus geen intern bedrijfsnetwerk - inbreekt, kan dat een andere strafverzwarende omstandigheid met dezelfde maximumstraffen betekenen. Daarvoor moet de dader:
- gebruik maken van de verwerkingscapaciteit van een geautomatiseerd werk met het doel om zichzelf te bevoordelen, of
- gebruik maken van het binnengedrongen geautomatiseerd werk om binnen te dringen in het geautomatiseerde werk van een derde.

Deze strafverhoging is ontstaan toen computerrekenkracht nog relatief schaars en duur was. Misbruiken van een computer via het internet is hiermee strafbaar op grond van het binnendringen in een geautomatiseerd werk. Ook is voor strafverhoging gekozen omdat het bij een keten van computerinbraken moeilijk is om de bron te achterhalen, en justitie daarom aftapbevoegdheden moet kunnen inzetten.

2.2.2 Stoornis in de gang of werking

Belemmeren van de toegang of het gebruik
Het belemmeren van de toegang tot of het gebruik van een geautomatiseerd werk door het aanbieden of toezenden van gegevens is strafbaar gesteld in artikel 138b Sr. Dit luidt:

Artikel 138b Sr

Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden.

Deze bepaling richt zich in het bijzonder op het strafbaar stellen van zogenoemde DDoS-aanvallen *(distributed denial of service)* en bijvoorbeeld *e-mail bombing*.

Op basis van artikel 138b Sr gelden de volgende criteria voor strafbaarstelling:
1. opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren,
2. door middel van het aanbieden of het toezenden van gegevens.

Toelichting
"Opzettelijk en wederrechtelijk" betekent in dit verband dat de dader de bedoeling had om de toegang tot of het gebruik van het geautomatiseerde werk te belemmeren, ongeacht of hij op de hoogte was van het feit dat hij daarmee een wederrechtelijke handeling uitvoerde.

"De toegang tot of het gebruik van (...) belemmeren" wijst erop dat dit artikel bewust is geschreven met het oog op (D)DoS-aanvallen. De definitie heeft tot doel om zoveel mogelijk (D)DoS-vormen erin onder te brengen. Zulke aanvallen kennen weliswaar een vergelijkbare aanvalstechniek, maar ze kunnen zeer verschillende doelen en uitwerkingen hebben. Het aanbieden of toezenden van gegevens is ook een voorbeeld van de bewust gekozen brede definitie. Semantische discussies over wat precies verstaan moet worden onder de term "toezenden" zijn daardoor overbodig.

Naast DDoS-aanvallen bevat artikel 138b Sr ook het platleggen van een mailbox door enorme hoeveelheden gegevens toe te zenden (e-mailbom). Spam is echter niet strafbaar op basis van dit artikel, behalve als het opzettelijk wordt toegezonden om de mailbox van de gebruiker te verstoppen.

Dit artikel is breder van toepassing dan artikel 161sexies Sr (zie hierna), aangezien voor toepasselijkheid van dat laatste artikel sprake moet zijn van een openbaar belang of van gevaar voor goederen of leven.

Strafmaat

Is een dader strafbaar onder art. 138b Sr, dan kan hij maximaal een jaar gevangenisstraf opgelegd krijgen of een geldboete van maximaal € 19.000,-

Stoornis in de gang of werking van een publiek geautomatiseerd werk

Het veroorzaken van stoornis in de gang of werking is, naast in artikel 138b, ook strafbaar gesteld in de artikelen 161sexies en 161septies Sr. Met deze artikelen wordt de ongestoorde automatische opslag, verwerking en overdracht van gegevens beschermd voor computers of gegevens met een publiek belang (bijvoorbeeld nuts- of overheidsdiensten) of waarbij levensgevaar dreigt. Het Wetboek van Strafrecht onderscheidt hierbij de situatie waarin iemand *opzettelijk* een werk vernielt (art. 161sexies Sr) van de situatie dat dit niet opzettelijk gebeurt, maar waarbij de dader *verwijtbaar nalatig* is (art. 161septies Sr).

Artikel 161sexies Sr

1. Hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft:
   1°. met gevangenisstraf van ten hoogste een jaar of geldboete van de vijfde categorie, indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens ten algemene nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst, ontstaat;
   2°. met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is;
   3°. met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie, indien daar van levensgevaar voor een ander te duchten is;
   4°. met gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie, indien daar van levensgevaar voor een ander te duchten is en het feit iemands dood ten gevolge heeft.
2. Met gevangenisstraf van ten hoogste een jaar of geld boete van de vijfde categorie wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in het eerste lid wordt gepleegd:
   a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of
   b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

Artikel 161sexies: opzet

Bij het opzettelijk veroorzaken van stoornis van een computer of openbaar telecommunicatienetwerk gaat het om:
1. het beschadigen of onbruikbaar maken van een geautomatiseerd werk, of
2. het vernielen van een geautomatiseerd werk, of
3. het buiten werking stellen van een veiligheidsmaatregel die ten opzichte van het geautomatiseerde werk is genomen.

Op basis van artikel 161sexies Sr zijn deze handelingen alleen strafbaar als een bepaald *gevolg* optreedt. Afhankelijk van de ernst van het gevolg staan er zwaardere strafmaxima op de gedraging. Het gaat om:
- verhindering of bemoeilijking met als gevolg stoornis bij de opslag of verwerking van gegevens ten algemene nutte (bijvoorbeeld van www.overheid.nl of van een elektriciteitscentrale), in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst;
- gemeen (vanuit het publiek belang gezien) gevaar voor goederen of voor de verlening van diensten;
- levensgevaar voor een ander;
- levensgevaar voor een ander en het feit heeft iemands dood tot gevolg.

Artikel 161septies: schuld

De term opzettelijk (art. 161sexies) geeft aan dat de wil van de dader gericht moet zijn op het veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk. Het gaat om iedere vorm van opzet, inclusief voorwaardelijk opzet (het op de koop toe nemen dat de stoornis optreedt).

Bij schuld (art. 161septies) gaat het om verwijtbare nalatigheid, bijvoorbeeld als de systeembeheerder van een elektriciteitscentrale dusdanig slordig is dat er brandgevaar dreigt vanwege defecte computeraansturing.

Artikel 161septies Sr

Hij aan wiens schuld te wijten is dat enig geautomatiseerd werk of enig werk voor telecommunicatie wordt vernield, beschadigd of onbruikbaar gemaakt, dat stoornis in de gang of in de werking van zodanig werk ontstaat, of dat een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verijdeld, wordt gestraft:

1°. met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie, indien daardoor verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens ten algemenen nutte, stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst, of gemeen gevaar voor goederen of voor de verlening van diensten ontstaat;

2°. met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie, indien daardoor levensgevaar voor een ander ontstaat;

3°. met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie, indien het feit iemands dood ten gevolge heeft.

Een voorbeeld van een veiligheidsmaatregel is een technische voorziening zoals een firewall, logische toegangsbeveiliging zoals username en password of het gebruik van encryptie. Het kan ook de safety en besturingssystemen om een industrieel proces veilig te kunnen laten plaatsvinden betreffen, zoals industriële controle systemen als SCADA (Supervisory Control And Data Acquisition).

Bij de stoornis van gegevens ten algemene nutte moet het gaan om werken die iedereen ten dienste staan, dus niet de computersystemen die binnen een organisatie worden gebruikt. Het systeem is ten algemene nutte als er een openbare dienst mee verleend wordt (Nijboer, 2002).
Dit artikel geldt vooral de toenemende automatisering van overheidsinstellingen. Steeds meer contacten met de burger vinden geautomatiseerd plaats of worden geautomatiseerd afgehandeld. Denk aan belastingaangifte, aanvragen van huursubsidie en opvragen van informatie.

Teweeg brengen van gemeen gevaar voor dienstverlening ten algemene nutte is strafbaar gesteld, omdat dit in economisch opzicht in de informatiemaatschappij van vergelijkbaar belang is als de productie en handel in goederen (Kamerstukken 1989/90, 21551, 1989-1990).
Een voorbeeld van gemeen gevaar is de stoornis van een computernetwerk van de elektriciteits- of watervoorziening of een andere vitale infrastructuur.[10]

Voorbereidingshandelingen

In navolging van het Cybercrime-verdrag is het misbruik van hulpmiddelen strafbaar gesteld.[11] Het gaat om voorbereidingshandelingen voor het veroorzaken van stoornis in de werking van een publiek geautomatiseerd werk. Hiervoor is artikel 161sexies uitgebreid met lid 2.

In dit artikel is strafbaar gesteld het maken, verkrijgen, verspreiden of bezitten van hulpmiddelen om bijvoorbeeld een DDoS-aanval te plegen of computers te saboteren om daarmee een publieke voorziening te treffen. Ook het bezit van wachtwoorden of toegangscodes, die geschikt zijn om het genoemde delict uit te kunnen voeren, is strafbaar. Nog een criterium voor strafbaarstelling is dat iemand de hulpmiddelen moet maken, (ver)kopen of bezitten met het oogmerk (dus willens en wetens) dat er daadwerkelijk een delict zoals bedoeld in artikel 161sexies lid 1 mee zal worden gepleegd. Deze bedoeling zal moeten blijken uit zijn woorden, daden of uit de omstandigheden van het incident.

Strafmaat

In beide artikelen wordt een opsomming gegeven van de gevolgen die kunnen optreden door het veroorzaken van stoornis in een geautomatiseerd werk. De strafbaarstelling is gebaseerd op het optreden van één van deze gevolgen. Afhankelijk van de gevolgen die intreden kan de strafmaat variëren van een gevangenisstraf van ten hoogste één tot vijftien jaar of een geldboete van €76.000,-.

Als sprake is van schuld in plaats van opzet, ligt de strafmaat lager. Net als bij het opzettelijk veroorzaken van stoornis in een geautomatiseerd werk is bij het veroorzaken van stoornis door schuld de strafmaat afhankelijk van de gevolgen. De strafmaat kan variëren van een gevangenisstraf of hechtenis van ten hoogste zes maanden tot een gevangenisstraf of hechtenis van ten hoogste twee jaar of een geldboete van €19.000,-.

Bij voorbereidingshandelingen is de straf dezelfde als die op de hoofddelicten staat. Dat wijkt af van de algemene strafbaarstelling van voorbereidingshandelingen, waarbij de straf met de helft wordt verminderd (art. 46 Sr). Dat betekent dat op misbruik van hulpmiddelen voor (enkel) hacken en computersabotage een gevangenisstraf van ten hoogste een jaar of geldboete van € 76.000,- staat.

10. In de rechtspraak is in het verleden een DDoS-aanval op de webpagina van een e-winkel onder art. 161sexies gebracht, maar dat was voordat art. 138b Sr was ingevoerd en past niet goed bij het ‘gemeengevaarlijke’ karakter van art. 161sexies en 161septies.
11. Artikel 139d lid 2 en 3 en artikel 161sexies lid 2 Sr zijn hiervoor toegevoegd.

2.2.3 Onbruikbaar maken, veranderen of aantasten van gegevens

Het onbruikbaar maken, veranderen of anderszins aantasten van gegevens is strafbaar gesteld in de artikelen 350a en 350b Sr. Deze artikelen beschermen het ongestoorde gebruik van computergegevens tegen onder meer onbevoegde verandering of het ontoegankelijk maken van die gegevens (Kamerstukken 2004/05, 26671, 2005).

Het Wetboek van Strafrecht onderscheidt de situatie waarin iemand *opzettelijk* gegevens onbruikbaar maakt of verandert (art. 350a Sr) van de situatie dat dit niet opzettelijk gebeurt, maar er wel sprake is van *schuld* (art. 350b Sr).

In de artikelen 250 a en 350 b Sr. zijn twee gedragingen strafbaar gesteld: het aantasten van gegevens (lid 1 en 2), en het ter beschikking stellen en verspreiden van gegevens die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, zoals computervirussen, wormen en andere malware (lid 3).

Artikel 350a: opzet

Artikel 350a Sr

1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.
2. Hij die het feit, bedoeld in het eerste lid, pleegt na door tussenkomst van een openbaar telecommunicatienetwerk, wederrechtelijk in een geautomatiseerd werk te zijn binnengedrongen en daar ernstige schade met betrekking tot die gegevens veroorzaakt, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.
3. Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die zijn bestemd om schade aan te richten in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
4. Niet strafbaar is degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken.

Op basis van artikel 350a Sr zijn de criteria voor strafbaarstelling van het *opzettelijk* onbruikbaar maken en veranderen van gegevens:

1. Er is sprake van gegevens.
2. De gegevens zijn via een geautomatiseerd werk opgeslagen, of worden door een computer verwerkt of overgedragen.
3. De gegevens worden opzettelijk en wederrechtelijk veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, of er worden opzettelijk andere gegevens aan toegevoegd.

Naast het opzettelijk veranderen of onbruikbaar maken van gegevens is expliciet strafbaar gesteld het ter beschikking stellen en verspreiden van gegevens die schade aanrichten door zichzelf te vermenigvuldigen. Dit artikel is specifiek gericht op computervirussen en andere vormen van malware. Voor strafbaarheid is het voldoende dat iemand de malware ter beschikking stelt of verspreidt, ongeacht of de malware ook daadwerkelijk schade aanricht.

Merk op dat spyware hier *niet* onder valt; dergelijke software is niet bestemd om *schade in de computer* aan te richten. Op spyware is mogelijk wel het eerste lid van art. 350a Sr van toepassing.

Artikel 350b: schuld

Artikel 350b Sr

1. Hij aan wiens schuld te wijten is dat gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, wederrechtelijk worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, dan wel dat andere gegevens daaraan worden toegevoegd, wordt, indien daardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt, gestraft met gevangenisstraf of hechtenis van ten hoogste een maand of geldboete van de tweede categorie.
2. Hij aan wiens schuld te wijten is dat gegevens wederrechtelijk ter beschikking gesteld of verspreid worden die zijn bestemd om schade aan te richten in een geautomatiseerd werk, wordt gestraft met gevangenisstraf of hechtenis van ten hoogste een maand of geldboete van de tweede categorie.

Toelichting

Het artikel beschermt niet alleen gegevens die op het moment van handelen van de dader in een geautomatiseerd werk aanwezig zijn (opgeslagen). Ook de gegevens die gedurende de handeling van de dader worden verwerkt of overgedragen (waaronder het verzenden) vallen hieronder. Gegevens die worden verwerkt of overgedragen zijn bijvoorbeeld gegevens die van een floppy naar een beeldscherm, van een computer naar een printer en van een computer naar een andere computer worden overgezet (Nijboer, 2002).

Het 'onbruikbaar maken' van gegevens kan bijvoorbeeld plaatsvinden door het wijzigen, veranderen, toevoegen, wissen of ontoegankelijk maken van de gegevens, zoals het wijzigen van een toegangscode. Het ontoegankelijk maken kan leiden tot het onbruikbaar maken van gegevens. Veranderen of wissen van gegevens is een andere vorm van onbruikbaar maken. Ook het toevoegen van gegevens is strafbaar, omdat het de integriteit van de verzameling computergegevens als geheel aantast.

Opzettelijk betekent dat de verdachte:
- de bedoeling moet hebben gehad om gegevens ter beschikking te stellen en te verspreiden, en
- wist dat de gegevens bestemd zijn om schade aan te richten.

De criteria voor de 'culpoze' (aan schuld te wijten) malwareverspreiding zijn hetzelfde als bij de opzettelijke variant, behalve dat het nu gaat om verwijtbare nalatigheid. Een dader is niet strafbaar in het geval hij de gegevens verspreidt met de bedoeling om de schade, die veroorzaakt werd door een eerder (door een ander) verspreid programma, te beperken (art.350a, lid 4 Sr).

Strafmaat

Is aan bovengenoemde criteria voldaan, dan kan de rechter een gevangenisstraf van ten hoogste twee jaar of een geldboete van € 19.000,- opleggen.

De rechter kan een hogere straf opleggen als iemand een openbaar telecommunicatienetwerk gebruikt om in te breken in een geautomatiseerd werk en vervolgens ernstige schade toebrengt aan gegevens die zich in dat geautomatiseerd werk bevinden. De gevangenisstraf kan dan worden verhoogd tot maximaal vier jaar.

Veranderen, wissen, onbruikbaar of ontoegankelijk maken en/of toevoegen van andere gegevens wordt aangemerkt als schade.
Ernstige schade is bijvoorbeeld schade die grote financiële gevolgen heeft en/of schade die moeilijk te herstellen is. De rechtspraak noemt als voorbeeld als (een deel van) een computersysteem van een bedrijf meer dan 12 uur ontoegankelijk is.[12]

Het opzettelijk en wederrechtelijk ter beschikking stellen en verspreiden van malware wordt gestraft met gevangenisstraf van ten hoogste vier jaar of een geldboete van € 76.000,-.

Als sprake is van schuld in plaats van opzet, ligt de strafmaat lager. Het wederrechtelijk veranderen of onbruikbaar maken van gegevens door schuld kan worden bestraft met een gevangenis of hechtenis van ten hoogste één maand of een geldboete van € 3.800,-. Ook het wederrechtelijk ter beschikking stellen en verspreiden van malware kan worden bestraft met een gevangenisstraf, hechtenis van ten hoogste één maand of een geldboete van € 3.800,-.

2.2.4 Afluisteren

Deze paragraaf beschrijft de artikelen 139c, 139d en 139e Sr voor het aftappen en opnemen van gegevens in relatie tot een telecommunicatienetwerk of via een geautomatiseerd werk.[13]

Aftappen en/of opnemen van gegevens

Het aftappen en/of opnemen van gegevens door een geautomatiseerd werk of telecommunicatienetwerk is strafbaar gesteld in artikel 139c Sr:

Artikel 139c Sr

1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk.
2. Het eerste lid is niet van toepassing op het aftappen of opnemen:
   1°. van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.
   2°. door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting, behoudens in geval van kennelijk misbruik;
   3°. ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2002.

De termen aftappen en opnemen hebben in de strafwet al een min of meer vastomlijnde betekenis en worden gebruikt voor het onderscheppen en vastleggen van stromende gegevens (zoals in art. 126m Sv). Gaat het om het kopiëren van bestaande, opgeslagen gegevens, dan wordt de term *overnemen* gebruikt.

Voor dit artikel is gedacht aan de bescherming van de overdracht van gegevens binnen computers of via een elektro-

12. HR 19 januari 1999, NJ 1999, 251.
13. In een recent conceptwetsvoorstel 'Versterking bestrijding computercriminaliteit' wordt onder meer voorgesteld om de artikelen 139a, 139b, 139c en 139e te wijzigen. Zie http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/kamerstukken/2010/07/28/wetsvoorstel-versterking-bestrijding-computercriminaliteit/wetsvoorstel.pdf

nisch communicatienetwerk, of door daarop aangesloten randapparatuur.

Voor strafbaarheid van het aftappen en/of opnemen van gegevens gelden de volgende criteria:[14]

1. Er moet sprake zijn van gegevens.
2. Deze gegevens worden via een telecommunicatienetwerk, een geautomatiseerd werk of daarop aangesloten randapparatuur overgedragen.
3. Iemand gebruikt een technisch hulpmiddel om de gegevens af te tappen en/of op te nemen.
4. De gegevens zijn niet voor hem, mede voor hem of voor degene in wiens opdracht hij handelt bestemd.
5. Het aftappen gebeurt opzettelijk.
6. Er is geen sprake van een van de genoemde uitzonderingen:
   - het opvangen van radiosignalen zonder bijzondere inspanning;
   - aftappen of opname door of in opdracht van de gerechtigde voor een door hem gebruikte aansluiting (bijvoorbeeld een werkgever), behalve als deze zijn bevoegdheid kennelijk misbruikt;
   - voor de goede werking van een openbaar telecommunicatienetwerk, of door de strafvordering of door inlichtingen- en veiligheidsdiensten.

Toelichting

Omdat de gegevens niet voor de dader, mede voor de dader of voor degene in wiens opdracht hij handelt bestemd zijn, betekent dat de dader normaliter geen toestemming had voor het aftappen en/of opnemen. In dat geval handelt hij onrechtmatig.

In een aantal situaties is het aftappen en/of opnemen van gegevens wel toegestaan:

1. In het geval dat er sprake is van het opnemen van gegevens door apparaten die radiocommunicatiesignalen ontvangen, zoals radio's en portofoons (walkietalkies). De reden voor deze uitzondering is dat signalen verzonden via de ether vrij zijn.
   Als iemand echter een bijzondere inspanning verricht, bijvoorbeeld met speciale apparatuur of door langdurig een bepaald signaal fysiek te volgen, is hij wel strafbaar.
2. Als er sprake is van het aftappen en/of opnemen van een door, of in opdracht van, de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting. Er mag dan geen misbruik van worden gemaakt. Bijvoorbeeld als een bedrijf misbruik van haar netwerk door haar werknemers wil opsporen. Het bedrijf kan een technisch hulpmiddel (laten) installeren om het systeem af te tappen.
3. Het opzettelijk afluisteren van een gesprek met een technisch hulpmiddel, zonder zelf deelnemer te zijn of daartoe door een deelnemer opdracht te hebben gekregen, is strafbaar onder art. 139a Sr. Een persoon die wél gespreksdeelnemer is en zonder toestemming een gesprek heeft opgenomen, is *niet* strafbaar. Een deelnemer aan een vertrouwelijk gesprek mag dus heimelijk opnamen maken met bijvoorbeeld een *smartphone*.[15]
   Het op kenbare wijze opnemen van gesprekken in een publieke ruimte is eveneens niet strafbaar.

Gelet op de afbakening van deze handleiding zijn de artikelen over het afluisteren van gesprekken in of buiten een woning, besloten lokaal of erf (art. 139a en 139b Sr) buiten beschouwing gelaten.

Strafmaat

Het aftappen en/of opnemen van gegevens overgedragen door een telecommunicatienetwerk, een computersysteem of een daarop aangesloten randapparatuur kan worden gestraft met een gevangenisstraf van ten hoogste één jaar of een geldboete van € 19.000,-.

Het plaatsen van opname-, aftap- c.q. afluisterapparatuur

Het plaatsen van opname-, aftap- c.q. afluisterapparatuur is strafbaar gesteld in artikel 139d Sr. Dit luidt:

Artikel 139d Sr

1. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen, een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn.
2. Met dezelfde straf wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab, eerste lid, 138b of 139c wordt gepleegd:
   a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of
   b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden gekregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

14. Als het conceptwetsvoorstel 'Versterking bestrijding computercriminaliteit' wordt ingevoerd, wordt iedere vorm van opzettelijk en wederrechtelijk met een technisch middel aftappen of opnemen van de niet-openbare overdracht van gegevens, of overnemen van opgeslagen niet-openbare gegevens voor zichzelf of voor een ander, strafbaar (art. 139c lid 1 Sr).
15. Als het conceptwetsvoorstel 'Versterking bestrijding computercriminaliteit' wordt ingevoerd, maakt dit ook het in een woning heimelijk (opzettelijk en wederrechtelijk met een technisch hulpmiddel) opnemen van een gesprek strafbaar (ar.139a Sr).

Artikel 139d Sr *(vervolg)*

3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft hij die het in het tweede lid bedoelde feit pleegt terwijl zijn oogmerk is gericht op een misdrijf als bedoeld in artikel 138ab, tweede of derde lid.

Het betreft hier de fase vóór het aftappen en/of opnemen. Als iemand daarvoor een technisch hulpmiddel wil gebruiken, zal hij dit eerst ergens moeten plaatsen.

De volgende criteria gelden voor strafbaarheid van het plaatsen van dergelijke apparatuur:

1. Er moet sprake zijn van plaatsing van een technisch hulpmiddel ergens.
2. Met het plaatsen heeft iemand de bedoeling om een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk af te luisteren, af te tappen en/of op te nemen.
3. Er is geen toestemming verleend door een rechthebbende om het technische hulpmiddel te plaatsen.

Toelichting
Om te beoordelen of iemand de bedoeling heeft gehad om een gesprek, telecommunicatie of andere gegevensoverdracht af te luisteren en/of op te nemen, is de kennelijke intentie van de dader doorslaggevend. Voldoende is dat een technisch hulpmiddel is geplaatst, het hoeft nog niet in werking te zijn gesteld.[16]

Toestemming kan blijken uit woorden of daden van de rechthebbende, meestal de eigenaar van de bedoelde plaats of geautomatiseerd werk.

Voorbereidingshandelingen
In navolging van het Cybercrime-verdrag is ook het misbruik van hulpmiddelen strafbaar gesteld. Het gaat om voorbereidingshandelingen voor het plegen van een computerdelict of afluisteren. Hiervoor zijn lid 2 en 3 toegevoegd aan artikel 139d Sr. In dit artikel is strafbaar gesteld het maken, verkrijgen, verspreiden of bezitten van hulpmiddelen om bijvoorbeeld te hacken, een DoS-aanval te plegen, computers te saboteren of af te luisteren. Hulpmiddelen om virussen of andere malware te maken vallen hier overigens niet onder (zie daarvoor artikel 350a Sr). Onder hulpmiddelen wordt zowel software als hardware verstaan. Ook het bezit van wachtwoorden of toegangscodes die geschikt zijn om deze delicten uit te voeren is strafbaar.

Nog een criterium voor strafbaarstelling is dat iemand de hulpmiddelen moet maken, (ver)kopen of bezitten met het oogmerk (dus willens en wetens) dat er daadwerkelijk een computerdelict zoals bedoeld in artikelen 138ab lid 1, 138b of 139c mee zal worden gepleegd. Deze bedoeling zal moeten blijken uit zijn woorden of daden.
Het maken of bezitten is toegestaan als de hulpmiddelen bedoeld zijn om (rechtmatig) de beveiliging van een computersysteem te testen.[17]

Reclame maken voor een technisch hulpmiddel voor het heimelijk afluisteren, aftappen of opnemen van gesprekken, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk, is eveneens strafbaar gesteld (art. 441a Sr).

Strafmaat
Het plaatsen van opname-, aftap- c.q. afluisterapparatuur kan worden gestraft met een gevangenisstraf van ten hoogste één jaar of een geldboete van € 19.000,-.

Bij voorbereidingshandelingen is de straf dezelfde als voor de hoofddelicten. Dat wijkt af van de algemene strafbaarstelling van voorbereidingshandelingen, waarbij de straf met de helft wordt verminderd (art. 46 Sr). Dat betekent dat op misbruik van hulpmiddelen voor (enkel) hacken of afluisteren een gevangenisstraf van ten hoogste een jaar of geldboete van € 19.000,- staat.
De straf kan worden verhoogd tot een gevangenisstraf van ten hoogste vier jaar als het hulpmiddel tot doel heeft om binnen te dringen in een computersysteem en vervolgens gegevens op te nemen of verder te hacken (als bedoeld in art.138ab, lid 2 of lid 3).

Het beschikken over en gebruiken van door afluisteren verkregen gegevens
Het voorhanden hebben en gebruiken van gegevens die door onrechtmatig afluisteren, aftappen en/of opnemen zijn verkregen is strafbaar gesteld in artikel 139e Sr.
Dit luidt:

Artikel 139e Sr

Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft:

1°. hij die de beschikking heeft over een voorwerp waarop, naar hij weet of redelijkerwijs moet vermoeden, gegevens zijn vastgelegd die door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk zijn verkregen;

16. Zoals bijvoorbeeld een netwerkadapter in promiscuous mode plaatsen.
17. TK 2000 - 2001, 23530, nr 45, p. 6.

Artikel 139e Sr *(vervolg)*

2°. hij die gegevens die hij door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht of andere gegevensverwerking door een geautomatiseerd werk heeft verkregen of die, naar hij weet of redelijkerwijs moet vermoeden, ten gevolge van zulk afluisteren, aftappen of opnemen te zijner kennis zijn gekomen, opzettelijk aan een ander bekend maakt;

3°. hij die een voorwerp als omschreven onder 1° opzettelijk ter beschikking stelt van een ander.

Hierbij zijn de volgende varianten strafbaar:
1. De beschikking hebben over voorwerpen waarop afgeluisterde, afgetapte en/of opgenomen gegevens zijn vastgelegd. Vereist is dat de dader weet, of redelijkerwijs moet vermoeden, dat de gegevens zijn verkregen door onbevoegd afluisteren, aftappen of opnemen.
2. Het opzettelijk bekendmaken aan een ander van gegevens die hij heeft verkregen door onrechtmatig afluisteren, aftappen of opnemen en het opzettelijk bekendmaken aan een ander van gegevens waarvan hij weet of zou moeten vermoeden dat deze door onrechtmatig afluisteren, aftappen of opnemen verkregen zijn.
3. Het opzettelijk ter beschikking stellen van het hierboven onder 1 genoemde voorwerp aan een ander.

Toelichting
Onder voorwerpen vallen alle gegevensdragers (media), zoals een usb-stick. Dit criterium geeft aan dat de wil van de dader erop gericht moet zijn, het voorwerp aan een ander te geven. Onder het begrip 'ter beschikking stellen' kan ook worden verstaan het aan een ander meedelen van de inhoud van het voorwerp.

Strafmaat
Het beschikken over en gebruiken van door het afluisteren, aftappen c.q. opnemen verkregen gegevens kan worden gestraft met een gevangenisstraf van ten hoogste zes maanden of een geldboete van € 19.000,-.

Schending van geheimhouding
Hoewel het geen cybercrime in enge zin betreft, wordt ook het schenden van een geheimhoudingsplicht beschreven. Het bekendmaken of misbruiken van gegevens die door een misdrijf zijn verkregen of waar men vanuit een arbeidsovereenkomst over beschikt, is mogelijk strafbaar onder artikel 273 Sr. Dit luidt:

Artikel 273 Sr

1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die opzettelijk
   1°. aangaande een onderneming van handel, nijverheid of dienstverlening bij welke hij werkzaam is of is geweest, bijzonderheden waarvan hem geheimhouding is opgelegd, bekend maakt of
   2°. gegevens die door misdrijf zijn verkregen uit een geautomatiseerd werk van een onderneming van handel, nijverheid of dienstverlening en die betrekking hebben op deze onderneming, bekend maakt of uit winstbejag gebruikt, indien deze gegevens ten tijde van de bekendmaking of het gebruik niet algemeen bekend waren en daaruit enig nadeel kan ontstaan.
2. Niet strafbaar is hij die te goeder trouw heeft kunnen aannemen dat het algemeen belang de bekendmaking vereiste.
3. Geen vervolging heeft plaats dan op klacht van het bestuur van de onderneming.

Het is *niet* strafbaar als iemand, die rechtmatig toegang heeft tot een computer en tot niet-openbare gegevens daarin, deze zonder toestemming overneemt. Bijvoorbeeld een medewerker van een bedrijf of instelling die opzettelijk persoonlijke gegevens van een bekende Nederlander kopieert met de bedoeling ze aan een ander te verkopen.[18]

Afluisteren door medewerker van een communicatiedienst
Beheerders van (interne) bedrijfsnetwerken en aanbieders van (openbare) telecommunicatiediensten hebben een geheimhoudingsplicht tegenover hun gebruikers en klanten. Schending van de geheimhouding door beheerders van besloten communicatienetwerken of medewerkers van een Internet Service Provider (ISP) is strafbaar gesteld in artikel 273d Sr. Dit luidt:

Artikel 273d Sr

1. Met gevangenisstraf van ten hoogste een jaar en zes maanden of geldboete van de vierde categorie wordt gestraft de persoon werkzaam bij een aanbieder van een openbaar telecommunicatienetwerk of een openbare telecommunicatiedienst:
   a. die opzettelijk en wederrechtelijk van gegevens kennisneemt die door tussenkomst van zodanig netwerk of zodanige dienst zijn opgeslagen, worden verwerkt of overgedragen en die niet voor hem zijn bestemd, zodanige gegevens voor zichzelf of een ander overneemt, aftapt of opneemt;

18. Als het conceptwetsvoorstel "Versterking bestrijding computercriminaliteit" wordt ingevoerd, wordt het opzettelijk en wederrechtelijk met een technisch hulpmiddel niet-openbare gegevens overnemen voor zichzelf of voor een ander, strafbaar (art. 139c lid 1 Sr).

Artikel 273d Sr ***(vervolg)***

b. die de beschikking heeft over een voorwerp waaraan, naar hij weet of redelijkerwijs moet vermoeden, een gegeven kan worden ontleend, dat door wederrechtelijk overnemen, aftappen of opnemen van zodanige gegevens is verkregen;
c. die opzettelijk en wederrechtelijk de inhoud van zodanige gegevens aan een ander bekendmaakt;
d. die opzettelijk en wederrechtelijk een voorwerp waaraan een gegeven omtrent de inhoud van zodanige gegevens kan worden ontleend, ter beschikking stelt van een ander.

2. Het eerste lid is van overeenkomstige toepassing op de persoon werkzaam bij een aanbieder van een niet-openbaar telecommunicatienetwerk of een niet-openbare telecommunicatiedienst.

In het eerste lid is gesteld dat het voor een medewerker van een telecombedrijf (inclusief ISPs) strafbaar is opzettelijk en wederrechtelijk kennis te nemen van de inhoud van communicatiegegevens (zoals gesprekken, e-mail, voicemail, chat, sms enz.) van klanten.

Lid 2 stelt bovendien dat dit ook geldt voor beheerders van niet-openbare communicatiediensten en computernetwerken, bijvoorbeeld een bedrijfsnetwerk.

Toelichting
Het inkijken, overnemen of doorgeven van de inhoud van communicatie van klanten door medewerkers bij een aanbieder van een communicatienetwerk of -dienst of beheerders van een bedrijfsnetwerk, is strafbaar. Dit geldt alleen als het wederrechtelijk gebeurt.

Als een (ISP) in zijn contract met klanten heeft opgenomen dat hij, onder strikte voorwaarden, de inhoud van communicatie kan inzien, is het bekijken van de communicatie niet wederrechtelijk. Bijvoorbeeld als de klant zoveel e-mails verstuurt dat het systeem instabiel wordt, of bij het toepassen van een geautomatiseerd spamfilter op inkomende e-mail.

Strafmaat
Het misbruik of de schending van de geheimhouding door een medewerker van een openbare telecommunicatiedienst of bijvoorbeeld een (netwerk- of systeem)beheerder van een besloten bedrijfsnetwerk, kan worden gestraft met een gevangenisstraf van ten hoogste anderhalf jaar of een geldboete van € 19.000,-

2.3 Cybercrime in ruime zin
Deze handleiding behandelt cybercrime in enge zin. Maar gewone criminaliteit met misbruik of gebruik van ICT-middelen komt misschien wel vaker voor. Vormen van cybercrime in enge zin kunnen dienen als voorbereiding op of uitvoering van een ander misdrijf. Inbreken op computersystemen is vaak niet een op zichzelf staand delict.

In deze handleiding wordt ter verduidelijking een aantal misdrijven beschreven, die met behulp van ICT-middelen kunnen worden gepleegd. Hiervoor is gebruik gemaakt van een onderzoek naar welke wetsartikelen door de politie in het verleden aan dossiers zijn gekoppeld (Leukfeldt E.R., 2010).

2.3.1 Oplichting en e-fraude
Cybercrime komt steeds vaker voor als middel om vermogensdelicten te plegen zoals oplichting, fraude, afpersing en verduistering.

Oplichting
Fraude staat niet als zodanig in het Wetboek van Strafrecht maar wordt meestal als oplichting (art. 326 Sr) en/of valsheid in geschrifte (art. 225 Sr) aangemerkt. In de digitale wereld komen vormen voor als oplichting via verkoopsites, handel in valse goederen, valse financiële transacties, veilingfraude en voorschotfraude.

Digitale oplichting zoals *phishing*, waarbij via een vervalste website of e-mail om persoonlijke gegevens wordt gevraagd, komt op grote schaal voor. Phishing is meestal strafbaar op basis van artikel 326 Sr.

Artikel 326 Sr

1. Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het verlenen van een dienst, tot het ter beschikking stellen van gegevens, tot het aangaan van een schuld of tot het teniet doen van een inschuld, wordt, als schuldig aan oplichting, gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
2. Indien het feit wordt gepleegd met het oogmerk om een terroristisch misdrijf voor te bereiden of gemakkelijk te maken, wordt de op het feit gestelde gevangenisstraf met een derde verhoogd.

Misbruik van telecommunicatie door bedrog
Misbruiken van een publieke telecommunicatiedienst met als oogmerk daarvoor niet volledig te betalen valt onder artikel 326c Sr. Dit luidt:

Artikel 326c Sr

1. Hij die, met het oogmerk daarvoor niet volledig te betalen, door een technische ingreep of met behulp van valse signalen, gebruik maakt van een dienst die via telecommunicatie aan het publiek wordt aangeboden, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
2. Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft hij die opzettelijk een voorwerp dat kennelijk is bestemd, of gegevens die kennelijk zijn bestemd, tot het plegen van het misdrijf, bedoeld in het eerste lid,
   a. openlijk ter verspreiding aanbiedt;
   b. ter verspreiding of met het oog op de invoer in Nederland voorhanden heeft of
   c. uit winstbejag vervaardigt of bewaart.
3. Hij die van het plegen van misdrijven als bedoeld in het tweede lid, zijn beroep maakt of het plegen van deze misdrijven als bedrijf uitoefent wordt gestraft hetzij met gevangenisstraf van ten hoogste vier jaren en geldboete van de vijfde categorie, hetzij met één van deze straffen.

Deze vorm van misbruik kan worden gestraft met een gevangenisstraf van ten hoogste vier jaren of een geldboete van € 76.000,-.

2.3.2 Diefstal en verduistering

Diefstal en diefstal onder verzwaarde omstandigheden zijn strafbaar onder respectievelijk artikelen 310, 311 of 312 Sr.

Artikel 310 Sr

Hij die enig goed dat geheel of ten dele aan een ander toebehoort wegneemt, met het oogmerk om het zich wederrechtelijk toe te eigenen, wordt, als schuldig aan diefstal, gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.

Verduistering, het opzettelijk enig goed dat aan een ander toebehoort en dat hij onder zich heeft wederrechtelijk toe-eigenen, is strafbaar onder artikelen 321, 322 of 323 Sr.

Artikel 321 Sr

Hij die opzettelijk enig goed dat geheel of ten dele aan een ander toebehoort en dat hij anders dan door misdrijf onder zich heeft, wederrechtelijk zich toeëigent, wordt, als schuldig aan verduistering, gestraft met gevangenisstraf van ten hoogste drie jaren of geldboete van de vijfde categorie.

Diefstal of verduistering is het wederrechtelijk wegnemen van een goed zodanig dat de rechtmatige eigenaar er niet meer over kan beschikken. Diefstal van gegevens is nu *niet* als zodanig strafbaar omdat de eigenaar de gegevens feitelijk niet kwijt raakt. Een wezenlijke eigenschap van een 'goed' is dat er niet meer over kan worden beschikt als een ander ermee vandoor gaat. Gegevens of informatie zijn *geen* goed. Als een persoon een computerbestand kopieert en doorsluist, raakt de eigenaar de gegevens niet kwijt: ze staan nog in de computer. Er is uiteraard wel sprake van diefstal als het fysieke medium waarop de gegevens staan opgeslagen, wordt ontvreemd.[19]

Toch kunnen virtuele objecten onder sommige omstandigheden als goederen gekwalificeerd worden. Bij twee zaken werd succesvol aangevoerd dat ook in de virtuele wereld goederen kunnen voorkomen omdat het om unieke zaken ging.
In de Habbo-hotel-[20] en RuneScape-uitspraken beriep de verdediging zich erop dat men slechts informatie ("eentjes en nulletjes") had gekopieerd, wat geen diefstal is. De uitspraak was revolutionair: voor het eerst werd geaccepteerd dat het in deze specifieke gevallen niet alleen ging om gegevens maar dat deze gegevens een uniek identificeerbare virtuele zaak vormden. Als men na het overnemen van gegevens vervolgens deze gegevens verwijdert, is er sprake vernieling van gegevens, wat een aparte handeling is onder artikel 350a Sr.[21]

Het is *niet* strafbaar om (onrechtmatig verkregen) computergegevens, bijvoorbeeld gegevens afkomstig van gecompromitteerde computers, wachtwoorden of toegangscodes van gebruikers, door te verkopen of te verhandelen (heling). Onder de huidige wetgeving is het wel verboden om een wachtwoord of andersoortige toegangsinformatie door te sluizen als je daarmee beoogt een misdrijf te plegen (zie voorbereidingshandelingen onder 2.2.3 en 2.2.4 bij artikelen 161sexies en 139d Sr). Personen die wederrechtelijk verkregen digitale informatie zonder een zodanig specifiek oogmerk doorsluizen aan een derde, zijn nu niet strafbaar omdat ook bij heling sprake moet zijn van een 'goed'.[22]

19. http://www.om.nl/onderwerpen/cybercrime/@153915/hirsch_ballin/
20. Habbo Hotel is een virtuele wereld waar tieners elkaar kunnen ontmoeten met zelf ontworpen karakters (zogenaamde Habbo's). Binnen de virtuele wereld vind je Openbare Ruimtes waar spelers met elkaar kunnen kletsen en Gastenkamers die gemaakt worden door de spelers. Bezoekers van Habbo Hotel kunnen hun Gastenkamer voorzien van meubels en kunnen bijvoorbeeld een huisdier adopteren.
    In november 2007 heeft het Korps Amsterdam-Amstelland een verdachte aangehouden voor diefstal van virtuele goederen uit het Habbo Hotel. De 17-jarige tiener uit Breda zou zich voor zo'n 4.000 euro aan virtuele meubels wederrechtelijk hebben toegeëigend.
21. Zie voor de complete uitspraken http://jure.nl/bh9789 en http://jure.nl/BK2773
22. Als het conceptwetsvoorstel 'Versterking bestrijding computercriminaliteit' wordt ingevoerd, wordt het beschikking hebben over niet-openbare gegevens waarvan redelijkerwijs moet worden vermoeden dat deze zijn verkregen door wederrechtelijk afluisteren, aftappen, opnemen of overnemen van een gesprek, gegevensoverdracht of gegevensverwerking door middel van telecommunicatie of een geautomatiseerd werk en het zodanige gegevens opzettelijk ter beschikking van een ander stellen of aan een ander bekend maken, strafbaar (art.139e Sr).

2.3.3 Afpersing

Afpersen is strafbaar als afpersing (art. 317 Sr), afdreiging (art. 318 Sr) en soms ook als bedreiging (art. 285 Sr). Verschijningsvormen zijn bijvoorbeeld dreigen met lamleggen van netwerken of websites (DDoS), beschadigen of verstoren van productiesystemen, vernietigen of ontoegankelijk maken van computergegevens, het openbaar maken van gevoelige informatie of het dreigen met smaad. Ook het afpersen of afdreigen van gegevens is strafbaar, zoals het onder dreiging van geweld iemand dwingen zijn pincode af te geven.

De artikelen 317 Sr, 318 Sr en 285 Sr luiden:

Artikel 317 Sr

1. Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, door geweld of bedreiging met geweld iemand dwingt hetzij tot de afgifte van enig goed dat geheel of ten dele aan deze of aan een derde toebehoort, hetzij tot het aangaan van een schuld of het teniet doen van een inschuld, hetzij tot het ter beschikking stellen van gegevens, wordt, als schuldig aan afpersing, gestraft met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie.
2. Met dezelfde straf wordt gestraft hij die de dwang, bedoeld in het eerste lid, uitoefent door de bedreiging dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, onbruikbaar of ontoegankelijk zullen worden gemaakt of zullen worden gewist.
3. De bepalingen van het tweede en derde lid van artikel 312 zijn op dit misdrijf van toepassing.

Artikel 318 Sr

1. Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, door bedreiging met smaad, smaadschrift of openbaring van een geheim iemand dwingt hetzij tot de afgifte van enig goed dat geheel of ten dele aan deze of aan een derde toebehoort, hetzij tot het aangaan van een schuld of het teniet doen van een inschuld, hetzij tot het ter beschikking stellen van gegevens, wordt als schuldig aan afdreiging, gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
2. Indien het feit wordt gepleegd met het oogmerk om een terroristisch misdrijf voor te bereiden of gemakkelijk te maken, wordt de op het feit gestelde gevangenisstraf met een derde verhoogd.
3. Dit misdrijf wordt niet vervolgd dan op klacht van hem tegen wie het gepleegd is.

Artikel 285 Sr

1. Bedreiging met openlijk in vereniging geweld plegen tegen personen of goederen, met geweld tegen een internationaal beschermd persoon of diens beschermde goederen, met enig misdrijf waardoor gevaar voor de algemene veiligheid van personen of goederen of gemeen gevaar voor de verlening van diensten ontstaat, met verkrachting, met feitelijke aanranding van de eerbaarheid, met enig misdrijf tegen het leven gericht, met gijzeling, met zware mishandeling of met brandstichting, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.
2. Indien deze bedreiging schriftelijk en onder een bepaalde voorwaarde geschiedt, wordt ze gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.
3. Bedreiging met een terroristisch misdrijf wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.
4. Indien het feit, omschreven in het eerste, tweede of derde lid, wordt gepleegd met het oogmerk om een terroristisch misdrijf voor te bereiden of gemakkelijk te maken, wordt de op het feit gestelde gevangenisstraf met een derde verhoogd.

2.3.4 Belediging en stalking

Smaad is strafbaar onder artikel 261 Sr, een eenvoudige belediging onder artikel 266 Sr en belediging aan het adres van bijzondere organen of functionarissen onder artikel 267 Sr.

Cyberstalking kan worden vervolgd als belaging (art. 285b Sr) of, afhankelijk van de situatie, worden gezien als een vorm van bedreiging (art. 285 Sr).

2.3.5 Discriminatie

De relatieve anonimiteit van het internet geeft ruimte aan het publiceren van haatzaaiende teksten en radicale en terroristische uitingen. In Nederland is de vrijheid van meningsuiting vastgelegd in artikel 7 van de Grondwet. Maar de wet stelt wel grenzen aan de vrijheid van meningsuiting. Beledigen van bevolkingsgroepen en het aanzetten tot discriminatie zijn niet toegestaan. Discriminatie in zijn algemeenheid is verboden op grond van artikel 1 van de Grondwet. Artikelen 137c tot en met 137e Sr stellen verschillende vormen van discriminatie strafbaar.

Artikel 137e van het Wetboek van Strafrecht stelt het openbaren van discriminerende uitingen strafbaar. In principe is de plaatser van een uiting op bijvoorbeeld een website zelf aansprakelijk. Onder omstandigheden kan de eigenaar van de website ook aansprakelijk worden gesteld. Onder artikel

137e is een website-eigenaar (mogelijk) medeverantwoordelijk voor de publicaties en reacties van de bezoekers van de website.

Als bezoekers berichten kunnen plaatsen op de website, bijvoorbeeld als reactie op een artikel, in een gastenboek of op een forum, komen hun uitingen via de website in de openbaarheid. Een website-eigenaar is zelf verantwoordelijk voor zijn website. Toezicht houden op geplaatste reacties is één manier waarmee een websitebeheerder de kans verkleint om aansprakelijk gesteld te worden voor andermans reacties. In elk geval is het van belang voor de beheerder om, zodra hij kennis krijgt van (onmiskenbaar) onrechtmatige inhoud, deze zo spoedig mogelijk te verwijderen, om aan aansprakelijkheid te ontkomen.

2.3.6 Identiteitsdiefstal

Identiteitsdiefstal is als zodanig niet expliciet strafbaar gesteld in Nederland. Meestal worden de identiteits- of toegangsgegevens wel verkregen via strafbare handelingen. Bovendien worden de verkregen identiteits- of toegangsgegevens vaak misbruikt bij diefstal of oplichting (art. 310, 326 Sr) of bij valsheid in geschrifte, opgave van onware gegevens en schending van de verplichting gegevens te verstrekken (art. 225 t/m 232 Sr). Het vervaardigen, ontvangen, aanschaffen, verkopen, overdragen of voorhanden hebben van stoffen, voorwerpen of gegevens bestemd tot het plegen van deze laatste misdrijven, kan ook strafbaar zijn (art. 234 Sr).

Identiteitsdiefstal wordt onder andere uitgevoerd voor het verkrijgen van toegang tot bankrekeningen van slachtoffers. Het opzettelijk vervalsen van een betaalpas of een andere drager van identiteitsgegevens, die bestemd is voor het verrichten of verkrijgen van betalingen of andere prestaties langs geautomatiseerde weg, is strafbaar onder artikel 232 Sr. Dit is mogelijk van toepassing bij *phishing* of *skimming*.

Artikel 232 Sr

1. Hij die opzettelijk een betaalpas, waardekaart, enige andere voor het publiek beschikbare kaart of een voor het publiek beschikbare drager van identiteitsgegevens, bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties langs geautomatiseerde weg, valselijk opmaakt of vervalst, met het oogmerk zichzelf of een ander te bevoordelen, wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.
2. Met dezelfde straf wordt gestraft hij die opzettelijk gebruik maakt van de valse of vervalste pas of kaart als ware deze echt en onvervalst, dan wel opzettelijk zodanige pas of kaart aflevert, voorhanden heeft, ontvangt, zich verschaft, vervoert, verkoopt of overdraagt, terwijl hij weet of redelijkerwijs moet vermoeden dat de pas of kaart bestemd is voor zodanig gebruik.

2.3.7 Piraterij

Cyber- of digitale piraterij is het illegaal kopiëren, verspreiden of aanbieden van auteursrechtelijk beschermde materialen. Vooral muziek, films, e-books en software zijn populair. In Nederland is het maken van een thuiskopie van muziek- of filmbestanden toegestaan onder de Auteurswet 1912. Men hoeft ook niet eigenaar te zijn van het origineel, dus een origineel exemplaar ervan te bezitten. Effectief betekent dit dat downloaden voor eigen gebruik van tekst, muziek of films veelal niet strafbaar is. Het verspreiden van auteursrechtelijk beschermde werken is dat wel. Het up- en downloaden van auteursrechtelijk beschermde software is in vrijwel de meeste gevallen wel strafbaar.

Verspreiding vindt met name plaats via *torrents*, *peer-to-peer-netwerken* of zogenoemde *usenet groups*. In torrents (via peer-to-peer-netwerken) wordt gelijktijdig een bestand binnengehaald en direct weer verspreid. Hierbij is sprake van up- en downloaden. Gebruik van usenetgroepen haalt bestanden van een centrale server binnen. Dan is er sprake van uitsluitend downloaden.

2.3.8 Kinderporno en grooming

De relatieve verborgenheid en anonimiteit van personen op het internet heeft geleid tot een internationaal ondergronds circuit van kinderpornografie in het cyberdomein. Misdrijven tegen de zeden zijn strafbaar onder de artikelen in Titel XIV in het Wetboek van Strafrecht. Kinderpornografie is strafbaar gesteld in artikel 240b Sr.

Ook het lokken van kinderen komt in de virtuele wereld voor. Hierbij worden door communicatie via de computer - meestal via het internet - kinderen benaderd om een ontmoeting te regelen om ontucht te plegen *(grooming)*. Dit is strafbaar onder artikel 248e Sr. Beide artikelen volgen hierna.

Artikel 240b Sr

1. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie wordt gestraft degene die een afbeelding - of een gegevensdrager, bevattende een afbeelding - van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrokken, verspreidt, aanbiedt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert, uitvoert, verwerft, in bezit heeft of zich door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst de toegang daartoe verschaft.
2. Met gevangenisstraf van ten hoogste acht jaren of geldboete van de vijfde categorie wordt gestraft degene die van het plegen van een van de misdrijven, omschreven in het eerste lid, een beroep of een gewoonte maakt.

Artikel 248e Sr

Hij die door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst een persoon van wie hij weet of redelijkerwijs moet vermoeden dat deze de leeftijd van zestien jaren nog niet heeft bereikt, een ontmoeting voorstelt met het oogmerk ontuchtige handelingen met die persoon te plegen of een afbeelding van een seksuele gedraging waarbij die persoon is betrokken, te vervaardigen wordt, indien hij enige handeling onderneemt gericht op het verwezenlijken van die ontmoeting, gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.

2.4 Telecommunicatiewet en -besluiten

Omdat het aanpakken van spam en misbruik via cookies met misbruik van computersystemen wordt geassocieerd, zijn hieronder enkele bepalingen uit de telecommunicatiewet opgenomen.

2.4.1 Spam

De waarborgen omtrent spam uit de Europese Richtlijn 2002/58/EG zijn omgezet naar artikel 11.7 van de Telecommunicatiewet.[23] Het spamverbod heeft betrekking op het versturen van spam *in of vanuit* Nederland.
Dit artikel luidt:

Artikel 11.7 Tw

1. Het gebruik van automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is uitsluitend toegestaan, mits de verzender kan aantonen dat de desbetreffende abonnee daarvoor voorafgaand toestemming heeft verleend, onverminderd hetgeen is bepaald in het tweede en derde lid.
2. Indien de abonnee, bedoeld in het eerste lid, een rechtspersoon is dan wel een natuurlijke persoon die handelt in de uitoefening van zijn beroep of bedrijf, geldt met betrekking tot het door middel van elektronische berichten overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden dat geen voorafgaande toestemming is vereist:
   a. indien de verzender bij het overbrengen van de communicatie gebruik maakt van elektronische contactgegevens die door de abonnee daarvoor zijn bestemd en bekendgemaakt, en deze zijn gebruikt in overeenstemming met de door de abonnee aan die contactgegevens verbonden doeleinden, of
   b. indien de abonnee is gevestigd buiten de Europese Economische Ruimte en voldaan is aan de in het desbetreffende land geldende voorschriften met betrekking tot het verzenden van ongevraagde communicatie.
3. Een ieder die elektronische contactgegevens voor elektronische berichten heeft verkregen in het kader van de verkoop van zijn product of dienst mag deze gegevens gebruiken voor het overbrengen van communicatie voor commerciële, ideële of charitatieve doeleinden met betrekking tot eigen gelijksoortige producten of diensten, mits bij de verkrijging van de contactgegevens aan de klant duidelijk en uitdrukkelijk de gelegenheid is geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens, en, indien de klant hiervan geen gebruik heeft gemaakt, hem bij elke overgebrachte communicatie de mogelijkheid wordt geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Artikel 41, tweede lid, van de Wet bescherming persoonsgegevens is van overeenkomstige toepassing.
4. Bij het gebruik van elektronische berichten voor de in het eerste lid genoemde doeleinden dienen te allen tijde de volgende gegevens te worden vermeld:

23. Staatsblad 2004, 308.

a. de werkelijke identiteit van degene namens wie de communicatie wordt overgebracht, en
b. een geldig postadres of nummer waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten.

5. Het gebruik van andere dan de in het eerste lid bedoelde middelen voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is toegestaan met inachtneming van het bepaalde in het zesde tot en met twaalfde lid, tenzij de abonnee op de in het zesde lid bedoelde wijze dan wel anderszins te kennen heeft gegeven dat hij de ongevraagde communicatie niet wenst te ontvangen.
6. Er is een register waarin de contactgegevens van de abonnee worden opgenomen die daarmee te kennen geeft dat hij ongevraagde communicatie als bedoeld in het vijfde lid niet wenst te ontvangen. De inschrijving in het register is voor onbepaalde tijd totdat de abonnee te kennen geeft dat zijn contactgegevens uit het register verwijderd kunnen worden. Het register wordt gehouden door een door Onze Minister aan te wijzen beheerder. De beheerder is verantwoordelijke als bedoeld in artikel 1, onder d, van de Wet bescherming persoonsgegevens.

Om te kunnen spreken van een overtreding van het spamverbod moet aan de volgende criteria worden voldaan:

1. Er wordt gebruikgemaakt van automatische oproepsystemen zonder menselijke tussenkomst, faxen of elektronische berichten.
2. Er is sprake van het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden.
3. De ongevraagde communicatie is gericht aan abonnees.
4. De abonnee heeft voorafgaand aan ontvangst van de ongevraagde communicatie geen toestemming verleend voor ontvangst.

Toelichting

Voor het versturen van spam is gekozen voor het zogenoemde ‘opt-in-regime’. Het opt-in-regime houdt in dat ongevraagde communicatie enkel en alleen mag worden verstuurd als de abonnee hieraan voorafgaande uitdrukkelijk zijn toestemming heeft verleend. De bewijslast voor de verkregen toestemming van de ontvanger ligt bij de verzender van de ongevraagde communicatie.

Het spamverbod geldt voor verzending van berichten aan een abonnee. Hieronder verstaat de wet een natuurlijk- of rechtspersoon die partij is in een overeenkomst met een aanbieder van openbare elektronische communicatiediensten voor de levering van dergelijke diensten.[24]
Het spamverbod geldt dus voor natuurlijke personen, bijvoorbeeld consumenten, maar ook voor zakelijke e-mailadressen.

Ongevraagde elektronische berichten zoals e-mail, sms, nieuwsbrief, fax en dergelijke mogen niet verstuurd worden aan bedrijven, tenzij een bedrijf expliciet heeft aangegeven dat het ongevraagde berichten wil ontvangen, bijvoorbeeld op diens website. Het is dus wel toegestaan spam te versturen aan een bedrijf wanneer deze zelf contactgegevens publiceert met als doel dergelijke e-mail te ontvangen.

Het spamverbod uit de Europese richtlijn geldt alleen voor Europese lidstaten. Grote delen van alle spam komt van buiten Europa, bijvoorbeeld uit de Verenigde Staten of Azië. In Nederland kan alleen worden opgetreden tegen personen of organisaties die spam versturen in of vanuit Nederland.

Er is een uitzondering waardoor het onder strikte voorwaarden wel mogelijk is om zonder voorafgaande toestemming commerciële e-mails te verzenden.
Deze voorwaarden zijn:

- de commerciële mail wordt gestuurd aan bestaande klanten;
- de commerciële mail heeft betrekking op *eigen gelijksoortige producten of diensten*;
- bij de verkrijging van de contactgegevens is aan de klant duidelijk en uitdrukkelijk de gelegenheid geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die contactgegevens;
- bij elke overgebrachte communicatie wordt de klant alsnog de mogelijkheid geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verdere gebruik van zijn elektronische contactgegevens.

Strafmaat

De handhaving van het spamverbod in Nederland is neergelegd bij de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA). Deze bevoegdheid is gebaseerd op artikel 15.1, derde lid, van de Telecommunicatiewet. Deze bestuursrechtelijke handhaving houdt in, dat de OPTA bij niet-naleving van artikel 11.7 van de Telecommunicatiewet bevoegd is een bestuurlijke boete van ten hoogste € 450.000,- op te leggen.[25] Ook kan de OPTA in geval van overtreding van artikel 11.7 van de Telecommunicatiewet kiezen zijn bevoegdheid te gebruiken om een last onder dwangsom op te leggen.[26]

24. Artikel 1.1 sub p Tw.
25. Vergelijk artikel 15.1, derde lid en artikel 15.2 , vierde lid Tw jo artikel 15.4 TW.
26. Vergelijk artikel 15.1, derde lid, Tw jo. artikel 15.2, tweede lid, Tw jo. artikel 5:32 van de Algemene wet bestuursrecht.

2.4.2 Cookies

In artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen zijn overeenkomstig de Europese Richtlijn privacy en elektronische communicatie voorwaarden gesteld voor het gebruik van zogenaamde cookies en soortgelijke software om persoonsgegevens en de persoonlijk levenssfeer te beschermen. Een cookie is een mechanisme voor een webserver om gegevens op te slaan op de harddisk van de computer. Dit artikel luidt:

Artikel 4.1

1. Een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een abonnee of gebruiker van openbare elektronische communicatiediensten dan wel gegevens wenst op te slaan in de randapparatuur van de abonnee of gebruiker van openbare elektronische communicatiediensten, dient voorafgaand aan de desbetreffende handeling de abonnee of gebruiker:
   a. op een duidelijke en nauwkeurige wijze te informeren omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en
   b. op voldoende kenbare wijze gelegenheid te bieden de desbetreffende handeling te weigeren.
2. Het bepaalde in het eerste lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel:
   a. de verzending van communicatie over een openbaar elektronisch communicatienetwerk uit te voeren of te vergemakkelijken, of
   b. de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is.

De wettelijke voorwaarden voor een dienstenaanbieder om een cookie in te zetten zijn:
- Voorafgaand aan de plaatsing wordt de abonnee op eenduidige wijze geïnformeerd over het doel van de cookie.
- De dienstenaanbieder geeft gelegenheid de werking van de cookie te weigeren.

Slechts voor de inzet van cookies voor de in het tweede lid geformuleerde doeleinden geldt de informatieplicht niet.

Toelichting

Cookies worden doorgaans voor legitieme doeleinden ingezet. Helaas worden cookies ook gebruikt voor nietlegale toepassingen en zonder medeweten van de computergebruiker. Het volgen van surfgedrag van een computergebruiker met behulp van cookies kan, als hierbij bijvoorbeeld persoonsgegevens worden vastgelegd, in strijd zijn met de Wet bescherming persoonsgegevens. Deze verbiedt het zonder voorafgaande toestemming of andere legitieme grondslag, en zonder voldoende doelbinding opslaan en verwerken van persoonsgegevens.

De invoering van de informatieplicht heeft de inzet van cookies met waarborgen omkleed. Cookies kunnen immers ook het gebruik van bepaalde diensten op het internet gebruiksvriendelijker maken. Een cookie kan het accepteren van algemene voorwaarden voor bepaalde dienstverlening eenvoudiger maken. Iedere keer als de gebruiker gebruikmaakt van deze dienstverlening, hoeft het proces van acceptatie niet opnieuw worden doorlopen. Pas wanneer de algemene voorwaarden voor de dienstverlening worden gewijzigd, moet de gebruiker de nieuwe voorwaarden accepteren.

Voor de dienstverleners op het internet verdient het aanbeveling om voor de inzet van cookies aan te sluiten bij het privacy-beleid op grond van de Wet bescherming persoonsgegevens. Men voldoet aan de informatieplicht door een privacy-statement op de website van de dienstverlener te plaatsen.
In dit privacy-statement moet staan:
- voor welke doeleinden persoonsgegevens worden verwerkt;
- welke persoonsgegevens worden verwerkt;
- wat de rechten van de betrokkenen zijn voor de gegevensverwerking, en
- waar de betrokkene zijn rechten kan uitoefenen.

Strafmaat

Het toezicht op de naleving van de voorwaarden voor het gebruik van cookies - zoals opgenomen in artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen - ligt bij de OPTA, zoals in artikel 15.1, derde lid, van de Telecommunicatiewet staat.
Deze bestuursrechtelijke handhaving betekent dat de OPTA bij niet-naleving bevoegd is een boete van ten hoogste € 450.000,- op te leggen. Ook mag de OPTA een last onder dwangsom opleggen.

HOOFDSTUK 3

Verschijningsvormen van cybercrime

Steeds vaker gebruiken aanvallers van elektronische communicatienetwerken combinaties van verschillende technieken. Onderstaande verschijningsvormen komen nog maar zelden in geïsoleerde vorm voor. Dit hoofdstuk gaat in op verschijningsvormen van cybercrime in enge zin, de technische aspecten en de strafbare gedragingen waaraan deze zijn toe te rekenen. Het gaat met name om verschijningsvormen van cybercrime op bedrijfssystemen of via een elektronisch communicatienetwerk, bijvoorbeeld het internet. Bij iedere verschijningsvorm wordt aandacht besteed aan:

- wat wordt er onder de verschijningsvorm verstaan;
- de technische verschijningsvorm en het herkennen ervan;
- de benodigde gegevens voor het vaststellen;
- strafbaarstelling.

Vanwege eventuele strafbaarstelling wordt vanuit technisch perspectief per verschijningsvorm aangegeven of er sprake is van bepaalde gedragingen. Daarna wordt per verschijningsvorm uitgelegd of deze ook strafbaar is op grond van bijvoorbeeld het Wetboek van Strafrecht of de Telecommunicatiewet. Daadwerkelijke strafbaarstelling hangt af van de concrete omstandigheden.

3.1 Malware

Malware is een verzamelnaam voor alle vormen van software met kwaadaardige bedoelingen, zoals computervirussen, wormen, Trojaanse paarden, spyware of *keyloggers*. Het onderscheid tussen de diverse vormen van malware vervaagt steeds meer. Deze handleiding maakt geen specifiek onderscheid meer tussen bijvoorbeeld computervirussen, wormen of Trojaanse paarden, maar geeft wel een korte omschrijving om de technische herkenbaarheid inzichtelijker te maken.

Wat is een virus?

Een virus is een kwaadaardige programmacode dat zichzelf toevoegt aan bestaande stukken programmacode; dit wordt *infecteren* genoemd. Er zijn zowel virussen als wormen in omloop die zichzelf aanpassen en veranderen om detectie te ontlopen. Deze worden *polymorphic* (in verschillende verschijningsvormen) genoemd.

Wat is een worm?

Meestal is een worm een stuk code dat zichzelf repliceert zonder of met minimale menselijke tussenkomst. Wormen zijn mogelijk alleen maar aanwezig en actief in het computergeheugen. Dit soort wormen bevindt zich dan dus alleen in het geheugen van een systeem *(memory-resident)* en zijn daardoor op bestandsniveau niet of moeilijk te herkennen. Een worm repliceert zich door gebruik te maken van kwetsbaarheden in computer- en netwerksystemen.

Virussen en wormen kwamen vroeger veel voor met het doel om de maker roem en naamsbekendheid te verschaffen onder computervandalen *(naming and faming)*. Computercriminaliteit is steeds geavanceerder geworden en heeft zich geprofessionaliseerd. Virussen en wormen dienen steeds vaker een breder doel of zijn onderdeel van een uitgebreidere aanval.

Een voorbeeld is zogenoemde *ransomware* waarbij computerbestanden van geïnfecteerde slachtoffers worden versleuteld en pas na betaling weer vrijgegeven. De malware versleutelt bekende bestandstypes. Het slachtoffer krijgt vervolgens een bericht met e-mailadres om de sleutel aan te vragen tegen betaling van een aanzienlijk geldbedrag.

Wat is een Trojaans paard?

Met de term *Trojan horse* (Trojaans paard) wordt een kwaadaardig programma bedoeld dat ongemerkt met een ander programma meekomt en dat onder valse voorwendselen (direct of indirect) op een computer wordt uitgevoerd.

Tegenwoordig wordt de term Trojaans paard - of simpelweg *trojan* - gebruikt als verzamelterm voor programma's die, van binnenuit, onopgemerkt op een computer actief zijn en die een kwaadwillende ongemerkt toegang geeft of (ongewenste) acties uitvoert. Denk hierbij aan het openen van netwerkpoorten of het onderscheppen van gegevens. Voorbeelden zijn zogenoemde *backdoors*, *bots*, *rootkits*, keyloggers of spyware. Trojaanse paarden zijn een vorm van malware.

Om Trojaanse paarden zo lang mogelijk onopgemerkt te laten blijven, worden ze steeds geavanceerder. Daarvoor worden verschillende technieken gebruikt, zoals het uitschakelen van beveiligingssoftware (*personal firewalls* of antivirussoftware) en het camoufleren van hun activiteiten.

Een trojan komt veelal mee met andere (illegaal verspreide) software. Daarnaast raken computers vaak geïnfecteerd omdat iemand een besmette e-mail opent. Maar ook een usb-stick kan besmet zijn of een bestand dat van een website wordt gedownload *(drive by download)*. Dit heet een *client-side attack*.

Een Trojaans paard kan ook worden gebruikt om virussen en wormen te verspreiden. Het belangrijkste verschil is, dat virussen en wormen zichzelf verspreiden naar slachtoffers *(push)* en Trojaanse paarden meestal door het slachtoffer worden binnengehaald *(pull)*.

Zo worden trojans verspreid:

- als *verborgen component* bij (legale) software die is aangeschaft of gedownload. Besmette populaire games of zogenoemde gratis antivirussoftware (fake antivirus), gedownload van het internet, zijn de bekendste voorbeelden.
- *geautomatiseerd* via kwetsbaarheden in software, veelal webbrowsers. Trojaanse paarden worden bijvoorbeeld geïnstalleerd vanaf een webpagina waarop mensen per ongeluk terechtkomen;
- als *component bij een virus of worm*, zodat deze, na het infecteren van de computer, ook een Trojaans paard installeert;
- via een *software-update*. Soms is een software-update dusdanig door een kwaadwillende gemanipuleerd dat deze een Trojaans paard bevat;
- via *e-mail*. Soms wordt op zeer grote schaal e-mail verspreid (spam) waaraan als bijlage een Trojaans paard hangt. Door de ontvanger over te halen de bijlage te installeren wordt het Trojaans paard verspreid;
- direct door een *hacker*. Deze installeert een Trojaans paard om het systeem te misbruiken en/of later makkelijker opnieuw te kunnen binnendringen.

Er zijn veel soorten Trojaanse paarden. Grofweg kan een onderscheid gemaakt worden tussen het ongewenst verzamelen van gegevens en het ongewenst toegang verlenen tot een systeem. Hieronder worden enkele soorten trojans uitgelegd.

Backdoor
De term backdoor wordt heel algemeen gebruikt voor (onderdelen van) software die buiten de normale methoden om toegang geeft tot een systeem. Een voorbeeld hiervan is een stuk programmacode dat door een programmeur in een programma is gestopt, zodat hij of zij zichzelf later toegang kan verschaffen tot de software of het systeem waar het op draait. Veel malware bevatten tegenwoordig een backdoor component, die een kwaadwillende op een later tijdstip toegang kan verschaffen tot de geïnfecteerde computer.

Rootkit
Een rootkit is een Trojaans paard dat zich, met volledige beheerderrechten, in een besturingssysteem heeft genesteld en essentiële onderdelen van het systeem vervangt. Alle rootkits hebben als overeenkomst dat ze verborgen willen blijven en dat ze actief willen zijn. Ze moeten dus geladen worden door het besturingssysteem. Het blijft echter moeilijk om de aanwezigheid van de rootkit vanaf het systeem zelf te detecteren, omdat sporen van de aanwezigheid door de vervangen onderdelen worden verborgen. Vooral rootkits die zich in het hart van het besturingsysteem (kernel) nestelen zijn moeilijk te detecteren. Veel rootkits bevatten een backdoor component.

Keylogger
Een keylogger is de benaming voor een specifiek soort software die maar één ding doet: het loggen van toetsaanslagen en eventueel muisklikken. De gelogde gegevens worden vaak automatisch verstuurd naar een derde partij. Een keylogger kan op zichzelf staan maar komt ook voor als onderdeel van een backdoor of een rootkit.

Spyware
Spyware is de benaming voor (onderdelen van) software die specifieke gegevens van een computer verzamelen, zoals bijvoorbeeld surfgedrag. Spyware wordt soms door de softwarefabrikant toegevoegd en soms door anderen aan bestaande software toegevoegd. In zeldzame gevallen wordt in licentievoorwaarden melding gemaakt van spyware-activiteiten, maar over het algemeen is dit niet het geval. Spyware 'verstopt' zich vaak niet echt en is redelijk gemakkelijk op te sporen.

Bot
De term bot wordt over het algemeen gebruikt voor malware met een backdoor component. Bots melden zich aan bij een centrale commandoserver ('Command & Control'-kanaal) waarna ze commando's kunnen ontvangen.[27] Zo worden computers waarop bots aanwezig zijn vaak gebruikt om gezamenlijk DDoS-aanvallen (Distributed Denial of Service) uit te voeren, maar kunnen ze ook worden ingezet als proxies die kunnen worden gebruikt voor het versturen van spam.

3.1.1 Technische verschijningsvormen en herkenbaarheid
Gezien de aard van malware is het moeilijk om definities te geven waaraan ze te herkennen zijn. Wel is de wijze waarop malware zich verspreidt een indicatie voor de technische herkenbaarheid.
Bekende malware wordt meestal door antivirusprogramma's herkend aan de hand van specifieke kenmerken *(signatures)* of aan het 'gedrag'. Malware gebruikt onder meer de volgende verspreidingsmechanismen (vectoren):

Verspreiding via het netwerk door kwetsbaarheden in software
Verspreiding (replicatie) via het netwerk gebeurt meestal zonder menselijke tussenkomst. Een worm kan worden geprogrammeerd zich op een andere computer te installeren en zich zo verder te verspreiden door misbruik te maken van bijvoorbeeld de zogenoemde *buffer overflow*.[28]

Een buffer overflow ontstaat alleen onder bepaalde omstandigheden. Malware die zich op zo'n agressieve manier verspreidt, genereert een toename in de netwerkbelasting. Daardoor kan de malware snel worden herkend. De malware is een worm als (de toename van) het netwerkverkeer uniformiteit vertoont. Dit treedt bijvoorbeeld op als de worm veelvuldig bepaalde data naar een bepaalde poort stuurt.

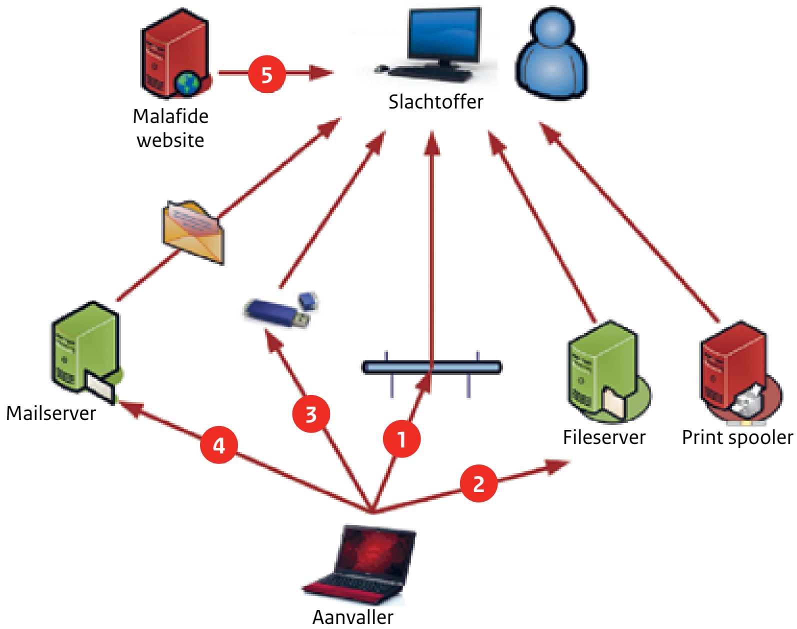
Verspreiding via netwerkshares of intern netwerk
Op het Windows-platform wordt veel gerepliceerd. Als een computer onjuist is geconfigureerd bijvoorbeeld geeft deze toegang met schrijfrechten aan onbevoegden. Verspreiding is in dit geval automatisch, maar activering van de malware op de computer gebeurt meestal nadat deze opnieuw gestart is. De malware kan referenties naar zichzelf wegschrijven om bij een herstart automatisch te activeren. In bijlage G staat een lijst van de voornaamste netwerkshares en opstartlocaties op verschillende platformen waar de malware gebruik van maakt.

Verspreiding via e-mail
Het Windows-platform is ook heel populair om geïnfecteerde e-mail te verspreiden. Het programmaatje verzamelt uit een aantal bronnen e-mailadressen, zoals uit het adresboek, mailfolders, lokale bestanden.[29] De meeste malware bevat algoritmes om de e-mail die ze versturen niet gemakkelijk automatisch te herkennen. Vaak zijn dan de onderwerpregel, de tekst zelf en de bijlage dynamisch aangepast. Deze replicatiemethode is eigenlijk alleen te herkennen aan de e-mails zelf en aan een verhoogde e-mailactiviteit.

27. Vaak werden IRC-kanalen gebruikt maar ook HTTP of bijvoorbeeld peer-to-peer-netwerken. Tegenwoordig zijn de C&C kanalen divers en moeilijker op te sporen.
28. Slammer d.m.v. SQL-server of Ramen d.m.v. wu-ftpd, rpc.statd en lpd
29. In zo'n geval ook wel een mailer of massa-mailer genoemd.

Malware verspreidingsvormen

1. Rechtstreeks via netwerk en (lokale) softwarekwetsbaarheden
2. Via (interne) netwerk file shares of (geïnfecteerde) print spoolers
3. Via infectie van bestanden
4. Via e-mail
5. Via malafide website



Verspreiding via infectie van andere bestanden
Malware kan zich ook verspreiden door infectie van andere bestanden, zij het met een vrij lage snelheid. De malware verspreidt zich bijvoorbeeld via besmette usb-sticks of (onbevoegd) aangesloten randapparatuur of laptops.
Malware kan virale code toevoegen aan andere programma's én in scripts of macro's.
Handmatig zijn deze veranderingen alleen goed te herkennen doordat bijvoorbeeld de grootte van een bestand is veranderd. Van oudsher scannen verreweg de meeste virusscanners bestanden op bepaalde kwetsbare punten en zoeken daar naar de aanwezigheid van kenmerkende code (signature).

Een klein aantal nieuwe virusscanners werken met het principe van vergelijking. Door gegevens over bestanden te vergelijken met een opgeslagen lijst gegevens, bijvoorbeeld *hash-waarden*, kan worden vastgesteld of een bestand is veranderd. De meest recente scanners gebruiken een vergelijking tussen computers onderling (Reputation-based malware detection). Bij deze nieuwe techniek is echter wel een (internet) netwerkverbinding nodig om de antivirus-software te gebruiken. Daardoor is deze techniek niet geschikt voor geïsoleerde netwerkomgevingen.

Het herkennen van Trojaanse paarden
Het herkennen van een Trojaans paard is meestal niet eenvoudig, omdat het tot doel heeft ongemerkt op een computer te verblijven. Een trojan kan worden ontdekt door:

- de aanwezigheid van onbekende processen die op de computer draaien;
- de aanwezigheid van onbekende (vreemde) bestanden op de computer;
- onverwachte open netwerkpoorten op de computer;
- onverwacht netwerkverkeer van en naar de computer;
- onverklaarbare systeem crash;
- afwijkende gedragingen, zoals onbekende vensters (pop-ups) en reclamemeldingen.

Trojans nestelen zich op zo'n manier in het besturingssysteem, dat ze automatisch zullen opstarten.
Een onderzoek moet dus gestart worden op de plekken waar programma's automatisch gestart worden.
Bijlage G bevat een lijst van de voornaamste opstartlocaties op verschillende platformen.

Als er sterke verdenking bestaat dat op een systeem een Trojaans paard aanwezig is, en inspectie vanaf het systeem zelf niets oplevert, dan kan dit het best worden onderzocht met tools waarvan de integriteit vaststaat. Dit zijn bijvoorbeeld read-only-media waarmee het systeem opgestart is, zoals een opstart-dvd met betrouwbare analysetools. Tools van het systeem zelf kunnen namelijk aangepast zijn door het Trojaanse paard, om ervoor te zorgen dat het onopgemerkt blijft.[30]

Rootkits kunnen worden ontdekt door een analyse van het systeem te maken op een hoog en een laag niveau.
Het hoge niveau houdt in dat vanuit het geïnstalleerde besturingssysteem naar de harde schijf wordt gekeken.
Voor het lage niveau wordt vanaf een opstart-dvd naar de harde schijf gekeken. Door de uitkomsten te vergelijken en

30. Een bekende en gratis beschikbare bootable dvd met audit en onderzoeksprogramma's is BackTrack (http://www.backtrack-linux.org/).

verschillen te zoeken, kunnen aanwijzingen worden gevonden of een rootkit aanwezig is.

Het besturingssysteem kan een lijst opleveren van alle bestanden op de lokale harde schijf *(directory listing)*. Deze lijst kan worden vergeleken met de informatie uit de *Master File Table* (MFT) die de daadwerkelijke bestandsindeling op de harde schijf bevat.[31]

Trojaanse paarden die zich bijvoorbeeld nestelen tussen het systeem van de gebruiker en de achterliggende dienst *(man-in-the-middle)* waarnaar de gegevens worden verzonden, zijn in staat om de gebruiker wijs te maken dat er niets aan de hand is. Deze trojans manipuleren wat de gebruiker te zien krijgt.

Zo'n Trojaans paard is bijvoorbeeld tot onderdeel van de webbrowser gemaakt en 'regelt' de communicatie van en naar een internetbank. De trojan laat bijvoorbeeld gemanipuleerde bedragen zien op het beeldscherm. De enige manier om vast te stellen of de getoonde informatie ook realiteit is, is door de gegevens te vergelijken met een papieren rekeningafschrift of contact met de bank op te nemen.[32]

3.1.2 Benodigde gegevens voor vaststelling

Voor het vaststellen van malware zoals een computervirus of Trojaans paard is informatie nodig waaruit blijkt dat er sprake is van een malware-besmetting. Een melding van het antivirusprogramma kan de eerste aanzet zijn. Ook kunnen afwijkende gedragingen van de computer een aanwijzing zijn, zoals onbekende meldingen in een firewall of IDS-logboek (Intrusion Detection System). Verder kan de computer zelf of de internetverbinding trager worden, er verschijnen zomaar foutmeldingen op het scherm of het besturingssysteem of applicaties lopen vaak vast.

De belangrijkste benodigde technische informatie is:
- een technische beschrijving van de getroffen systemen;
- een lijst van geïnstalleerde applicaties;
- een lijst van besmette of gewijzigde computerbestanden;
- een overzicht van de actieve processen in het computergeheugen;
- logbestanden;
- informatie over de aanwezige firewall en antivirusmaatregelen.

Voor het technisch onderzoek is het wenselijk om daarnaast ook de beschikking te hebben over een kopie van het computervirus of de bestanden die bij het Trojaans paard horen. Dit kan bijvoorbeeld door het isoleren van de besmette computerbestanden. De malware kan hiermee op een testsysteem worden geanalyseerd om het gedrag vast te leggen.

Voor de analyse kan een *image* van het schone systeem vóórdat dit werd geïnfecteerd waardevolle informatie geven, bijvoorbeeld door het te vergelijken met een image van het gecompromitteerde systeem.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen van infectie en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Mogelijk.
Er wordt binnengedrongen als er een programmacode, die oorspronkelijk niet op de computer stond, wordt ingebracht en uitgevoerd. Als de rechtmatige gebruiker echter (ongericht) besmet wordt met een computervirus of een Trojaans paard door het binnenhalen van een geïnfecteerd bestand, wordt dit niet direct gezien als binnendringen in een geautomatiseerd werk.
Dit is wél het geval zodra iemand de malware gebruikt om zonder toestemming van de rechtmatige eigenaar programmatuur aan te brengen of handelingen uit te voeren. Bijvoorbeeld als iemand op de computer iets doet als onderdeel van een botnet (zelfstandig opererende programmaatjes).

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.
Door het toedoen van een virus of andere malware kan in het geautomatiseerde werk stoornis worden veroorzaakt. De malware kan bijvoorbeeld (kritieke) bestanden verwijderen of onopgemerkt computerbestanden op een systeem aanpassen. Op het eerste gezicht functioneert het systeem normaal. Het verwijderen van de malware is waarschijnlijk alleen mogelijk door bepaalde of alle delen van de software opnieuw te installeren. Bovendien is het mogelijk dat andere programma's, die afhankelijk zijn van de originele, niet geïnfecteerde besturingssysteemcomponenten, niet meer correct functioneren. In dat geval is wél een stoornis veroorzaakt.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Mogelijk.
Door de malware worden er gegevens toegevoegd aan andere gegevens of toegevoegd aan het geautomatiseerd werk. Daarnaast kunnen opgeslagen gegevens zijn veranderd, gewijzigd of vernield. Dit hoeft echter niet. De meeste Trojaanse paarden zullen dit niet veroorzaken, omdat ze onopgemerkt willen blijven.

31. Ter vergelijking kan dezelfde informatie ook worden geverifieerd met een lijst, die men verkrijgt door het systeem op te starten vanaf een read-only medium, zoals een dvd.
Rootkits kunnen mogelijk ook worden ontdekt met hulpprogramma's zoals de Microsoft Rootkit-Revealer (http://technet.microsoft.com/en-us/sysinternals/bb897445.aspx).
32. Out-of-band verificatie.

Worden gegevens afgetapt of afgeluisterd? Mogelijk.
Dit geldt niet voor alle malware. Veel vormen van malware zullen gegevens die interessant zijn voor de kwaadwillende of nodig zijn voor de verdere verspreiding, proberen af te tappen en door te sturen. Vooral Trojaanse paarden zijn bedoeld om gegevens ongeautoriseerd te kopiëren, door te sturen en te misbruiken.

Strafbaarheid
Er is altijd sprake van strafbare gegevensaantasting (art. 350a lid 1 Sr), wanneer er onrechtmatig gegevens worden toegevoegd aan andere computergegevens. Alleen bij programma's (spyware) die in de licentieovereenkomst vermelden dat er gegevens worden verzameld, is het toevoegen van gegevens niet onrechtmatig.

Alle vormen van het opzettelijk en wederrechtelijk verspreiden van gegevens die bestemd zijn om schade aan te richten in een computer vallen onder artikel 350a lid 3 Sr. Volgens de wetgever vallen daar ook computervirussen, Trojaanse paarden en logische bommen (programma dat 'ontploft') onder.

Als er (opzettelijk of door schuld) stoornis in de gang of werking wordt veroorzaakt bij computers of netwerken met een publieke functie, waarbij tevens sprake is van een openbaar belang (stoornis in de uitvoering van een nutsdienst of openbaar telecommunicatienetwerk of -dienst), van gemeen gevaar voor goederen of diensten of levensgevaar, is dit strafbaar (artikel 161sexies en 161septies Sr).

Bij veel vormen van malware is sprake van het ongeautoriseerd binnendringen in het geautomatiseerde werk als gevolg waarvan strafbaarheid op grond van computervredebreuk kan bestaan (art.138ab Sr). Een uitzondering daarop is een Trojaans paard dat meelift met andere programmatuur en dus door de gebruiker zelf wordt geïnstalleerd. Echter als het Trojaanse paard vervolgens wordt gebruikt om wederrechtelijk handelingen uit te voeren in de computer of acties te laten verrichten (bij phishing of in een botnet), is er in ieder geval sprake van binnendringen in een geautomatiseerd werk volgens artikel 138ab lid 1 Sr.

Zodra de malware gegevens gaat verzamelen en doorsturen, is ook sprake van een strafbaar feit onder artikel 138ab, lid 2 Sr, het plegen van computervredebreuk en het vervolgens overnemen van gegevens. Mogelijk kan dit ook worden geschaard onder artikel 139c, eerste lid Sr, het aftappen en/of opnemen van gegevens.

Ransomware is een vorm van cybercrime in ruime zin en wordt strafbaar gesteld als een vorm van afpersing (art.317 Sr lid 2) of afdreiging (art.318 Sr lid 1).[33]

Op het openlijk ter beschikking stellen van programma's waarmee malware gemaakt kan worden, bijvoorbeeld op het internet, kunnen de strafrechtelijke bepalingen van toepassing zijn voor deelneming aan of strafbare voorbereiding van strafbare feiten (art. 48 en art.139d lid 2 Sr). Artikel 139d lid 2 stelt voorbereidingshandelingen zoals het vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen strafbaar.

3.2 Computerinbraak
Deze paragraaf behandelt verschillende vormen van *hacking*, lokaal en op afstand via een telecommunicatie- of computernetwerk inbreken en/of misbruik maken van computersystemen. In een aantal subparagrafen worden vervolgens technieken uitgelegd die gebruikt worden bij computerinbraken.

Wat is computerinbraak?
Computerinbraak of hacken is een verzamelterm voor het wederrechtelijk binnendringen in een computersysteem. Hierbij kan onderscheid worden gemaakt tussen ongerichte en gerichte cyberaanvallen *(targeted attacks)*.

Ongerichte cyberaanvallen zijn geautomatiseerd en hebben geen specifiek bedrijf of computersysteem als doelwit. Bij ongerichte aanvallen wordt grootschalig getest op het bestaan van kwetsbaarheden om vervolgens het computersysteem trachten te misbruiken, bijvoorbeeld door het installeren van malware.

Bij gerichte cyberaanvallen is een specifiek bedrijf of computersysteem het doelwit. De cyberaanval bestaat uit maatwerk om de kans van slagen en het risico op detectie te verkleinen. Voor gerichte cyberaanvallen is meestal meer kennis nodig en het vergt een langere voorbereidingstijd.

Drie vormen van computerinbraak
- *Fysieke inbraak*: Fysieke inbraak houdt in dat een hacker zich fysieke toegang verschaft tot een systeem. De hacker kan via een console toegang forceren of een onderdeel uit een systeem verwijderen (harddisk).
- *Lokale inbraak*: Lokale inbraak betekent dat een hacker gebruikersrechten heeft op een systeem. Via een exploit (serie commando's) of het afkijken van een wachtwoord kan een hacker zijn gebruikersrechten uitbreiden.
- *Inbraak op afstand*: Een hacker heeft bij deze vorm van inbraak geen gebruikersrechten op een systeem. Door één of meerdere exploits kan een hacker zichzelf toch toegang verschaffen tot een systeem.

33. Afdreiging: dwingen tot afgifte van een goed of aangaan van een schuld door bedreiging met smaad of openbaring van een geheim.

Cyberaanvallen
Cyberaanvallen kunnen plaatsvinden langs verschillende aanvalspaden, ook wel vectoren genoemd. Mogelijke aanvalspaden zijn:

- direct via het internet;
- via VPN (Virtual Private Network) aan het bedrijfsnetwerk gekoppelde thuiswerkplekken;
- via draadloze toegangspunten;
- met ongeautoriseerde apparatuur, zoals niet-toegestane laptops of usb-sticks;
- inbraak of insluiping en fysieke manipulatie van computersystemen;
- manipulatie van personen.

Cyberaanvallen kunnen bovendien plaatsvinden op diverse (technische) niveaus: de netwerklaag, de platformlaag en de applicatielaag.

- Op de *netwerklaag* kunnen gegevens worden afgeluisterd (*sniffen*) of informatie worden verzameld (*enumeration*), bijvoorbeeld door het scannen van computersystemen (*poortscan* of *portscan*).
- Op de *platformlaag* zijn de aanvallen gericht op het misbruik maken van bekende en nieuwe kwetsbaarheden in besturingssystemen (*exploits*). Maar ook aanvallen op de hardware en de daarin ingebouwde programmacode (*firmware*) komen voor.
- Op de *applicatielaag* kan misbruik worden gemaakt van fouten, die gemaakt zijn door de ontwikkelaars, in het ontwerp zitten of in de configuratie, of het gevolg zijn van implementatie van een (web)applicatie.

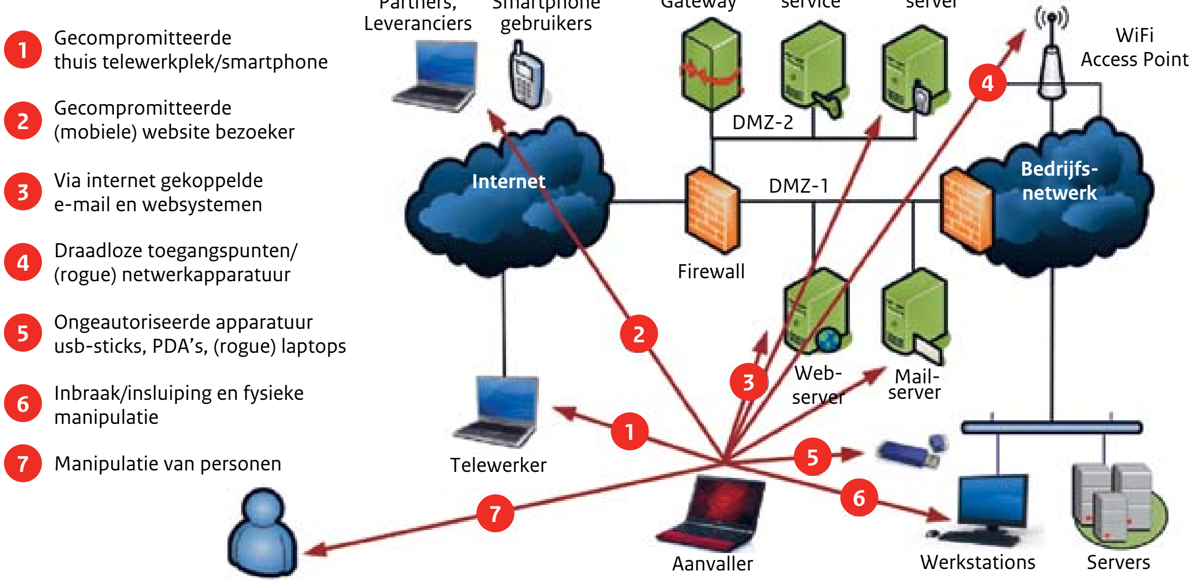
Een hacker kan van softwarematige fouten of kwetsbaarheden in het systeem gebruikmaken om toegang te krijgen tot een systeem voor een lokale inbraak of voor inbraak op afstand. Voorbeelden van veelvoorkomende kwetsbaarheden zijn:

Buffer overflow
Veel kwetsbaarheden zijn gebaseerd op een buffer overflow. Een *buffer* is een reeks gereserveerde geheugenblokken, die gebruikt wordt voor het vasthouden van data. De grootte van deze buffer is op voorhand gedefinieerd. Een buffer overflow ontstaat op het moment dat er meer informatie naar een buffer wordt geschreven dan de buffer toelaat. Hierdoor wordt de grens van de buffer overschreden, met als gevolg dat programmacode kan worden geïnjecteerd. Een hacker kan hiermee applicaties laten crashen of bepaalde acties laten uitvoeren om zich zo toegang tot het systeem verschaffen.

Code-injectie
Op computersystemen zijn vaak verschillende programma's tegelijkertijd actief. Door een commando of gegevensinvoer kan men gevolgen laten optreden in andere actieve programma's. Er worden dus vanuit de ene applicatie aan een andere gegevens toegevoegd. Die andere applicatie kan worden geïnstrueerd heimelijke opdrachten uit te voeren.

Een voorbeeld van code-injectie is wanneer een bepaalde tekststring via een webapplicatie wordt ingevoerd, deze aan te vullen met andere tekststring. Bijvoorbeeld de string om wachtwoordgegevens te versturen: '| mail user < /etc/passwd' zijn. Via de webapplicatie krijgt het besturingssysteem opdracht om de output van het wachtwoordenbestand '/etc/passwd' te mailen. Met de wachtwoorden krijgt een hacker toegang tot het systeem.

Aanvalsvectoren



Een soortgelijke techniek wordt ook toegepast bij zogenoemde *SQL-injection (Structured Query Language)*, waarbij door listig misbruik van een niet goed geprogrammeerde applicatie direct commando's aan de database zelf gegeven kunnen worden.

Configuratiefouten
Door configuratiefouten kunnen kwetsbaarheden ontstaan of worden standaardconfiguraties gebruikt die niet afdoende zijn afgeschermd. Eén zo'n kwetsbaarheid is bijvoorbeeld het gebruik van standaardwachtwoorden. Ook kan een kwaadwillende zo misbruik maken van onnodig draaiende services op een systeem.

Zwakke wachtwoorden
Meestal zijn wachtwoorden de belangrijkste afscherming voor geautoriseerde toegang tot computersystemen en informatie. Mensen hebben de neiging om eenvoudig te onthouden wachtwoorden te kiezen. Bijvoorbeeld bestaande woorden waarin letters door een cijfer worden vervangen, of wachtwoorden afgeleid van persoonlijke interesses of omstandigheden (familienamen, data, postcodes, autonamen, huisdieren en dergelijke).
Aanvallers proberen met geautomatiseerde hulpstukken informatie over een persoon te verzamelen, om de wachtwoorden te raden door verschillende combinaties te testen.

Onbeveiligde data en netwerkprotocollen
Veel netwerkprotocollen en -structuren zijn niet ontwikkeld met de visie op informatiebeveiliging zoals wie die nu kennen. Deze netwerkinrichtingen bevatten daarom de nodige intrinsieke kwetsbaarheden. Ethernet is het meest gebruikte netwerkprotocol. Het is een zogenoemd *shared medium*: het computernetwerk wordt gedeeld met meerdere systemen. Via een *sniffer* kan via ethernet onbeveiligde data worden onderschept of 'afgeluisterd'. Ook WiFi-netwerken en communicatieprotocollen zoals telnet, FTP (File Transfer Protocol) en SMTP (Simple Mail Transfer Protocol) zijn gevoelig voor het achterhalen van onbeveiligde gegevens en privacygevoelige informatie door hackers.

Zero-day
Een zero-day-aanval misbruikt een nog onbekende of niet gemelde zwakke plek in een computerprogramma. Zero-day-kwetsbaarheden zijn nog niet bekend bij de software-ontwikkelaar of er is nog geen oplossing *(patch)* beschikbaar om het gat te dichten. Zero-day-exploits worden gebruikt of gedeeld door hackers voordat de softwareontwikkelaar weet heeft van de kwetsbaarheid.

Fysieke computerinbraak
Bij een fysieke computerinbraak kan de beveiliging op het lokale besturingssysteem worden omzeild door het systeem te starten vanaf een ander medium, zoals een opstart-cd-rom of *bootable disk*.[34] Alle toegangs- en beveiligingsmaatregelen op die computer zijn dan waardeloos. Alleen een volledig versleutelde harde schijf (encryptie harddisk) kan bescherming bieden, mits het systeem volledig is uitgeschakeld tijdens de aanval.

Wordt de computer fysiek benaderd terwijl deze in bedrijf is, dan zal harddiskversleuteling niet helpen; het besturingssysteem en/of de hardware kan worden gecompromitteerd. Voor deze aanvalstechniek worden bijvoorbeeld usb-sticks, cd-roms of dvd's gebruikt, die via *autorun* (automatisch starten van een proces) worden gestart. Ook kan men de *firewire*-aansluiting hiervoor gebruiken.

Een andere vorm van fysieke computerinbraak is het plaatsen van een fysieke keylogger. Deze wordt geplaatst tussen het toetsenbord en de computer. Het zijn meestal kleine usb-stekkers waar de toetsenbordkabel op wordt aangesloten. De keylogger legt alle toetsaanslagen vast, ook wachtwoorden.
Keyloggers moeten door de kwaadwillende weer worden opgehaald om de gegevens eraf te halen. Sommige keyloggers zijn in staat om via e-mail of een andere netwerkverbinding de gegevens te versturen.

De meest simpele vorm van fysieke inbraak is wanneer een kwaadwillende direct toegang verkrijgt omdat een computer onbeheerd en niet vergrendeld is achtergelaten. Onbeheerd achterlaten lokt ook nieuwsgierigen en gelegenheidscriminelen.
Een kwaadwillende kan eenvoudig toegang verkrijgen tot gevoelige informatie, gegevens wijzigen of toevoegen, of e-mail versturen onder de gebruikersnaam van de nog aangemelde gebruiker.
Feitelijk is dit ook een vorm van lokale computerinbraak. Computervredebreuk zal in dit geval moeilijk te bewijzen zijn (art. 138ab Sr). Maar het wederrechtelijk wijzigen of vernietigen van gegevens blijft natuurlijk strafbaar.

Lokale computerinbraak
Bij lokale computerinbraak heeft de aanvaller al (geautoriseerde en legale) toegang. De aanvaller verschaft zich ongeautoriseerd toegang tot delen van het systeem door het omzeilen van beveiligingsmaatregelen, misbruiken van een gebruikersnaam en wachtwoord of door het inzetten van exploits gericht op de zwakke plekken. De aanvaller eigent zich bijvoorbeeld hogere gebruikersrechten toe dan waarvoor hij geautoriseerd is (elevatie van toegangsrechten). Dergelijke aanvallen kunnen worden uitgevoerd door het eigen personeel, tijdelijke medewerkers of bezoekers met fysieke toegang tot de systemen.

34. Ook andere opstart media zijn mogelijk, zoals via dvd, usb-stick of netwerk. Bootable disks met kant en klare 'crack'-software voor met name Windows-platformen, waarmee direct op de lokale harde schijf kan worden gelezen en geschreven, zijn vrij verkrijgbaar op het internet.

Het ontdekken van 'insiders' is lastig, omdat het gedrag in grote lijnen overeenkomt met normaal computergebruik. Bovendien zullen netwerk-IDS-oplossingen deze aanvallen in het geheel niet signaleren, omdat de aanvaller lokaal werkt. Een lokale (personal) firewall, antivirusscanner en een host-based-IDS kunnen dit gedrag meestal wel detecteren en registeren.

Niet zelden blijken gefrustreerde (ex-)medewerkers de boosdoener te zijn. Zij kopiëren bijvoorbeeld gevoelige informatie, versturen spam of beledigende e-mailberichten, passen wachtwoorden aan of openen achterdeuren in het systeem via Trojaanse paarden of verborgen WiFi-apparatuur. Een lokale computerinbraak zet daarmee de achterdeur wijd open naar het bedrijfsnetwerk.

Computerinbraak op afstand

Bij een computerinbraak op afstand probeert de aanvaller toegang te krijgen via een (draadloze) netwerkverbinding. Een aanval bestaat doorgaans uit een verkennende en een aanvallende fase.

In de *verkennende fase* worden systemen die via een netwerk als het internet benaderbaar zijn, afgetast op netwerkpoorten en daaraan gekoppelde actieve services. Zo kan een aanvaller bijvoorbeeld ontdekken dat een webserver actief is. Door kwetsbaarheden (exploits) of zwakke systeemconfiguraties (standaardwachtwoorden) te misbruiken, krijgt een aanvaller toegang tot de webserver.

Meestal hangt een webserver niet direct aan een bedrijfsnetwerk, maar is bijvoorbeeld in een bufferzone geplaatst. Dit noemt men een DMZ-netwerk *(demilitarized zone)*. Soms zijn er meerdere DMZ-netwerken aanwezig.

Servers aangesloten op een DMZ-netwerk hebben geautoriseerde verbindingen naar interne systemen nodig, zoals naar database- of mailservers. Door de eerder gecompromitteerde webserver als springplank te gebruiken kan een aanvaller zich verder toegang verschaffen tot het interne bedrijfsnetwerk.

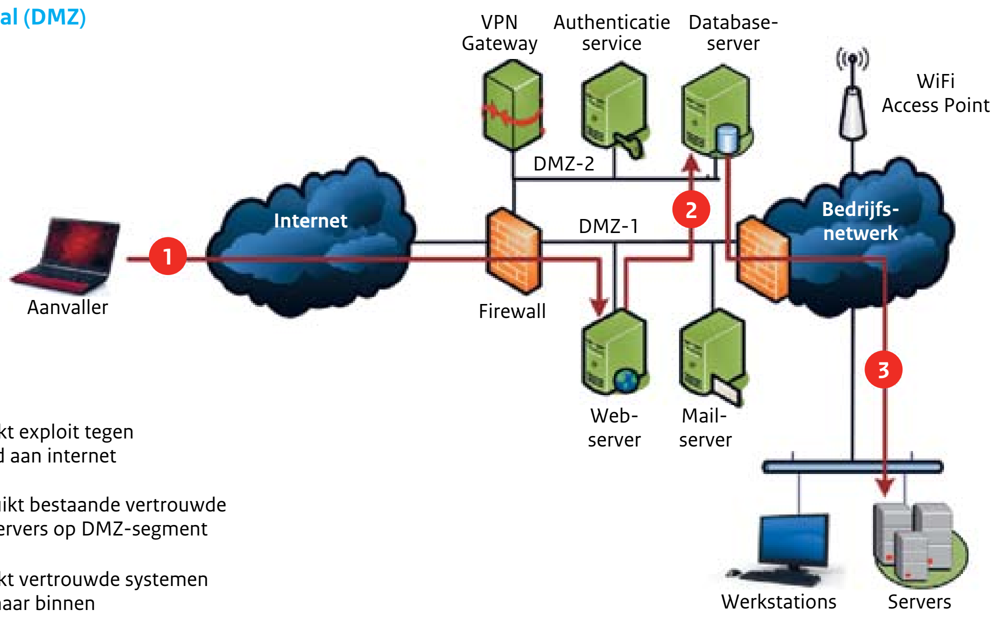
Veel organisaties bieden hun medewerkers voorzieningen voor telewerken. De verbinding tussen het werkstation of laptop van de gebruiker en het bedrijfsnetwerk wordt versleuteld om de veiligheid van de gegevens die via het internet heen en weer gaan, te waarborgen. Dit heet een Virtual Private Network (VPN).

Gebruikers worden vaak niet alleen herkend via hun gebruikersnaam en wachtwoord, maar ook omdat ze een *token* gebruiken *(2-factor authenticatie)*.
Een token kan voor iedere keer dat verbinding wordt gemaakt een éénmalige toegangscode genereren.
Ook kunnen smartcards als token worden gebruikt.

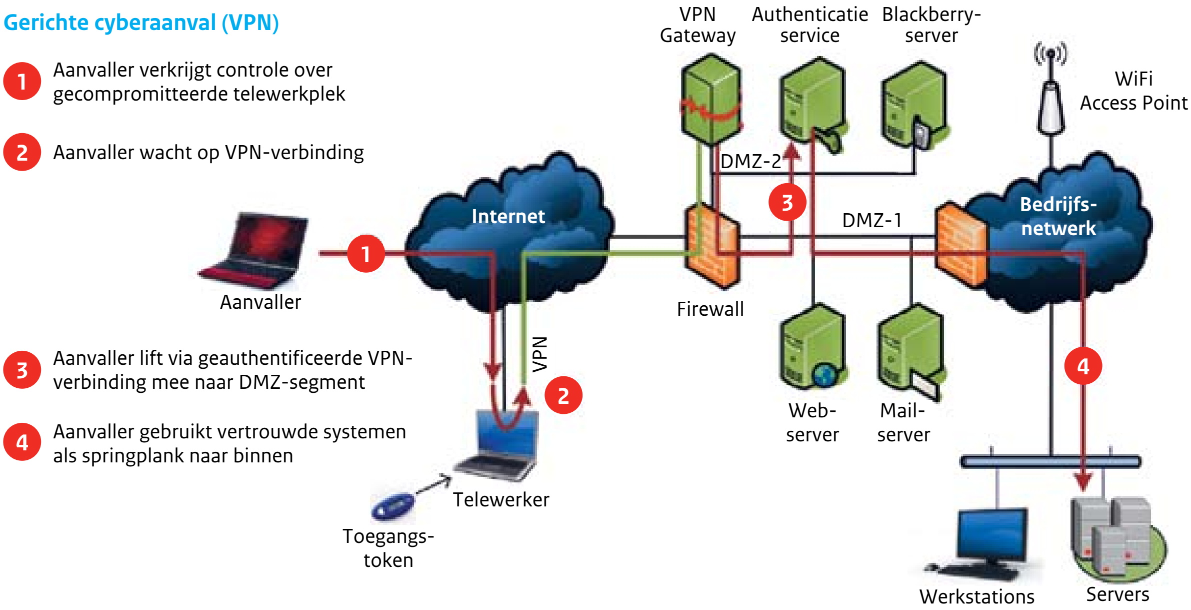
VPN-verbindingen sluiten niet uit dat een aanvaller niet binnen kan dringen.
Als eerste stap kan de aanvaller proberen de werkplek van de gebruiker te compromitteren. Omdat de gebruikerswerkplek vaak buiten de directe invloed van de systeembeheerder staat, is het niet zeker dat deze voldoende is beveiligd. Werkstations van gebruikers worden regelmatig gebruikt voor privédoeleinden. Hierdoor vergroot de kans op besmetting met malware.

Een aanvaller hoeft in dat geval alleen maar te wachten tot de werkplek via VPN verbinding maakt. De aanvaller lift op deze verbinding mee naar binnen en vervolgens naar de

Gerichte cyberaanval (DMZ)



1. Aanvaller gebruikt exploit tegen server gekoppeld aan internet
2. Aanvaller misbruikt bestaande vertrouwde koppeling met servers op DMZ-segment
3. Aanvaller gebruikt vertrouwde systemen als springplank naar binnen



bedrijfssystemen. Firewalls en IDS-oplossingen kunnen dit niet of moeilijk detecteren, omdat de VPN-verbinding vanaf een toegestane werkplek en geauthentiseerde gebruiker afkomstig is. Vanuit het perspectief van het VPN-systeem is het namelijk een legitieme verbinding.

Ook *access points*, draadloze toegangspunten, kunnen bij onvoldoende beveiliging kwetsbaar zijn. Verder vormen de draadloze mogelijkheden op laptops, PDA's en andere apparaten die (tijdelijk) zijn aangesloten op het bedrijfsnetwerk ook kwetsbaarheden voor ongeautoriseerde toegang.

Technische verschijningsvormen en herkenbaarheid
Veel (gerichte) cyberaanvallen worden voorafgegaan door voorbereidingen en technische verkenningen van het doelwit. Via dit vooronderzoek verzamelt de aanvaller zoveel mogelijk gegevens over een systeem.
Daarvoor hoeft de hacker soms niet eens contact te maken met het doelsysteem. Via informatiebronnen als een *routing registry*, zoekmachines en DNS (Dynamic Name Service) kan de hacker de benodigde gegevens verzamelen. Wordt er gebruikgemaakt van publiekelijk beschikbare informatie, dan is het moeilijk de aanvaller te traceren.

Kwaadwillenden kunnen de volgende technieken toepassen:

Footprinting
Bij *footprinting* wordt een systeem rechtstreeks onderzocht om te kijken welke softwareversies actief zijn. Soms kan footprinting worden gedetecteerd. Op deze wijze gegevens achterhalen wordt *enumeration* genoemd.

Via footprinting probeert de aanvaller te achterhalen:
- IP (Internet Protocol)-adres(sen)van het systeem;
- locatie van het systeem;
- hostname van het systeem in de DNS;
- softwareversie van besturingssysteem en van applicaties;
- proceseigenaren van bepaalde applicaties;
- directorystructuur van een systeem;
- lijst van gebruikersaccounts;
- lijst van actieve services.

Op oudere Windows-platformen kan informatie worden verkregen via zogenaamde *nulsessies*. Dit zijn verbindingen waarvoor geen gebruikersnaam en wachtwoord nodig zijn. Een Windows-computer kan als het ware worden bevraagd om bepaalde gegevens te geven. Dit is nodig om een Windows-platform in bijvoorbeeld een bedrijfsnetwerk te laten functioneren. In nieuwere versies is dit aangepast.[35]

Veel netwerkapparatuur zoals routers, printers en servers ondersteunen ook het Simple Network Management Protocol (SNMP). Hoewel dit protocol in de latere versies is voorzien van beveiligingsopties, komen er nog veel installaties voor waarbij deze niet zijn toegepast. Footprinting kan dan eenvoudig worden uitgevoerd door een aanvaller *(SNMP walking)*.[36]

Netwerkanalyse
Een aanvaller kan technieken als sniffing (afluisteren van netwerkverkeer), *portscanning* of *netwerk-mapping*-methodieken hanteren om de topologie van een netwerk te bepalen en om informatie over een systeem in te winnen.

Sniffing is mogelijk zodra de aanvaller toegang heeft tot het netwerk via de fysieke netwerkbekabeling of door een gecompromitteerde netwerkrouter of werkstation te

35. Een nulsessie kan worden getest met bijvoorbeeld het commando net use \\ipaddress "" /user:""
36. SNMP werkt standaard over netwerkpoort 161 en heeft als instelling 'public'. Met (gratis) SNMP-browsers kan veel informatie van een systeem zo worden opgevraagd.

gebruiken. Door het netwerkverkeer af te luisteren krijgt de aanvaller informatie over de aangesloten systemen.
Is het netwerkverkeer onversleuteld, zoals op vrijwel alle interne bedrijfsnetwerken, dan kan een aanvaller ook wachtwoorden van onbeveiligde netwerkprotocollen onderscheppen.
De aanvaller van buitenaf moet eerst inbreken op het systeem om netwerkverkeer te sniffen. Een insider daarentegen kan meteen sniffen.

Met portscanning, DNS-bevraging of netwerk-mapping *(traceroutes)* vormt de aanvaller zich een beeld van de netwerktopologie. Welke systemen bevinden zich waar in het netwerk? Welke functies hebben ze en welke services draaien er op?

Benodigde gegevens voor vaststelling

Voor het vaststellen van een gerichte cyberaanval is veel deskundigheid nodig.
De aanvaller zal zijn acties heimelijk en waarschijnlijk gespreid over een langere periode uitvoeren. Alle afwijkende 'gedragingen' van een computer kunnen een aanwijzing zijn, zoals onbekende meldingen in een firewall of IDS-log, trager wordende prestaties of langzame internetverbinding, foutmeldingen of veelvuldig vastlopende computers of applicaties.

De belangrijkste benodigde technische gegevens zijn:

- een overzicht van de gedane constateringen en het tijdstip waaruit blijkt, of op basis waarvan wordt vermoed, dat er sprake is van een cyberincident;
- een technische beschrijving van de systemen;
- een lijst van geïnstalleerde programmatuur;
- een lijst van gewijzigde computerbestanden;
- een overzicht van actieve processen in het computergeheugen;
- logbestanden;
- informatie over het netwerk, firewalls en andere beveiligingsmaatregelen.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Mogelijk.

Er is sprake van binnendringen als een hacker bepaalde gebruikersrechten op onrechtmatige wijze heeft verkregen. Het maakt niet uit of daarvoor wordt binnengedrongen via het computernetwerk of door het lokaal manipuleren van de computer.
Zo is het fysiek aansluiten van illegale randapparatuur aan bijvoorbeeld de firewire-aansluiting of het plaatsen van een dvd met malware die instructies stuurt naar de computer, een vorm van het aanbieden van een vals signaal.

Heeft een gebruiker onder normale omstandigheden legitiem toegang heeft tot (delen van) het geautomatiseerd werk, dan is er ook sprake van binnendringen als gebruikersrechten op onrechtmatige wijze worden verkregen.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.

Meestal blijft het systeem in eerste instantie normaal functioneren. Kijkt een aanvaller na binnendringing alleen rond, dan hoeft dit niet meteen een stoornis te veroorzaken. Wanneer echter de functionaliteit of gegevens zijn aangetast, is er wel sprake van een stoornis.
Kan het systeem vervolgens alleen worden hersteld door malware te verwijderen en (del van) software opnieuw te installeren, dan is er ook een stoornis veroorzaakt.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Mogelijk.

Bij alle vormen van inbraak (fysiek, lokaal of op afstand) kan het voorkomen dat gegevens veranderd, gewijzigd of vernield worden. Daarnaast zijn misschien malware of rootkits geïnstalleerd. Niet alle hackers zullen dit doen, omdat zij onopgemerkt willen blijven.

Worden gegevens afgetapt of afgeluisterd? Mogelijk.

Een kwaadwillende heeft zich in dat geval (fysiek, lokaal of op afstand) toegang verschaft, het beheer van het systeem overgenomen of malware geplaatst om toekomstige communicatie vanaf de computer te onderscheppen.
Dit komt bij veel vormen van computerinbraak voor.

Strafbaarheid

Bij computerinbraak heeft iemand de bedoeling zonder toestemming van de eigenaar in een geautomatiseerd werk binnen te dringen. Dit is strafbaar gesteld in artikel 138ab lid 1 Sr.

Het kan zijn dat de dader nog andere handelingen verricht, zoals het overnemen en voor zichzelf of een ander vastleggen van gegevens. In dat geval is tevens sprake van een misdrijf op grond van artikel 138ab lid 2 Sr.

Gebeurt de cyberinbraak via openbare telecommunicatienetwerken en de dader hackt door, dan is er sprake van strafbaarheid op grond van artikel 138ab lid 3 Sr.

Het is ook mogelijk dat, nadat is binnengedrongen, opzettelijk gegevens worden vernield. Deze situatie is, als de vernieling ernstige schade oplevert, expliciet strafbaar gesteld in artikel 350a lid 2 Sr.

Als iemand na binnendringing een technisch hulpmiddel aanbrengt zodat hij gegevens af kan tappen en/of op kan nemen van het telecommunicatienetwerk, dan kan iemand ook strafbaar zijn op grond van het aftappen en/of opnemen van gegevens (artikel 139c lid 1 en 139d Sr).

Wanneer door aftappen wederrechtelijk verkregen gegevens worden opgeslagen op een voorwerp zodanig dat de aanvaller erover kan beschikken en deze voorhanden heeft, zoals een usb-stick, dan is dit strafbaar onder artikel 139e lid 1 Sr. Als dergelijke gegevens opzettelijk aan een ander bekend worden gemaakt, dan is dat strafbaar onder artikel 139e lid 2 Sr.

Als gevolg van de computerinbraak en het handelen van de hacker, kan *opzettelijk* dan wel door *schuld* een geautomatiseerd werk worden vernield. In dat geval kan aanvullend strafbaarheid op grond van de artikelen 161sexies en 161septies Sr bestaan als er sprake is van een openbaar belang (stoornis in de uitvoering van een nutsdienst, een openbaar telecommunicatienetwerk of telecommunicatiedienst), van gemeen gevaar voor goederen of levensgevaar.

3.2.1 Portscan

Wat is een portscan?

Een *portscan* is een techniek waarbij datapakketten over het netwerk naar een computersysteem worden verstuurd om te achterhalen welke netwerkpoorten en -services actief zijn. Daarbij wordt informatie over soort en versie van het besturingssysteem en services verkregen. Een portscan kan ook het voorwerk voor een inbraakpoging zijn.
De term *stealth scan* wordt soms gebruikt voor portscans die niet of moeilijk te detecteren zijn. De term is enigszins misleidend omdat naar aanleiding van nieuwe stealth-scantechnieken ook methodes worden ontwikkeld om deze te detecteren.

Technische verschijningsvormen en herkenbaarheid

Het is bijna onmogelijk om, op het moment dat bepaalde datapakketten ontvangen worden, te zien of het om legitiem verkeer gaat of niet. Dit is vaak pas achteraf vast te stellen. En dan nog is het mogelijk dat sommige zaken als ruis worden aangemerkt en niet als opzettelijke portscan.

Het meest voorkomende communicatieprotocol dat op IP-netwerken voorkomt, is het Transmission Control Protocol (TCP). Hierbij communiceren twee systemen onderling met elkaar nadat eerst een sessie is opgezet tussen beide systemen. Dit TCP-synchronisatieproces komt normaal in drie stappen tot stand *(three-way handshake)*.

Als eerste verzoekt een systeem (werkstation host A) tot het openen van een sessie door het versturen van een SYN-pakket (synchronise) naar het doelsysteem (server host B). Deze antwoordt met een bevestiging in een SYN/ACK-pakket (synchronise/acknowledgement) en een aangepast volgnummer van het datapakket. Host A antwoordt op zijn beurt met een bevestiging in een ACK-pakket (acknowledgement). Hiermee is de TCP-sessie tot stand gebracht en kunnen de data worden verzonden.

Verschillende portscan-technieken zijn gebaseerd op het testen van (delen van) een TCP-sessie. Door het voortijdig afbreken van het opbouwen van de sessie kan de kans op detectie worden verkleind.

Naast zoeken naar TCP-poorten op een systeem worden portscans ook uitgevoerd voor andere communicatieprotocollen, zoals het (connectieloze) UDP (User Datagram Protocol) en ICMP (Internet Control Message Protocol).

De meest voorkomende portscans op TCP/IP zijn:

TCP-connect-scan

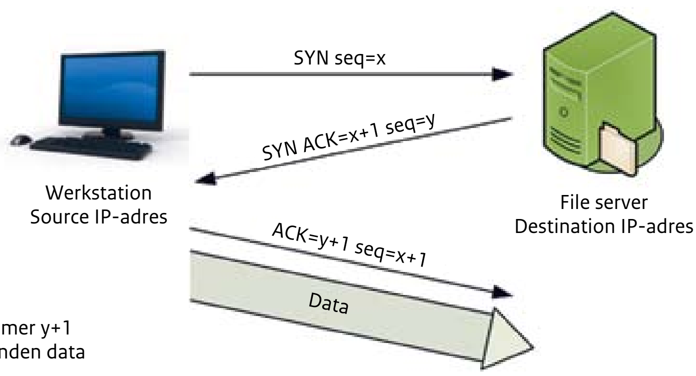
Een TCP-connect-scan is een scan die een volledige TCP-verbinding opzet tussen verzendende en de ontvangende computer over een TCP-poort. De volledige uitwisseling van gegevens om de verbinding tot stand te brengen wordt doorlopen (handshake). Deze uitwisseling bestaat uit een verzoek tot verbinding, een ontvangstbevestiging en een definitieve bevestiging (SYN -> SYN/ACK -> ACK). Dit is een erg betrouwbare manier van bepalen of netwerkpoorten op een systeem wel of niet open staan. Een aanvaller verraadt hiermee echter ook zijn eigen locatie in het netwerk, omdat het source-IP-adres wordt vermeld.

SYN-scan

Een SYN-scan is vergelijkbaar met een TCP-connect-scan, bij een SYN-scan wordt de handshake niet afgemaakt maar afgebroken. De aanvaller verbreekt de verbinding door op

TCP synchronisatieproces (handshake)

1. Werkstation (client) stuurt SYN packet met volgnummer x
2. Server bevestigt met SYN ACK packet met nummer x+1 en eigen volgnummer y
3. Werkstation antwoordt met ACK packet met nummer y+1 en nieuw volgnummer X+1 en vervolgt met verzenden data



de ontvangstbevestiging te antwoorden met een herstelcommando (RST of reset) (SYN -> SYN/ACK -> RST).

SYN/ACK-scan
Een SYN/ACK-scan maakt geen gebruik van de complete handshake. Bij een SYN/ACK scan stuurt een aanvaller als eerste een SYN/ACK-pakket. Een open poort zal hierop niet reageren, terwijl een gesloten poort zal antwoorden met het RST-pakket.

FIN-scan
Bij een FIN-scan (finished) stuurt een aanvaller een FIN-pakket naar een poort. Een open poort zal hier niet op reageren, terwijl een gesloten poort reageert met een RST-pakket.

NULL-scan
Een NULL-scan is een scan waarbij een datapakket wordt verstuurd dat geen enkele netwerkstatusparameter heeft aanstaan (flag). Er kan door de ontvangende computer dus niet worden gezien wat voor soort datapakket het is, een SYN-, ACK-, RST- of FIN-waarde ontbreekt. De door de aanvaller ontvangen reactie geeft een indicatie of een netwerkpoort open of dicht is. Bij geen reactie is een netwerkpoort waarschijnlijk open, terwijl een dichte netwerkpoort meestal zal reageren met een RST-pakket.

XMAS-scan
Een XMAS-scan (Christmas Tree) verstuurt een datapakket waarin alle netwerkstatusparameters of flags zijn gezet (SYN/ACK/RST/FIN/URG/PSH, oftewel Synchronise, Acknowledgement, Reset, Finished, Urgent, Push). Een gesloten poort reageert met een RST-pakket, terwijl een open poort niet reageert.

UDP ICMP_PORT_UNREACHABLE-scan
Deze scan maakt gebruik van het verbindingsloze UDP-protocol in plaats van het verbindingsgerichte TCP-protocol. Door een UDP-*datagram* te verzenden naar een netwerkpoort op het doelsysteem is te zien of een netwerkpoort open of dicht is. Een open poort zal niet reageren, terwijl bij een gesloten poort een niet-bereikbaar-bericht zal worden teruggestuurd.

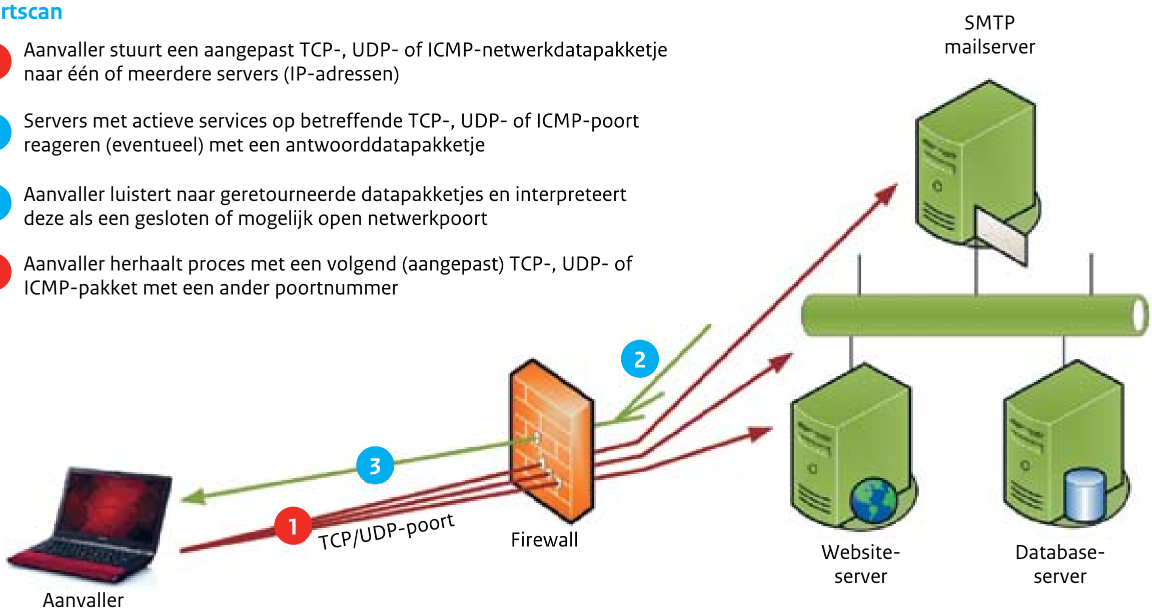
Decoy-scanning
Bij een decoy-scan gebruikt de aanvaller een techniek waarbij tijdens de portscan meerdere vervalste IP-adressen (*spoofed* IP-adressen naar het doelsysteem gestuurd worden. Deze techniek stelt aanvallers in staat om hun echte IP-adres te maskeren, of dit IP-adres te verbergen in een groep valse IP-adressen. Hoe meer IP-adressen als misleiding worden gebruikt in een scan, des te moeilijker wordt het te traceren welk IP-adres daadwerkelijk door de aanvaller is gebruikt.

Benodigde gegevens voor vaststelling
Voor het vaststellen van een portscan zijn vooral de logbestanden nodig van de verschillende netwerkcomponenten waarlangs de portscan heeft plaatsgevonden, zoals routers, *proxies*, firewalls en het doelsysteem. Met name de begin- en eindtijd(en), source-IP-adres, destination-IP-adres, netwerkpoorten en de headers van de netwerkpakketten zijn waardevol.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Portscan

1. Aanvaller stuurt een aangepast TCP-, UDP- of ICMP-netwerkdatapakketje naar één of meerdere servers (IP-adressen)
2. Servers met actieve services op betreffende TCP-, UDP- of ICMP-poort reageren (eventueel) met een antwoorddatapakketje
3. Aanvaller luistert naar geretourneerde datapakketjes en interpreteert deze als een gesloten of mogelijk open netwerkpoort
1. Aanvaller herhaalt proces met een volgend (aangepast) TCP-, UDP- of ICMP-pakket met een ander poortnummer



Strafbaarstelling

Wordt er binnengedrongen? Nee.

Bij een portscan worden gegevens naar een systeem gestuurd om te kijken of services beschikbaar zijn achter een bepaalde netwerkpoort. Als de scan succesvol is, worden de pakketten door de doelmachine ontvangen en er wordt op gereageerd. Er wordt niet binnengedrongen.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.

Het geautomatiseerde werk zal slechts op een bepaalde manier (volgens de gebruikte configuratie) reageren op de ontvangen pakketten. Er wordt geen stoornis veroorzaakt. Soms kan een systeem toch onverwacht reageren op een portscan of tijdelijk slechter bereikbaar zijn via het computernetwerk. De portscan kan dan de uitwerking van een kleine DoS-aanval op het gescande systeem hebben.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Nee.

De pakketten zijn in principe legitiem netwerkverkeer waarop op een normale manier gereageerd wordt.
Er worden hiermee geen gegevens gewijzigd of vernield.

Worden gegevens afgetapt of afgeluisterd? Nee.

Hoewel een aanvaller zal 'luisteren' naar eventuele reacties op de verzonden datapakketten, wordt overig netwerkverkeer niet afgeluisterd.

Strafbaarheid

Een portscan is niet strafbaar gesteld in het Wetboek van Strafrecht. Een portscan wordt gebruikt om te onderzoeken welke mogelijke onbeveiligde ingangen er zijn. Er is alleen sprake van kijken. Er wordt bij een portscan geen andere actie ondernomen. Er is dus geen sprake van het binnendringen in een geautomatiseerd werk, het vernielen van een geautomatiseerd werk, het onbruikbaar maken van gegevens of afluisteren.

De informatie die via de portscan wordt verzameld, kan echter gebruikt worden om een andere vorm van cybercrime voor te bereiden. Het zal van de omstandigheden van het geval afhangen of de portscan bedoeld is voor het (aansluitend) plegen van een strafbaar feit.

Wordt de portscan gezien als een voornemen van de dader tot het binnendringen in een computer, het vernielen van een geautomatiseerd werk, het vernielen van gegevens of afluisteren, dan kan strafbaarheid ontstaan op grond van poging.[37]

Het zal echter lastig zijn om de opzet van de verdachte aan te tonen, het voornemen om het systeem binnen te dringen. Een portscan wordt meestal niet met met speciale programmatuur uitgevoerd. Het is dan ook lastig om artikel 139d lid 2 (voorbereidingshandelingen) te bewijzen.

3.2.2 Spoofing en cache poisoning

Wat is spoofing?

Spoofing is je voordoen als iets of iemand anders. Spoofing is (digitale) identiteitsvervalsing en kan in vele vormen voorkomen. Elke techniek waarbij de bron of afzender niet op een betrouwbare manier geverifieerd wordt, is kwetsbaar voor spoofing. Veel voorkomende vormen zijn IP-spoofing, MAC-spoofing (Media Access Control), DNS-spoofing en e-mail-spoofing.

Wat is cache poisoning?

Een *cache* is een opslagplaats waarin veelgebruikte (netwerk-) data tijdelijk worden opgeslagen om snelheid te genereren. *Cache poisoning* treedt op wanneer een computer of server niet-authentieke gegevens ontvangt en in dit geheugen plaatst. De gemanipuleerde gegevens worden vervolgens gebruikt ten koste van de originele werkelijke gegevens. Het systeem is vergiftigd met vervalste informatie, vaak via spoofing. De meest voorkomende vormen zijn ARP- (Address Resolution Protocol) en DNS-cache-poisoning.

Technische verschijningsvormen en herkenbaarheid

IP-spoofing

Spoofing-technieken worden gebruikt voor ongeautoriseerd toegang krijgen tot een computer. Een aanvaller stuurt IP-pakketten naar een computer met als bronadres een (vervalst) IP-adres dat vertrouwd is. Deze datapakketten worden waarschijnlijk door firewalls doorgelaten.
Het is echter eenrichtingsverkeer van de aanvaller naar het doel-IP-adres. Het antwoord dat door de ontvangende computer wordt verzonden, komt namelijk niet terug bij de aanvaller maar wordt gestuurd naar het echte systeem met het betreffende IP-adres. Een aanvaller vuurt dus 'blind' netwerkverkeer af op het doelwit in een poging om dit te compromitteren.

IP-spoofing kan onder andere worden herkend door netwerkverkeer te monitoren.[38] Hierbij gaat het om netwerkverkeer waarbij de IP-adressering niet overeenkomt met de adressering van de werkelijke zender.

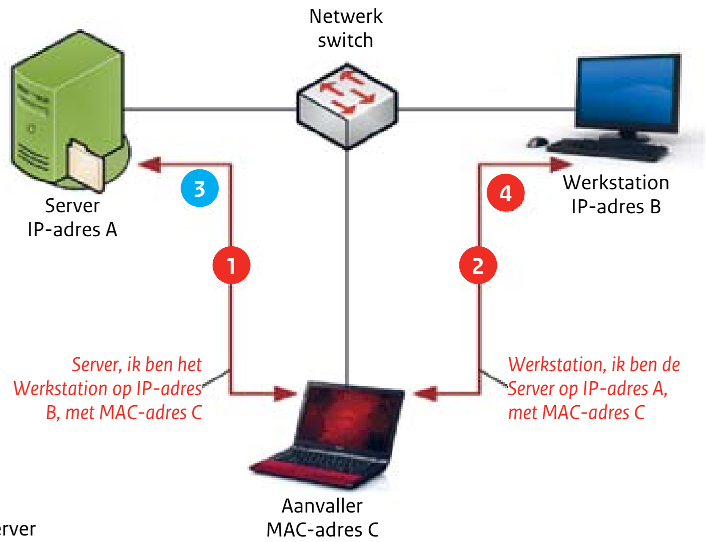
Het onderzoeken van *firewall logs* is een andere manier van detecteren. Op de meeste firewalls moet anti-spoofing-detectie mogelijk apart geconfigureerd worden.

MAC-spoofing

MAC-spoofing is een techniek voor het veranderen van een door de fabriek toegewezen MAC-adres (Media Access Control) van een netwerkinterface op een netwerkapparaat.

37. http://www.iusmentis.com/beveiliging/hacken/portscans
38. Bijvoorbeeld met behulp van (gratis) softwarepakketten als tcpdump, snort, netlog of wireshark of intrusion detection systems (IDS).

ARO-spoofing/cache poisoning



1. Aanvaller stuurt een aangepast ARP-datapakket naar een server met IP-adres van werkstation
2. Aanvaller stuurt een aangepast ARP-datapakket naar werkadres met IP-adres van server
3. Server stuurt nu al het netwerkverkeer bestemd voor werkstation naar aanvaller
4. Aanvaller stuurt al het netwerkverkeer tussen server en werkstation door maar luistert ondertussen af

Het veranderen van het toegewezen MAC-adres kan de toegangscontrolelijst (Access Control List) op servers of routers omzeilen. Een systeem verstopt zich in het netwerk of doet zich voor als een ander netwerkapparaat.

Een legitieme reden om het MAC-adres van een netwerkadapter te wijzigen is bijvoorbeeld om opnieuw netwerkverbinding te maken na een hardwarestoring of vervanging van het systeem.

Voor MAC-spoofing is een normale netwerkverbinding nodig, waarbij ook reacties van andere systemen worden ontvangen. MAC-spoofing is beperkt tot het lokale broadcast-domein.

ARP-spoofing/cache poisoning
Het ARP (Address Resolution Protocol) wordt gebruikt voor de koppeling van logische IP-adressen aan de hardwareadressen op de netwerklaag (Ethernet MAC-adressen). Een tabel (ARP-cache) wordt gebruikt om relatie te leggen tussen een IP-adres en het corresponderende MAC-adres. Bij ARP-spoofing krijgt de host valse informatie via valse ARP-verzoeken en -antwoorden. Met ARP-spoofing/cache poisoning kan bijvoorbeeld op een *switched* Ethernetnetwerk toch netwerkverkeer van het LAN (Local Area Network) worden onderschept en afgeluisterd.

ARP-spoofing/cache poisoning is op een systeem alleen te detecteren als er geen gebruik wordt gemaakt van proxy-ARP. ARP-spoofing/cache poisoning is herkenbaar aan deze eigenschappen:
- een IP-adres wordt zonder reden omgezet naar een foutief MAC-adres;
- een MAC-adres komt meerdere malen in de ARP-tabel voor.

DNS-spoofing/cache poisoning
Bij DNS-spoofing/cache poisoning wordt een *DNS-caching-nameserver* van het domein van een slachtofferwebsite gemanipuleerd. Een aanvaller stuurt vervalste informatie naar een DNS-caching-nameserver.
Deze methode wordt gebruikt om de database of de cache van een DNS-server aan te passen. Gebruikers die een IP-adres van een website opvragen, worden ongemerkt doorverwezen naar een malafide server. De suggestie wordt gewekt dat de informatie afkomstig is van een vertrouwd systeem.

DNS-spoofing/cache poisoning komt op verschillende manieren voor:
- Een aanvaller gebruikt een DNS-server om de verwijzing naar het IP-adres van een hostname aan te passen. Dit adres kan het IP-adres zijn van een systeem dat een aanvaller onder controle heeft. Of het IP-adres is een adres dat niet wordt gerout op het internet.[39]
  Het gevolg is dat dataverkeer niet op de plaats van bestemming aankomt.
  Deze methode is te herkennen aan:
  - doelsysteem krijgt geen nieuwe verzoeken meer (daling netwerkverkeer);
  - herkenning van inbraakpogingen aan de hand van een IDS of firewall;
  - datum van aanmaak/aanpassing/verwijdering van DNS-bestanden.[40]
- Een aanvaller vervalst het antwoord van een DNS-caching-nameserver vóórdat het daadwerkelijke antwoord terugkomt. Een systeembeheerder kan dit soort problemen

39. RFC1918 adressen of niet-gealloceerde IP-adressen
40. Met host-based IDS oplossingen, zoals Tripwire, kunnen mutaties aan bestanden worden bewaakt.

niet altijd detecteren, omdat de DNS-caching-nameserver vaak door iemand anders wordt beheerd.
- Een aanvaller vervuilt de DNS-cache door naar de caching-nameserver valse antwoorden te versturen.
  Een cache kan worden vervuild door:
  - Informatie verzenden naar de caching-nameserver met een TTL-parameter (Time-to-Live) die hoger is dan de oorspronkelijke informatie die zich in de caching-nameserver bevindt;
  - Vervuilde informatie over de domeinnaam (domein A) van een slachtofferwebsite verhullen in de *zonefile* van een ander domein (domein B). Als aan een willekeurige caching-nameserver op het internet informatie van domein B wordt opgevraagd, wordt de foutieve informatie van domein A meegenomen: de cache is vervuild.

In het document 'DNS misbruik, van herkenning tot preventie' (GOVCERT.NL, 30-07-2008) staat hierover meer informatie.

E-mail-spoofing
Bij e-mail-spoofing wordt misbruik gemaakt van het feit dat veel ontvangers van e-mail veronderstellen dat e-mail-berichten legitiem zijn. Vervalste e-mail wordt voornamelijk gebruikt om gebruikers ertoe te brengen zaken te doen, die ze anders niet zouden (moeten) doen. E-mail-spoofing wordt meestal in combinatie met *mail bouncing* en spam toegepast.

Technisch gezien is e-mail-spoofing niet met zekerheid te onderscheiden van legitieme e-mail. Een technische definitie van valse e-mail is niet te maken. Door analyse van e-mail-headers kan in sommige gevallen e-mail-spoofing worden herkend.

E-mail-spoofing wordt vaak in combinatie gebruikt met mail bouncing. Hierbij wordt e-mail gestuurd naar verschillende e-mailadressen vanaf een vervalst e-mailadres. Voor de verzending kan een *open relay server* worden gebruikt. De ontvangers van het e-mailbericht kunnen legitieme e-mailadressen zijn maar ook nep-e-mailadressen. Ontvangers van een dergelijke e-mail zijn geneigd om een antwoord terug te sturen naar het vervalste e-mailadres. Wanneer de e-mail is verzonden naar een (niet-bestaand) foutief e-mailadres, dan zal de ontvangende e-mailserver een automatisch antwoord met foutmelding terugsturen (bounce-bericht). Door van deze techniek gebruik te maken kunnen aanvallers testen of e-mailadressen bestaan.

URL-spoofing
Bij URL-spoofing (Uniform Resource Locator) worden verwijzingen naar websites (URLs) zodanig gekozen dat deze op het eerste gezicht lijken op normale bonafide websiteverwijzingen. Met typografische trucs, bijvoorbeeld door de letter 'o' te vervangen door een 0 (nul), wordt een slachtoffer verleid tot het openen van een link naar een malafide website. Deze techniek wordt veel gebruikt in phishing-aanvallen.

Deze vorm van URL-spoofing is eigenlijk een social-engineering-methode die inspeelt op slecht kunnen onderscheiden van typografische karakters en veel voorkomende typefouten bij het invoeren van een websiteadres.

Een andere vorm is om een afwijkende vreemde karakterset te gebruiken die overeenkomsten heeft met het Latijnse alfabet *(domain squatting)*. Deze aanpak is nog veel beter dan de gezichtsbedrogtrucs zoals hierboven beschreven. Websurfers kunnen bij domain squatting niet zien of ze naar een vervalst webadres worden geleid. In bepaalde lettertypes *(fonts)* lijken vreemde tekens op Latijnse tekens zoals in ons alfabet. In veel fonts ziet een Cyrillische 'o' eruit als zijn Latijnse tegenhanger.

BGP-spoofing
Het BGP (Border Gateway Protocol) is het inter-domein-routing protocol, dat wordt gebruikt om informatie over netwerkbereikbaarheid tussen ISPs (Internet Service Providers) uit te wisselen via het internet. De border-gateway-router van een ISP-netwerk onderhoudt een tabel van IP-netwerken die kunnen worden bereikt. BGP is kwetsbaar voor kwaadaardige aanvallen *(BPG peer spoofing)*, sessie-kaping en route-injectie, omdat het vertrouwt op de integriteit van de ontvangen informatie van andere systemen *(peers)*.

Benodigde gegevens voor vaststelling
Voor het vaststellen van spoofing en cache poisoning zijn de logbestanden nodig van de verschillende netwerk-componenten waarlangs de aanval heeft plaatsgevonden. Daarnaast kunnen alle afwijkende gedragingen van de computer een aanwijzing zijn, zoals onbekende meldingen in een firewall of IDS-log, trager wordende netwerk-prestaties of meldingen van verbindingsfouten. Met name het source- en destination-IP-adres, MAC-adressen en de (e-mail)headers van de netwerkpakketten zijn waardevol. De belangrijkste technische informatie is:
- een technische beschrijving van de systemen;
- logbestanden van routers, DNS-servers, firewalls en aangevallen systemen;
- informatie over het netwerk, firewalls en andere beveiligingsmaatregelen.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Mogelijk.

Het hangt af van de vorm waarmee is binnengedrongen. Bij e-mail-spoofing en IP-spoofing wordt niet direct binnengedrongen. Bij IP-spoofing kunnen de netwerkpakketten verzonden met vervalste IP-adressen wél malware of exploit-code meesturen om binnen te dringen. Bij ARP- en DNS-cache poisoning is wel sprake van binnendringen.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.

Het hangt af van de vorm. Als alleen een valse identiteit is aangenomen, bijvoorbeeld bij e-mail-spoofing, wordt geen stoornis in het geautomatiseerde werk veroorzaakt.

Als de cache van een DNS-server wordt vervuild of de DNS-zonefile wordt aangepast, is er sprake van beschadiging van de nameserver. Echter de werking van de nameserver wordt niet aangetast. Alleen de gegevens die in het geheugen zijn opgeslagen worden aangepast.

Bij IP-spoofing, ARP-spoofing of DNS-cache poisoning kan er, omdat de netwerkrouting wordt aangepast of omdat gegevens veranderd worden, wel stoornis in een geautomatiseerde werk optreden. De normale IP-routing, ARP- of DNS-functionaliteit wordt verstoord.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Mogelijk.

Het hangt af van de vorm: bij e-mail-spoofing en IP-spoofing worden niet direct gegevens gewijzigd of vernield. Bij ARP en DNS-spoofing/cache poisoning is dit wel het geval.

Worden gegevens afgetapt of afgeluisterd? Mogelijk.

Het hangt ook hierbij af van de vorm: bij e-mail-spoofing of IP-spoofing worden geen gegevens afgeluisterd. Bij ARP-cache poisoning is dit meestal wel het geval. Bij DNS-spoofing/cache poisoning worden bezoekers van een website omgeleid naar een malafide website. Een hacker zou op deze manier wachtwoorden of creditcardgegevens kunnen onderscheppen van de bezoekers.

Strafbaarheid

Hoewel dit niet voor alle vormen van spoofing geldt, is spoofing een techniek om met valse signalen binnen te dringen in een geautomatiseerde werk. In dat geval is er sprake van computervredebreuk zoals strafbaar gesteld in artikel 138ab Sr als gevolg van het aannemen van een valse hoedanigheid.
Wanneer spoofing de toegang tot een geautomatiseerd werk belemmert, is sprake van strafbaarheid onder artikel 138b Sr, omdat gegevens worden aangeboden of toegestuurd waardoor de eigenaar geen gebruik meer kan maken van zijn eigen systeem (denial of service).

Bij DNS-spoofing/cache poisoning is er meestal sprake van strafbare gegevensaantasting (art. 350a lid 1 Sr), omdat gegevens in het DNS-systeem worden aangepast of toegevoegd.

Worden gegevens gemanipuleerd of beschadigd, dan is er wel sprake van gegevensaantasting (art. 350a Sr) of van het veroorzaken van een stoornis in de werking van het geautomatiseerde werk (art. 161sexies Sr). Voor strafbaarheid op grond van artikel 161sexies Sr is wel vereist, dat één van de gevolgen genoemd in deze artikelen intreedt. Deze gevolgen zijn stoornis in de uitvoering van een nutsdienst of openbaar telecommunicatienetwerk of telecommunicatiedienst, van gemeen gevaar voor goederen of diensten, of levensgevaar.

Als voorbeeld voor de toepasselijkheid van de strafrechtelijke bepalingen bij IP-spoofing is het nodig dat er een IP-adres van iemand anders wordt gebruikt (valse hoedanigheid). Hierdoor kan een beveiliging worden omzeild (art. 138ab lid 1 sub a Sr). Als er sprake is van het overnemen van gegevens, kan dit mogelijkerwijs strafbaar zijn op grond van artikel 138ab lid 2 Sr. Bovendien worden als gevolg van IP-spoofing reacties naar een verkeerd IP-adres, en dus een verkeerd systeem, gestuurd. Hierdoor kan het geautomatiseerd werk worden vernield of beschadigd (art. 161sexies of art. 350a Sr).

Doordat netwerkverkeer naar een ander systeem of via een systeem onder controle van de aanvaller worden gestuurd, lekt mogelijk vertrouwelijke informatie uit. Spoofing kan zo onder meer leiden tot bedrijfsspionage, oplichting of bedrog. Het afluisteren van gegevens is strafbaar onder artikel 139c en 139d Sr.

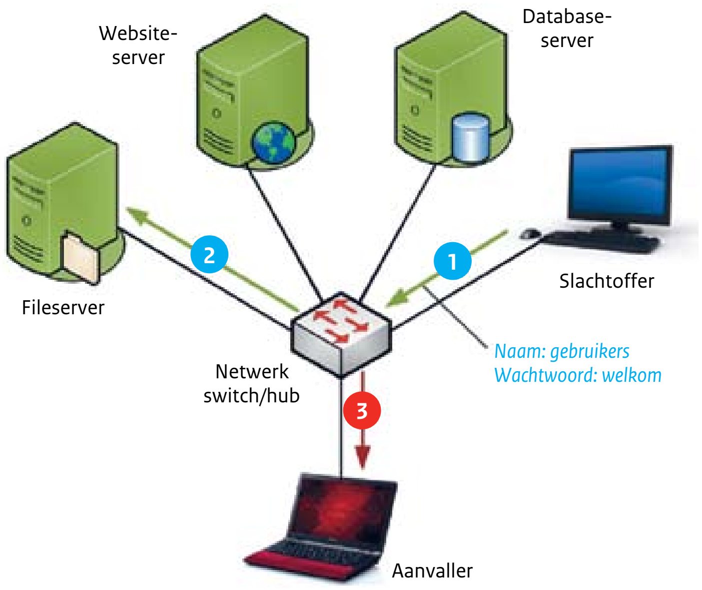
3.2.3 Sniffing

Wat is sniffing?

Sniffing is het bekijken (meekijken en afluisteren) van netwerkverkeer *(network eavesdropping)*. Normaal wordt sniffing legitiem ingezet voor het analyseren van netwerkverkeer, om knelpunten te identificeren of om prestaties van het netwerk te kunnen verbeteren.

Sniffing wordt echter ook kwaadaardig gebruikt voor bijvoorbeeld *netwerkmapping*, het onderscheppen van vertrouwelijke informatie of wachtwoorden. In het bijzonder onbeveiligde netwerkprotocollen, zoals HTTP (Hypertext Transfer Protocol), FTP *(file transfer)*, Telnet (besturing op afstand), SNMP (monitoren), LDAP (Lightweight Directory Access Protocol)), TDS (Tabular Data Stream voor SQL-server), IMAP4 (Internet Message Access Protocol), POP3 (Post Office Protocol) en SMTP (e-mail), zijn interessant om af te luisteren. Deze protocollen kunnen gebruikersnamen en wachtwoorden in leesbare vorm versturen.

Sniffing op lokaal netwerk



1 Slachtoffer stuurt netwerkverkeer naar server

2 Netwerkverkeer wordt gerout naar bestemming

3 Het netwerkverkeer wordt onderschept door aanvaller en afgeluisterd

Met de opkomst van draadloze netwerken en Bluetooth-apparatuur is sniffen relatief gevaarlijk geworden: om te kunnen sniffen is geen directe fysieke verbinding met het computernetwerk meer nodig.

Het gevaar voor afluisteren bestaat ook bij netwerkverbindingen over het bestaande elektriciteitsnet *(Ethernet over power)*. Hierbij wordt het netwerkverkeer getransporteerd via een adapter in het stopcontact. Zonder aanvullende maatregelen is de beveiliging vergelijkbaar met een onbeschermd draadloos netwerk. Iedereen in de omgeving met een vergelijkbare adapter in een stopcontact kan, afhankelijk van de fysieke bedrading van het lokale elektriciteitsnet, de signalen van andere adapters zien en onderscheppen.

Technische verschijningsvormen en herkenbaarheid
In principe is een sniffer passief op het netwerk aanwezig, omdat alleen wordt geluisterd en geen actieve netwerkverbindingen in stand worden gehouden. Daarom is het bijzonder moeilijk en foutgevoelig om te detecteren dat er op een computernetwerk afgeluisterd wordt door sniffing.

Sniffing kan worden uitgevoerd met speciale professionele netwerkapparatuur die alleen als zodanig te gebruiken is. Zulke apparatuur wordt gebruikt door telecommunicatiebedrijven en netwerkinstallateurs. Legitieme sniffers (netwerktaps) worden ook gebruikt in IDS-oplossingen. Sniffers die op hardware zijn gebaseerd, zijn juist ontworpen om geen verstoring op een netwerk te kunnen veroorzaken. Ze ontvangen alleen netwerkpakketten en zijn niet te detecteren.

De meest voorkomende vorm van sniffing gebruikt (gratis) software op standaard platformen.[41] Sniffers geïnstalleerd op standaardmachines zijn soms wel te detecteren. Om te functioneren als sniffer is de netwerkadapter geconfigureerd in een zogenaamde *promiscuous-modus*, zodat de adapter al het voorbijkomende netwerkverkeer accepteert. Bovendien kan het besturingssysteem van de computer waarop de sniffing-software is geïnstalleerd, ongewild netwerkpakketten uitsturen.

Het afluisteren van een lokaal netwerk (LAN) wordt vaak gecombineerd met ARP-spoofing en cache poisoning. De meeste Ethernet-netwerken gebruiken tegenwoordig switches voor efficiënt gebruik van de beschikbare infrastructuur. Hierdoor is niet zondermeer al het netwerkverkeer meer af te luisteren. Met behulp van ARP-cache poisoning wordt het netwerkverkeer omgeleid via een systeem, dat onder controle van de aanvaller staat, om datapakketten verzonden over netwerkswitches toch te kunnen onderscheppen *(man-in-the-middle)*.

Met kennis van de verschillende methodes kan sniffing vanaf standaardcomputers worden gedetecteerd via:

Ping-methode
Hierbij wordt een *ping request* naar het IP-adres van het systeem gestuurd, waarvan wordt vermoed dat er een sniffer actief is.[42] Een normaal functionerend systeem zal hierop reageren met een *ping replay*.
Om het te detecteren wordt in het ping request een MAC-adres meegezonden dat niet juist is en dus niet bestaat op het netwerksegment. Als er toch op het ping request wordt gereageerd, dan staat op de betreffende computer het filter op MAC-adres uit (en staat de netwerkadapter dus in promiscuous-modus). Sniffers kunnen

41. Enkele bekende (gratis) software tools zijn tcpdump, wireshark, Cain maar daarnaast zijn er ook commerciële netwerkanalyse programma's.
42. Als variatie op de ping-methode is het mogelijk om elk protocol te gebruiken waarop een antwoord te verwachten valt. Het gedrag van het sniffende systeem zal afwijken van de normaal te verwachten reactie.

softwarematige MAC-filtering aanbrengen om detectie met de ping-methode te omzeilen.[43]

DNS-methode
Veel (niet-commerciële) sniffers proberen bij onderschepte IP-adressen direct de hostname te zoeken door reverse DNS look-ups. Door bij de DNS-server te monitoren op *reverse DNS look-ups* is het mogelijk om sniffers te detecteren. De reverse lookups zijn uit te lokken door zelf een *ping-sweep* uit te voeren op het lokale netwerk of door IP-verkeer naar niet-bestaande IP-adressen te sturen. Wanneer als gevolg hiervan toch reverse lookups te zien zijn, is er mogelijk een sniffer geïnstalleerd.

Honeypot-uitlokking
Deze methode kijkt indirect of er sniffers aanwezig zijn door aanmaak en gebruik van nep-gebruikersaccounts op een testcomputer te monitoren. Regelmatige aanmelding met het nepaccount op het netwerk kan door een eventuele sniffer worden onderschept. Vervolgens kan worden gecontroleerd of de nepaccount is gebruikt buiten bekende aanlogtijden om. Zulk gebruik kan duiden op de aanwezigheid van een sniffer.

Nadat is vastgesteld dat er wordt afgeluisterd, is het zaak om het verdachte systeem fysiek te lokaliseren. Alvorens dit te isoleren van het netwerk moet worden onderzocht welke componenten op het systeem het eigenlijke sniffen uitvoeren. Mogelijk is het systeem gecompromitteerd en wordt het sniffen uitgevoerd door een Trojaans paard.

Benodigde gegevens voor vaststelling
Voor het vaststellen van een sniffer zijn logbestanden weinig relevant. Vaak wordt sniffing alleen indirect vastgesteld doordat gevoelige informatie bekend is geworden bij onbevoegde personen of omdat een gebruikersaccount en wachtwoord zijn gecompromitteerd en gebruikt in een cyberincident.

Met de beschreven technische methoden kan sniffing mogelijk worden vastgesteld als eigen verschijningsvorm. Hiervoor zijn benodigd:

- Ping-methode of variant:
  - beschrijving van het gebruikte protocol met de verwachte resultaten;
  - logbestand van het netwerkverkeer waaruit blijkt dat een bepaald systeem reageert op een ping request terwijl dat niet zou moeten gebeuren (échte resultaten in plaats van verwachte resultaten).
- DNS-methode:
  - logbestand van het netwerkverkeer waaruit valt op te maken dat, na het verzenden naar een bepaald IP-adres, een DNS-request werd uitgevoerd om de bijbehorende hostname op te vragen.
- Uitlokking door honeypot:
  - documentatie van het gecreëerde account, datum en tijd en locatie van aanmaak, en data en tijden waarop ‘legitiem’ ingelogd wordt of zal worden;
  - logbestand van het systeem waaruit inlogpogingen op het gecreëerde account worden vastgelegd. Hierin zullen zowel legitieme inlogpogingen als pogingen via onderschepte informatie te zien zijn.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling
Wordt er binnengedrongen? Nee.
Sniffen hoeft alleen passief netwerkverkeer op te pakken. Wel is het zo dat, om verkeer op een netwerk te sniffen, toegang tot dat netwerk nodig is. Mogelijk dat de dader hiervoor een technisch hulpmiddel moet plaatsen waardoor hij in staat is gegevens af te tappen en/of op te nemen, zodat dus sprake is van binnendringen. Een voorbeeld hiervan is het installeren van een Trojaans paard dat netwerkverkeer afluistert en doorstuurt naar de dader.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Nee.
Door een sniffer wordt het automatisch werk niet vernield, beschadigd of gewijzigd. Vaak verdient het wel de voorkeur om na ontdekking het systeem opnieuw te installeren en niet alleen de ontdekte malware te verwijderen.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Nee.
Door alleen het onderscheppen van netwerkverkeer worden de afgeluisterde gegevens niet veranderd. Als sniffer-software onrechtmatig op een geautomatiseerd werk wordt toegevoegd om het aftappen mogelijk te maken, is er sprake van gegevensaantasting, ook al worden de opgeslagen of verzonden gegevens en software niet veranderd. Er worden ook gegevens aangetast bij de afgetapte computers als ARP-spoofing/cache poisoning worden ingezet om afluisteren over een switched netwerk mogelijk te maken.

Worden gegevens afgetapt of afgeluisterd? Ja.
Sniffen is afluisteren van netwerkverkeer. Vertrouwelijke informatie kan uitlekken.

Strafbaarheid
Bij sniffing worden gegevens verzonden over een telecommunicatienetwerk onderschept. Als er opzettelijk gegevens worden onderschept is dit strafbaar gesteld in artikel 139c Sr. Daarnaast kan, als gevolg van het plaatsen van een technisch hulpmiddel, strafbaarheid optreden op grond van artikel 139d en artikel 350a lid 1 Sr.

43. Er bestaan softwarematige netwerkanalyse tools die promiscuous modus scans kunnen uitvoeren.

Daarnaast kunnen met name artikel 139d lid 2 en 3 Sr (voorbereidingshandelingen) relevant zijn bij de aanpak van sniffen. In dit artikel wordt het ter beschikking stellen en het voorhanden hebben van technische hulpmiddelen strafbaar gesteld, wanneer deze hoofdzakelijk ontworpen of geschikt gemaakt zijn voor het plegen van de misdrijven van art. 138ab en 139c Sr en als de intentie bestaat om daarmee wederrechtelijk af te luisteren.

Wanneer wederrechtelijk verkregen gegevens worden opgeslagen op een voorwerp zodanig dat de aanvaller erover kan beschikken en dit voorhanden heeft, bijvoorbeeld op een usb-stick, kan dit strafbaar zijn onder artikel 139e lid 1 Sr. Als dergelijk verkregen gegevens opzettelijk aan een ander bekend worden gemaakt is dat strafbaar onder artikel 139e lid 2 Sr.

3.2.4 Misbruik van draadloze netwerken en apparatuur

Het gebruik van draadloze apparatuur is in de afgelopen jaren sterk gegroeid. Vrijwel alle laptops, tablets, PDA's en smartphones bevatten tegenwoordig geïntegreerde WiFi (IEEE 802.11) en Bluetooth-voorzieningen. Daarnaast wordt het mobiele telefoonnetwerk (GSM/GPRS, UMTS, HSDPA) intensief gebruikt voor altijd-en-overal-toegang tot internet en bedrijfsvoorzieningen. Ook in de procesautomatisering rukt het gebruik van draadloze technieken op. De risico's van draadloze verbindingen en apparatuur zijn:

- verstoring van de verbinding;
- uitlekken van informatie door afluisteren of onderscheppen;
- binnendringen in het (bedrijfs)netwerk;
- misbruiken van de verbinding of het apparaat.

Draadloze netwerken bestaan normaal uit toegangspunten (access points) en mobiele apparatuur met draadloze netwerkkaarten. Het toegangspunt is meestal een netwerkrouter met WiFi (IEEE 802.11), die gebruikers toegang geeft tot het achterliggende thuis- of bedrijfsnetwerk waarmee het toegangspunt is verbonden. Daarnaast kunnen ook direct WiFi-verbindingen tussen computers onderling opgezet worden.

Een extra gevaar vormt een zogenoemd *rogue access point*. Dit is een draadloos toegangspunt dat op een (bedrijfs-) netwerk is geïnstalleerd zonder uitdrukkelijke toestemming van een netwerkbeheerder. Zo wordt een achterdeur opengezet naar de beveiligde omgeving door onbevoegden. Niet alleen goedkope ongeautoriseerd aangesloten WiFi-netwerkrouters, maar ook actieve WiFi-verbindingen op bijvoorbeeld laptops, aangesloten op het bedrijfsnetwerk, vormen een gevaar.

Op infrarode verbindingen wordt in deze handleiding niet verder ingegaan. Het beveiligingsrisico van infrarood wordt beperkt omdat zender en ontvanger daarbij zichtbaar moeten zijn voor elkaar.

Technische verschijningsvormen en herkenbaarheid

Een draadloze verbinding komt tot stand door radiografische golven. In tegenstelling tot een conventionele verbinding zijn de signalen dus niet fysiek aan netwerkbekabeling gebonden. Het grote voordeel is dus de plaatsonafhankelijkheid: de verbinding kan binnen een bepaalde radius tot stand worden gebracht.[44] De flexibiliteit van draadloze verbindingen maakt het meteen ook moeilijker te traceren op meeluisteren of misbruik.

De factsheet 'FS-2008-01 Draadloze netwerken' geeft meer achtergrondinformatie en aanbevelingen voor de beveiliging van draadloze netwerken (GOVCERT.NL, 28-09-2009).

Verstoren van de verbinding (jamming)

Een nadeel van radiogolven is dat deze gemakkelijk te verstoren zijn. Een draadloze verbinding kan met eenvoudige middelen dusdanig worden verstoord dat die verbinding niet meer beschikbaar is (denial of service). Dergelijke verstoringen zijn zeer goed per ongeluk mogelijk door foutieve configuraties van naburige draadloze apparatuur.

Een stoorzender kan worden herkend doordat deze een sterk signaal afgeeft op hetzelfde zendkanaal als de verstoorde verbinding. Met speciale apparatuur en richtantennes kan een stoorzender worden opgespoord door een driehoeksmeting (triangulatie) uit te voeren.

Afluisteren van het draadloze netwerk

Het is zeer eenvoudig om radiogolven op te vangen. Het ontvangende apparaat hoeft daarvoor niet per sé zelf onderdeel van de verbinding te zijn. Om de informatie die over een draadloze verbinding wordt verstuurd te beschermen wordt meestal gebruik gemaakt van versleuteling (encryptie).[45] De oudere vormen van WiFi-encryptie, WEP (WiFi Encryption Protocol) , maar ook de nieuwere vormen zoals WPA (Wi-Fi Protected Access), kunnen worden doorbroken door een aanvaller.

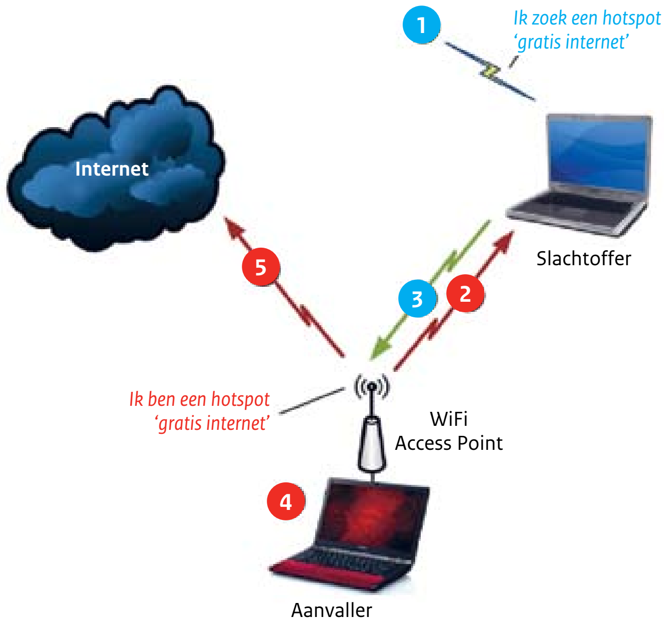
Bij een normaal actief gebruikt draadloos netwerk is het voldoende om gedurende enige tijd (enige uren) het netwerkverkeer passief af te luisteren. Een aanvaller verzendt

44. Het bereik van een WiFi-verbinding is sterk afhankelijk van het zendvermogen van de apparatuur, de gebruikte antennes en de fysieke omgeving (gebouwen, begroeiing etc.). Apparatuur met ingebouwde antennes, zoals laptops, hebben een gemiddeld bereik van 50 tot 100 meter. Netwerktoegangspunten hebben een gemiddeld (onderling) bereik van enkele honderden meters. Met richtantennes en speciale apparatuur kunnen aanzienlijk grotere afstanden worden overbrugd. Bluetooth heeft een beperkter bereik tot enkele tientallen meters.

45. Draadloze apparatuur beschikt vrijwel standaard over de mogelijkheid verbindingen te versleutelen. De WEP-standaard is tegenwoordig volstrekt ontoereikend om tot een acceptabel beveiligingsniveau te komen. De nieuwere WPA-2-standaard met lange sleutellengtes biedt wel afdoende bescherming voor de meeste toepassingen. Aanvullend kan een extra laag bovenop de verbinding worden aangebracht, zoals een VPN-verbinding of het gebruik van SSH of SSL.

WiFi Access Point spoofing

1. Slachtoffer zoekt WiFi toegangspunt. Aanvaller luistert op alle kanalen naar WiFi-netwerkveroeken
2. Aanvaller stuurt bevestiging met SSID-naam die wordt verwacht/gezocht of broadcast een 'hotspot'-naam
3. Slachtoffer verbindt met rogue acces point van aanvaller
4. Aanvaller luistert al het ontvangen netwerkverkeer af en/of vraagt om betaling voor toegang
5. Aanvaller stuurt al het netwerkverkeer door om slachtoffer te blijven misleiden



dan zelf geen dataverkeer naar het netwerk, maar slaat alle onderschepte datapakketten op. De sleutel van een WEP-beveiligd netwerk kan zo worden verkregen, waarna de aanvaller ongemerkt kan meeluisteren. Als het netwerk is beveiligd met WPA worden de verzamelde datapakketten (offline) geanalyseerd op bekende woorden *(dictionary attack)* met vooraf berekende sleutelwaarden *(rainbow tables)*.

Het passief afluisteren van een draadloos netwerk valt technisch niet te detecteren. Een aanvaller moet zich binnen het bereik van de uitgezonden radiogolven bevinden dan wel afluisterapparatuur hebben geplaatst om eventueel te worden ontdekt.

Onderscheppen van draadloze netwerken

Een andere techniek is als een aanvaller zich voordoet als een betrouwbaar toegangspunt om vervolgens de verbinding te kapen. Hierbij worden gebruikers verleid om verbinding te maken met een vals toegangspunt *(rogue access point)* dat lijkt op een bedrijfsnetwerk of een (gratis) internet dienst *(hotspot)*. De hacker kan zo al het netwerkverkeer omleiden en afluisteren. Daarnaast is het mogelijk dat het slachtoffer een webpagina krijgt aangeboden, waarop tegen geringe vergoeding toegang verkregen wordt tot het internet vanaf een openbare plaats, zoals een hotel, station of luchthaven.

Om de kans op een succesvolle aanval te vergroten verstoort de aanvaller tegelijkertijd het signaal van het echte toegangspunt of zendt een krachtiger signaal uit. Om de kans op ontdekking te verkleinen leidt de aanvaller het verkeer van gebruikers verbonden aan zijn valse toegangspunt vervolgens door naar het bedrijfsnetwerk of internet *(WiFi Acces Point spoofing)*. De gebruiker heeft zo alsnog beschikking over de verwachte netwerkverbinding en zal dan ook niet (of moeilijk) kunnen herkennen dat deze verbinding verloopt via een onbevoegd draadloos toegangspunt (man-in-the-middle).
Rogue access points kunnen worden gedetecteerd via *wireless intrusion detection/prevention-systemen* (WIDS) door het radiospectrum op ongeautoriseerde toegangspunten te controleren.

Binnendringen in (WiFi-)netwerk

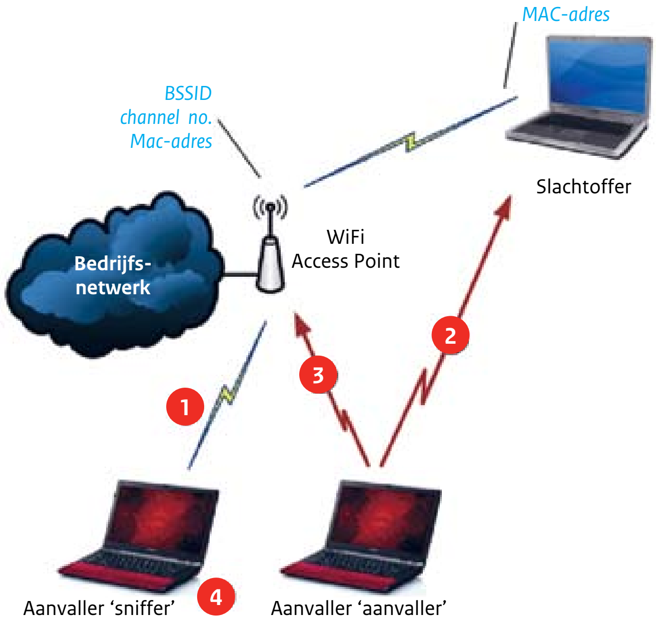
Om binnen te dringen in een draadloos netwerk zal een aanvaller de beschikking moeten hebben over de sleutel(s) waarmee het netwerk is beveiligd. Dit kan op een passieve methode, zoals beschreven in de paragraaf over afluisteren, waarbij de kans op ontdekking nihil is.
Er is ook een actieve manier om binnen te dringen. Omdat voor het doorbreken van de encryptie eerst voldoende datapakketten moeten worden verzameld, kan een aanvaller valse datapakketten gaan versturen naar een toegangspunt om dit proces van dataverzameling te versnellen.[46]

Aanvallen via draadloze verbindingen zijn een vorm van computerinbraak-op-afstand. Alleen de pogingen of wijze waarop toegang tot het netwerk wordt verkregen verschillen. Als eenmaal toegang tot een netwerk is verkregen, zullen bekende technieken als portscans, sniffing, spoofing en dergelijke worden gebruikt om het interne netwerk verder in kaart te brengen. Gerichte aanvallen op achterliggende systemen worden ingezet om verder door te dringen in het bedrijfsnetwerk.

46. Er zijn verschillende (gratis) tools en uitgebreide instructies om WiFi toegangspunten aan te vallen beschikbaar op het internet. Bij de meeste opstellingen worden één of twee onderscheppende/aanvallende laptops gebruikt en eventueel aangepaste (richt)antennes.

WiFi-encryptie-aanvallen

1. Aanvaller 'sniffer' luistert op alle kanalen naar WiFi-dataverkeer en slaat alle onderschepte datapakketten van/naar Access Point op
2. Aanvaller stuurt 'deauthenticate'-bericht naar verbonden werkstations, die vervolgens opniew verbinden en zo nieuwe ARP-verzoeken uitsturen
3. Aanvaller verstuurt onderschept ARO-datapakket ('ARP-spoofing') en blijft dit herhalen ('replay attack')
4. Aanvaller decrypt (WEP/WPA) sleutel offline als voldoende onderschepte datapakketten zijn verzameld



Onderscheppen van, pogingen tot, of succesvol binnendringen van een draadloos netwerk kan worden herkend aan:

- Toename van het draadloze netwerkgebruik;
- Veel verstoringen (onderbrekingen) van draadloze verbindingen;
- Vreemde of foutief gespelde netwerknamen in de nabijheid (Basic Service Set Identifications of BSSID's);
- Sterke WiFi-netwerk-toegangspunten in de nabijheid;
- Aanwezigheid van een groot aantal wireless access points;
- Onbekende MAC-adressen met verbinding naar het toegangspunt;
- Onbekende systemen (hosts) of IP-adressen aanwezig op het netwerk.

Bluetooth

Mobiele apparatuur (telefoons, laptops) uitgerust met Bluetooth kunnen zo kwetsbaar zijn dat gegevens (ongemerkt) worden opgevraagd. *Bluesnarfing* is een techniek die misbruik maakt van tekortkomingen in de authenticatie en/of datatransfer-mechanismen van het Bluetooth-protocol. Hierdoor kunnen gegevens op het mobiele apparaat (telefoonboek, kalender) worden benaderd. Bij sommige apparaten kan zelfs uitgebreide toegang tot sms-berichten, mediabestanden en spraakfuncties worden verkregen.

Andere aanvallen richten zich op het verzenden van sms-berichten of het misbruiken van het apparaat om te bellen naar betaalde nummers of diensten waarvoor de aanvaller geld ontvangt.

Meer achtergrond bij de bescherming van mobiele (draadloze) apparatuur wordt gegeven in het document 'Beveiliging van mobiele apparatuur en gegevensdragers' (GOVCERT.NL, 03-2009).

Benodigde gegevens voor vaststelling

Voor het vaststellen van een gerichte draadloze cyberaanval is veel deskundigheid nodig. Alle afwijkende gedragingen van de computer kunnen een aanwijzing zijn, zoals onbekende meldingen van draadloze toegang (Service Set Identifier of SSID-namen) of in een firewall of IDS-log, trager wordende netwerkprestaties of foutmeldingen. De belangrijkste benodigde technische informatie is:

- een overzicht van de gedane constateringen en het tijdstip waaruit blijkt, of op basis waarvan wordt vermoed, dat er sprake is van een cyberincident;
- een technische beschrijving van het draadloze netwerk en -systemen;
- een lijst van fysieke locaties en netwerktoegangspunten;
- een netwerkoverzichtstekening en -segmentering;
- een overzicht van de actieve processen in het computergeheugen;
- logbestanden;
- informatie over firewalls en andere beveiligingsmaatregelen.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Ja.

Er is sprake van binnendringen wanneer een hacker toegangsrechten tot het draadloze netwerk op een onrechtmatige manier heeft verkregen. Onrechtmatig wil zeggen dat deze niet zijn toegewezen door de beheerder of eigenaar van het systeem aan de desbetreffende persoon, bijvoorbeeld wanneer de encryptie van de draadloze verbindingen is doorbroken.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.
Bij (poging tot) binnendringing in het draadloze netwerk, afluisteren van het netwerkverkeer of binnendringing van een Bluetooth-apparaat, zal vaak op het eerste gezicht het draadloze netwerk en -apparatuur normaal blijven functioneren. Wanneer de functionaliteit van het systeem wordt aangetast zodat een systeem niet bereikbaar is, is er sprake van stoornis. Dit is het geval bij jamming en ook als MAC- en IP-adressen worden vervalst (spoofing).

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Nee.
Met alleen binnendringing van het draadloze netwerk worden nog geen gegevens direct veranderd, gewijzigd, vernield of toegevoegd. Dit is wel het geval bij vervolghandelingen op het (draadloze) netwerk of binnengedrongen (mobiele) apparatuur.

Worden gegevens afgetapt of afgeluisterd? Ja.
Met het doorbreken van de beveiliging van de draadloze verbinding of het zich voordoen als een betrouwbaar toegangspunt, wordt toegang verkregen tot alle verzonden gegevens, die kunnen worden afgeluisterd en opgenomen.

Strafbaarheid
Het opzettelijk en wederrechtelijk (zonder toestemming) gebruiken van andermans draadloos netwerk is strafbaar onder artikel 138ab Sr. Hiervoor is niet vereist dat daadwerkelijk een beveiliging is omzeild. Ook onbeveiligde netwerken mogen niet gebruikt worden, voor zover uit enigerlei omstandigheid kan worden afgeleid dat de eigenaar niet wil dat anderen er gebruik van maken (bijvoorbeeld via een waarschuwingsbericht of door het gebruik van woorden als ‘privé’ of ‘geen toegang’ in het SSID).

Het kan zijn dat de dader, nadat hij is binnengedrongen, nog andere handelingen verricht, zoals het overnemen en voor zichzelf of een ander vastleggen van gegevens. In dat geval is sprake van een misdrijf op grond van artikel 138ab lid 2 Sr.

Geschiedt de cyberaanval door tussenkomst van een openbaar (draadloos) telecommunicatienetwerk en wordt er vervolgens verder gehackt, dan kan er sprake zijn van strafbaarheid op grond van artikel 138ab lid 3 Sr.

Als gevolg van het binnendringen in een draadloos netwerk kan een hacker *opzettelijk* dan wel door *schuld* een geautomatiseerd werk vernielen. In dat geval kan ook strafbaarheid op grond van de artikelen 161sexies en 161septies Sr bestaan. Voor strafbaarheid op grond van artikel 161sexies of 161sexies Sr is wel vereist dat één van de gevolgen genoemd in deze artikelen intreedt (stoornis in de uitvoering van een nutsdienst of openbaar telecommunicatienetwerk of telecommunicatiedienst, van gemeen gevaar voor goederen of diensten of levensgevaar).

Worden er nadat is binnengedrongen opzettelijk gegevens vernield, dan is dit expliciet strafbaar gesteld in artikel 350a lid 2 Sr. Als na het binnendringen in een geautomatiseerd werk door schuld gegevens worden vernield, dan kan artikel 350b Sr van toepassing zijn.

Brengt iemand nadat hij is binnengedrongen, een technisch hulpmiddel aan waardoor hij in staat wordt gesteld gegevens af te tappen en/of op te nemen van het draadloze netwerk, dan is deze situatie strafbaar onder artikel 139d Sr. Het direct aftappen van gegevens van het draadloze netwerk kan strafbaar zijn op grond van het aftappen en/of opnemen van gegevens (art.139c lid 1 Sr), tenzij het gaat om het opvangen van radiosignalen zonder bijzondere inspanning.

Als het draadloos netwerk wordt misbruikt om bijvoorbeeld gratis toegang te krijgen tot telecommunicatiediensten, zoals internet, is er sprake van telecomfraude (art. 326c Sr).

3.2.5 Password guessing

Wat is password guessing?
Bij password guessing wordt getracht om een geautomatiseerd werk binnen te dringen door raden en/of uitproberen van wachtwoorden. Soms worden willekeurige combinaties gebruikt, maar een gerichte aanval kan ook gebruik maken van vooraf verzamelde informatie van online sociale netwerken (OSN), zoals LinkedIn, Twitter, Facebook en Hyves.

Technische verschijningsvormen en herkenbaarheid
Technisch gezien verschilt password guessing niet van een normale (of mislukte) inlogpoging. Wel is bij password guessing vaak sprake van een enorme hoeveelheid wachtwoorden die in korte tijd worden ingevoerd met geautomatiseerde hulpmiddelen.
Daarnaast kan een aanvaller de aanval op grote schaal uitvoeren, waarbij wachtwoorden voor meerdere gebruikersaccounts tegelijkertijd worden uitgeprobeerd. De aanvaller kan hierbij lijsten met veelgebruikte woorden en termen als wachtwoord gebruiken (*dictionary* attack) of alle combinaties van toegestane tekens uitproberen (*brute-force*-aanval).
Een derde techniek gebruikt vooraf berekende *hash-waarden* van wachtwoorden, specifiek gericht tegen een bepaald platform, zoals Windows (*rainbow tables*). Een dictionary- of rainbow-tables-aanval kan zeer snel verlopen. Een brute-force-aanval duurt lang en wordt vooral gebruikt om minder makkelijke wachtwoorden te achterhalen.

Bij alle soorten aanvallen zullen veelvuldige (mislukte) inlogpogingen voorkomen in de logbestanden. Deze inlogpogingen kunnen gelijktijdig of binnen een korte periode aansluitend zijn uitgevoerd.

Als gevolg van het raden van wachtwoorden kunnen gebruikersaccounts worden geblokkeerd; de meeste systemen zijn ingesteld op een beperkt aantal keer een foutief wachtwoord kunnen invoeren. Er treedt een denial-of-service voor deze gebruikers op. Een toename in het aantal geblokkeerde gebruikersaccounts of van gebruikersaccounts die normaal niet worden gebruikt, kan duiden op een aanval via password guessing.

Benodigde gegevens voor vaststelling
De belangrijkste benodigde technische informatie voor het vaststellen van password guessing is:
- een overzicht van de gedane constateringen en het tijdstip waaruit blijkt, of op basis waarvan wordt vermoed, dat er sprake is van een cyberincident;
- de lokale beveiliging- en netwerklogbestanden;
- informatie over firewalls en andere beveiligingsmaatregelen.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling
Wordt er binnengedrongen? Ja.
Password guessing is een methode om binnen te dringen. Bij een geslaagde poging is er sprake van binnendringen in een geautomatiseerd werk.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.
Password guessing maakt gebruik van de normale toegangsbeveiligingsmechanismen van het geautomatiseerde werk. Er wordt niet direct een stoornis veroorzaakt. Echter, afhankelijk van de instellingen van het aangevallen geautomatiseerde systeem, kan een gebruikersaccount tijdelijk of permanent worden geblokkeerd, bijvoorbeeld na drie mislukte aanmeldingspogingen. Hiermee wordt de normale toegang voor de rechtmatige gebruiker of computerservice geblokkeerd en daarmee wordt een storing veroorzaakt in het geautomatiseerde werk.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Nee.
Er is geen sprake van vernieling, beschadiging of onbruikbaar maken van gegevens. Bij password guessing wordt een normale handeling uitgevoerd, namelijk er wordt geprobeerd in te loggen. Deze handeling wordt herhaaldelijk verricht om het wachtwoord te achterhalen. Pas na een geslaagde inlogpoging heeft een hacker de mogelijkheid om gegevens te vernielen, beschadigen of onbruikbaar te maken.

Worden gegevens afgetapt of afgeluisterd? Nee.
Proberen binnen te dringen via password guessing is geen vorm van afluisteren van gegevens.

Strafbaarheid
Kenmerkend voor password guessing is dat wordt getracht de beveiliging te doorbreken of om met een vals signaal wederrechtelijk binnen te dringen. Zijn er eenmaal wachtwoorden gevonden, dan kan dit tot binnendringen in een geautomatiseerd werk leiden.

Misbruik van een wachtwoord valt onder artikel 138ab lid 1 Sr. Door zich voor te doen als iemand anders (valse hoedanigheid) wordt immers de toegang tot het geautomatiseerd werk verkregen. Slechts wanneer als gevolg van password guessing daadwerkelijk ongeautoriseerd wordt binnengedrongen, is er sprake van computervredebreuk (art. 138ab Sr).

Systematisch wachtwoorden proberen kan, als het duidelijk is dat de dader de bedoeling heeft binnen te dringen in een computer, wel als een strafbare poging tot computervredebreuk worden vervolgd (art. 45jo 138ab Sr). Mogelijk kan verder onder artikel 139d lid 2 Sr het verwerven van het wachtwoord, met het oogmerk daarmee binnen te dringen in een geautomatiseerd werk, strafbaar zijn.

Het veroorzaken van toegangsbelemmering doordat herhaaldelijk foute wachtwoorden worden aangeboden zodat een gebruikersaccount uiteindelijk blokkeert, kan worden gezien als toegang tot of gebruik van een geautomatiseerd werk. Dit is, net als DoS-aanvallen, strafbaar onder artikel 138b Sr.

Op grond van artikel 139d lid 2 sub a Sr kan het ter beschikking stellen, vervaardigen of het anderszins voorhanden hebben van programmatuur waarmee password guessing mogelijk is, strafbaar worden gesteld.[47]

3.3 Websiteaanvallen

Er zijn verschillende vormen van inbraak of misbruik van websites op afstand via een openbaar telecommunicatienetwerk. Het doel kan sterk verschillen van bijvoorbeeld *hacktivisme* (demonstreren), onderscheppen van informatie (voor phishing of spionage), kopiëren van (klant)gegevens of het verbergen en aanbieden van illegale webcontent (kinderporno), producten en diensten via een anderzijds legitieme website.

47. De handel, verspreiding of verwerven van wachtwoorden en toegangscodes is niet strafbaar tenzij daarmee als oogmerk het binnendringen in een systeem (art.138ab Sr), het belemmeren van de toegang (art.138b Sr), of het afluisteren van gegevens (art.139c Sr) wordt gepleegd. Als het conceptwetsvoorstel 'versterking bestrijding computercriminaliteit' wordt ingevoerd, wordt het in bezit hebben en verspreiden, strafbaar (art.139e Sr).

3.3.1 Misbruik van een webproxy

Wat is een webproxy?

Een *proxy* is een server tussen de computer van een gebruiker en het systeem dat men wil benaderen. De proxy is een ‘tussenpersoon’ die de opdrachten namens de gebruiker uitvoert. Een proxy wordt normaal gebruikt om een bedrijfsnetwerk gecontroleerd toegang te geven tot het internet. Een *open proxy* staat verbindingen van willekeurige gebruikers (IP-adressen) toe, bijvoorbeeld voor e-mail, IRC-verkeer (Internet Relay Chat), FTP of HTTP/HTTPS-internetverkeer.

Via een webproxy kan een derde partij netwerkverkeer aanbieden aan andere computers, die de computer van de derde partij niet als oorspronkelijke afzender van het netwerkverkeer zien. In plaats daarvan zien de ontvangende computers de (bonafide) webproxy als afzender. Een open webproxy is in essentie een foutief geconfigureerde server of website die door iedereen kan worden gebruikt.

Een open proxy kan op verschillende manieren ingezet worden. Door het opzetten van zogenoemde *tunnels* is het mogelijk om netwerkverkeer via de proxy op een andere netwerkpoort door te laten sturen. Met deze techniek is het mogelijk om in één keer een grote hoeveelheid mail voor verschillende geadresseerden op verschillende locaties aan te bieden. Deze techniek wordt vaak gebruikt bij het versturen van spam.

Verder worden open proxies vaak gebruikt als springplank voor verdere activiteiten. Het netwerkverkeer dat door een proxyserver wordt doorgestuurd, lijkt immers van die proxyserver te komen. Alleen uit de logbestanden van de proxyserver zelf kan de oorspronkelijke bron nog achterhaald worden. Een open proxy (of meerdere proxies achter elkaar gekoppeld, een *proxy chain*) kan daardoor effectief worden misbruikt om weinig sporen achter te laten op het internet.

Het gebruiken van een open webproxy voor illegale doeleinden kan ervoor zorgen dat deze (tijdelijk) niet meer beschikbaar is voor normale doeleinden. Bijvoorbeeld wanneer een derde partij zulke grote hoeveelheden netwerkverkeer produceert dat de rechtmatige gebruikers van de server er geen gebruik meer van kunnen maken. In dat geval is er sprake van een denial-of-service.

Steeds vaker infecteren wormen en virussen een computer door een Trojaans paard te installeren dat als open webproxy of open mail-relay fungeert. Dan is er dus geen sprake van een foutief geconfigureerde server maar van een met opzet geplaatst programma dat als proxy dienst doet. Geïnfecteerde systemen kunnen dan misbruikt worden om netwerkverkeer te tunnelen of door te sturen.

Technische verschijningsvormen en herkenbaarheid

Een open webproxy accepteert en stuurt netwerkverkeer door buiten de vooraf (impliciet) gedefinieerde functie om. Een proxyserver zal over het algemeen alleen gebruikt mogen worden om netwerkverkeer van binnen naar buiten (naar derden) te accepteren. Zodra een server netwerkverkeer van derden naar andere derden afhandelt is er sprake van een open webproxy.

Benodigde gegevens voor vaststelling

Voor het vaststellen van misbruik van een systeem als open webproxy is de belangrijkste benodigde technische informatie:

- een technische beschrijving van het netwerk;
- een overzicht van de misbruikte servers;
- de lokale beveiligings- en netwerklogbestanden;
- informatie over firewalls en andere beveiligingsmaatregelen.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Mogelijk.

Ook als het systeem geen afdoende basisbeveiliging heeft, blijft het aanbieden van netwerkverkeer door een niet-geautoriseerde persoon aan de server, te kwalificeren als binnendringen. Een webproxy is normaal opgezet om specifieke netwerkverbindingen te faciliteren voor geautoriseerde gebruikers of voor specifieke doeleinden. Een proxy is door de eigenaar dus niet bedoeld om als netwerkrouter te dienen die ál het netwerkverkeer probeert door te sturen. In ieder geval is er sprake van binnendringen als de open proxy- functionaliteit (bijvoorbeeld als malware) opzettelijk en wederrechtelijk op een computer is geïnstalleerd door een kwaadwillende.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.

Afhankelijk van de hoeveelheid netwerkverkeer dat door open proxy wordt verstuurd, kan er stoornis in een geautomatiseerd werk optreden.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Mogelijk.

Een open proxy stuurt in feite alleen aangeboden gegevens door. Er is meestal geen invloed op de normale bestaande of verwerkte gegevens van het systeem. Wel kan er sprake zijn van onrechtmatig gegevens toevoegen aan het systeem waaraan de gegevens worden aangeboden.

Worden gegevens afgetapt of afgeluisterd? Nee.

De kwaadwillende misbruikt het systeem maar valt dit niet zozeer aan. Wordt er niet verder binnengedrongen in het systeem, dan zullen over het algemeen geen gegevens worden afgetapt.

Strafbaarheid

Als kan worden aangetoond dat opzettelijk en wederrechtelijk is binnengedrongen en gebruikmaakt van een open proxy, volgt strafbaarheid onder artikel 138ab lid 1 sub b Sr. Hierbij maakt het niet uit of en waar de schade zich voordoet. Er wordt met behulp van een vals signaal binnengedrongen in een open proxy.
Het doorbreken van een beveiliging is niet vereist. Wel had de indringer uit de omstandigheden moeten kunnen opmaken dat het niet de bedoeling was het systeem als webproxy te gebruiken. Dit kan echter ook op andere manieren dan met beveiligingsmaatregelen duidelijk zijn gemaakt.

Het onrechtmatig aanbieden van gegevens aan een computer via een open proxy zal, als deze gegevens in de computer worden opgenomen of verwerkt, gekwalificeerd kunnen worden als gegevensaantasting (art. 350a lid 1 Sr). Als er schade ontstaat aan bedrijfsnetwerken of -servers kan dit eventueel civielrechtelijk worden verhaald.

Als de persoon de open relay misbruikt en hiermee een stoornis veroorzaakt in de uitvoering van een nutsdienst of openbaar telecommunicatienetwerk of telecommunicatiedienst, of met gemeen gevaar voor goederen of diensten, of levensgevaar, kan hij strafbaar zijn op grond van artikel 161sexies of 161sexies Sr. Hierbij moet dan wel worden aangetoond dat bijvoorbeeld spam wordt verstuurd waardoor de werking van een publiek netwerk of systeem wordt bemoeilijkt.

3.3.2 Defacing

Wat is een defacement?

Defacement van een website is het zonder toestemming veranderen, vervangen of vernielen van (het aangezicht van) een website. Defacing is een digitale vorm van vandalisme.

Er zijn twee manieren van defacing:

- Binnendringen in de webserver.
  Bij deze vorm van defacing wordt op afstand binnenge drongen in het systeem door bijvoorbeeld exploits, SQL-injectie of password guessing. Vervolgens wordt de website vernield of aangepast.
- Omleiding van internetverkeer (DNS-hack/name spoofing).
  Bij deze vorm van defacing wordt het internetverkeer doorgeleid naar een andere (malafide) website in plaats van de bonafide website.

Technische verschijningsvormen en herkenbaarheid

Defacing is in eerste instantie eenvoudig visueel te herkennen doordat er teksten, afbeeldingen of andere inhoud aanwezig is die niet in opdracht van de eigenaar zijn geplaatst.

Binnendringen in de webserver

Wanneer voor de vernieling of vervanging van een website wordt binnengedrongen, vindt meestal of een computerinbraak op afstand plaats (zie 3.2.3) of worden zwakke plekken misbruikt met exploits of bijvoorbeeld SQL-injectie. Voor defacement van een website is niet altijd toegang tot het systeem noodzakelijk. Het aanbieden van gemanipuleerde informatie kan voldoende zijn. Door bijvoorbeeld code te injecteren in invoervelden op een website zoals bij een discussieforum, kunnen eventuele kwetsbaarheden van een webapplicatie worden misbruikt om de inhoud van de website aan te passen of om toegang te verkrijgen tot het CMS (Content Management Systeem).

Om het defacement uit te voeren is informatie over de webserver nodig. Vooraf zal een aanvaller een vooronderzoek kunnen uitvoeren via footprinting en portscans. In dit voorbereidende stadium kunnen deze handelingen al worden herkend door firewalls en intrusion detection systems.

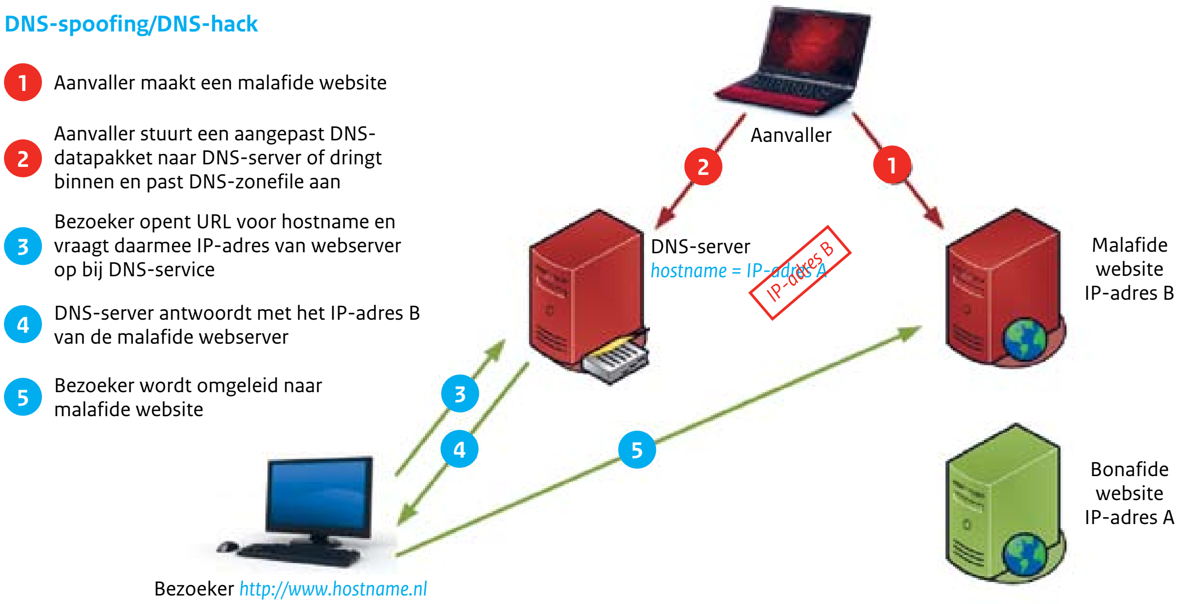
Een webserver bestaat uit statische of dynamische informatie en interactiemogelijkheden. Bij statische informatie wordt gebruik gemaakt van bestanden, waar de webcontent in is opgenomen. Deze bestanden worden als webpagina's aan de bezoeker van een website gepresenteerd. Bij defacement van een statische website zijn deze bestanden vervangen of aangepast door de hacker. Door bijvoorbeeld hash-waarden van originele bestanden te vergelijken met de actuele hash-waarden van bestanden kan dit worden herkend.

Bij een dynamisch gegenereerde website worden de gegevens opgeslagen in een database. Op verzoek van een bezoeker wordt een webpagina gegenereerd door een script, dat de content uit de database ophaalt en samenstelt tot een webpagina. Het script is opgenomen in een bestand op de webserver. De database kan zich op de webserver zelf of op een aparte databaseserver bevinden. Defacement van een dynamische website houdt in, dat het script op de webserver is aangepast of dat de inhoud in de database is aangepast.

Een website-defacement waarbij wordt binnengedrongen, kan worden herkend door:

- Het vergelijken van de website zelf via een webbrowser;
- Herkenning van inbraakpogingen aan de hand van firewall-logbestanden of een Intrusion Detection System (IDS);
- Logbestanden van de webserver;
- Datum van aanmaken, aanpassen of verwijderen van bestanden;
- Het vergelijken van de huidige bestanden met de originele bestanden. Dit kan gebeuren met behulp van een *fingerprint* (*checksum* of hash-waarden);
- Het vergelijken van de aanwezige informatie in de productiedatabase met die in een back-up-database.

DNS-spoofing/DNS-hack



Omleiding van internetverkeer (DNS-hack/name spoofing)
Website-defacement is ook mogelijk door verschillende manieren van DNS-spoofing/cache poisoning (zie 3.2.5). DNS zorgt voor een koppeling van de hostname aan een IP-adres. Bij een DNS-hack wordt door een DNS-server de hostname van de website gekoppeld aan een ander (malafide) IP-adres. Door de hostname zoals een websitebezoeker in een URL gebruikt naar een ander IP-adres te verwijzen, wordt de website niet meer bereikt op het oorspronkelijke IP-adres. De website is dus niet meer bereikbaar op basis van de hostname.
In sommige gevallen echter is de website nog wel rechtstreeks bereikbaar op het oorspronkelijke IP-adres. Dit is voor normale websitebezoekers niet te controleren, omdat zij niet het originele IP-adres van de website kennen. Ook de beheerder van de website die defaced is via DNS-hacking of DNS-spoofing, kan dit soort problemen niet altijd detecteren. De caching en/of root-name-server wordt namelijk niet per definitie door hem/haar beheerd.

Als gevolg van DNS-spoofing/cache poisoning zal het normale netwerkverkeer een ander patroon vertonen. Een bezoeker van de website wordt immers naar een ander (malafide) IP-adres omgeleid. Door deze routing komt het dataverkeer van de bezoeker dus niet aan op het netwerk waarop de webserver is aangesloten. De website ontvangt geen nieuwe bezoekers meer. Dit veroorzaakt een afname in het normale verkeerspatroon van de website.

Benodigde gegevens voor vaststelling
Voor het vaststellen van een defacement is de belangrijkste benodigde technische informatie:

- een overzicht van geplaatste of aangepaste bestanden met tijdstip van plaatsing/aanpassing;
- de code (string) die een aanvaller naar de website zendt of heeft gezonden;
- informatie over DNS en domeinregistratie;
- een technische beschrijving van het netwerk;
- een overzicht van de misbruikte servers;
- de lokale beveiligings- en netwerklogbestanden;
- informatie over firewalls en andere beveiligingsmaatregelen.

Als vermoed wordt dat de defacing plaatsvindt via DNS-aanpassingen of spoofing zijn bovendien gegevens van de DNS-server nodig, zoals de aanpassing van een A-record of de gewijzigde DNS-bestanden.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling
Wordt er binnengedrongen? Mogelijk.
Een hacker kan na toegang tot het systeem de website aanpassen. Echter bij defacement van een website is binnendringen in het systeem waarvan de webserver deel uitmaakt niet altijd noodzakelijk. Een hacker kan de inhoud van een website bijvoorbeeld aanpassen door malafide input te leveren via invulvelden op een website.

Bij een DNS-hack of DNS-name-spoofing wordt het defacement van een website op afstand uitgevoerd. Er wordt niet binnengedrongen op het systeem van de website. Er kan echter wel sprake zijn van binnendringen op het systeem van de DNS-server.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.
Als de inhoud van een website wordt aangepast, is er

sprake van beschadiging aan of stoornis van een website. Een bedrijf heeft een website opgezet met een bepaalde doelstelling. Als een hacker de website dusdanig aanpast zodat de website niet meer aan de doelstelling voldoet, is er sprake van een stoornis. Bij defacing is het veroorzaken van een stoornis van een geautomatiseerd werk meestal niet het primaire doel.

Als de cache van een DNS-server wordt vervuild of de DNS-zonefile wordt aangepast, is er sprake van beschadiging van de nameserver. De werking van de webserver wordt niet aangetast.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Ja.
Als de inhoud van een website wordt aangepast, is er sprake van beschadiging of vernieling van een website.

Bij een DNS-hack of DNS-name-spoofing worden de gegevens van de website niet aangetast. Alleen de gegevens die zich in de nameserver bevinden worden aangepast.

Worden gegevens afgetapt of afgeluisterd? Nee.
Meestal worden bij een defacement geen gegevens afgeluisterd. Een DNS-hack of DNS-name-spoofing heeft wel tot gevolg dat bezoekers van de website niet uitkomen op de oorspronkelijke website maar op een malafide website. Een hacker zou op deze manier wel informatie kunnen onderscheppen.

Strafbaarheid
Defacing is het zonder toestemming veranderen, vernielen of vervangen van een website. Dit is strafbaar gesteld op grond van het feit dat er sprake is van beschadiging van gegevens en/of manipulatie van gegevens (art.350a Sr).

Voordat websitegegevens kunnen worden gemanipuleerd zal vaak moeten worden binnengedrongen in het geautomatiseerde werk. Het zonder toestemming binnendringen in het geautomatiseerde werk is strafbaar gesteld in artikel 138ab Sr.

Hoewel niet gebruikelijk, kan als gevolg van defacing ook sprake zijn van computersabotage als een stoornis wordt veroorzaakt (art. 161sexies en 161septies Sr). Voor strafbaarheid op grond van artikel 161sexies of 161sexies Sr is wel vereist dat één van de gevolgen genoemd in deze artikelen intreedt (stoornis in de uitvoering van een nutsdienst of openbaar telecommunicatienetwerk of telecommunicatiedienst, van gemeen gevaar voor goederen of diensten of levensgevaar).

Defacing door een DNS-hack of name-spoofing zorgt voor doorleiden van internetverkeer naar een andere website. Hierdoor kan iemand verbinding krijgen met een andere website dan dat hij heeft aangeven. Hoewel in eerst instantie alle betrokken systemen normaal functioneren, worden onjuiste hostname/IP-adresgegevens verstrekt aan websitebezoekers. Dit kan strafbaar zijn op grond van de artikelen 138ab lid 1, 350a lid 1 en 350b lid 1 Sr. Weliswaar wordt niet direct een storing veroorzaakt bij individuele geautomatiseerde werken, maar wel wordt een stoornis veroorzaakt in het totale systeem, bestaande uit de computer van de websitebezoeker, openbare DNS-systemen en de te bezoeken bonafide website.

Zie voor de strafbaarheid van de DNS-hack paragraaf 3.2.5 bij domain-name-spoofing/cache poisoning.

3.3.3 SQL-injectie

Wat is SQL-injectie?
SQL-injectie is een aanvalstechniek waarbij via invoervelden op een website extra of aangepaste instructies worden opgegeven met als doel om de achterliggende database van een website bepaalde instructies te laten uitvoeren. Op deze wijze kan een aanvaller bijvoorbeeld ongeautoriseerd toegang krijgen tot de website, gegevens uit de database opvragen (zoals gebruikersnamen en wachtwoorden) of opdrachten door de website laten uitvoeren.

Webapplicaties maken vaak gebruik van databases voor het opslaan en oproepen van allerhande informatie. Structured Query Language (SQL) is de taal die elke database ondersteunt om toegang tot deze informatie mogelijk te maken. Elke database biedt de mogelijkheid om informatie uit de database op te vragen (SELECT), te verwijderen (DELETE) en te wijzigen (UPDATE). Daarnaast is het uiteraard mogelijk om nieuwe informatie aan de database toe te voegen (INSERT). Deze functionaliteiten vormen de basis van elke database.

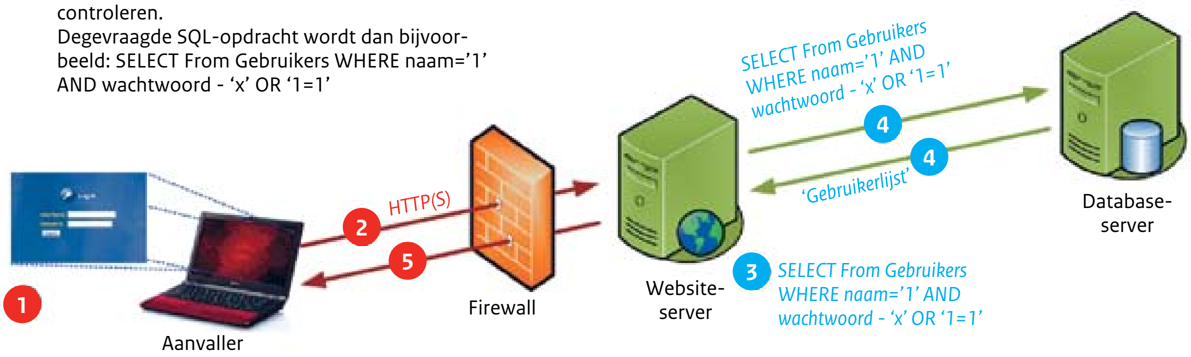
Vaak is het mogelijk om via de aanroep van in de database opgeslagen scripts *(stored procedures)* extra taken te laten uitvoeren zoals het versturen van e-mail. Sommige databases bieden zelfs de mogelijkheid om direct opdrachten en programma's op besturingsniveau aan te roepen.

SQL-injectie wordt veroorzaakt door onvoldoende controles op de invoer van gebruikersdata en onveilige programmeergewoonten. Is de kwetsbaarheid voor SQL-injectie aanwezig, dan kan een aanvaller op het internet SQL-verzoeken die een webapplicatie verstuurt naar de database manipuleren. Daarbij heeft de aanvaller vaak toegang tot het brede scala aan functionaliteiten dat de database biedt. De gevolgen van deze kwetsbaarheid zijn in grote mate afhankelijk van de programmalogica.

Technische verschijningsvormen en herkenbaarheid
Misbruik via SQL-injectie kan in de logbestanden worden teruggevonden. Dan is te zien of via HTTP GET- of HTTP

SQL-injectie

1. Kwaadwillende vult een webformulier in met aangepaste inhoud (zoals 'x' OR '1=1')
2. Het webformulier met aangepaste inhoud wordt opgestuurd naar de webserver
3. De webserver formuleert een SQL-opdracht (query) zonder de invoer van de gebruiker te controleren.
Degevraagde SQL-opdracht wordt dan bijvoorbeeld: SELECT From Gebruikers WHERE naam='1' AND wachtwoord - 'x' OR '1=1'
4. De SQL-opdracht wordt uitgevoerd op de database-server en het resultaat terug gemeld aan de webserver
5. Resultaat: alle gebruikers uit de tabel worden getoond



POST-opdrachten ongewenste informatie wordt meegestuurd. Kenmerken van pogingen tot SQL-injectie zijn:

- SQL-commando's zoals CAST, DECLARE, SELECT, WHERE in de communicatie;
- logische instructies in antwoordvelden die worden aangeboden aan de website
(zoals AND, OR, =, > operators);
- extreem lange waarden van een parameter, getypeerd door meer dan 500 karakters;
- de aanwezigheid van de keywords IFRAME en SCRIPT SRC in verschillende velden in de database.

Zie voor een uitgebreide toelichting de factsheet 'FS-2008-05 Massale SQL-injectie-aanvallen' (GOVCERT.NL, 23-06-2008).

Benodigde gegevens voor vaststelling

Vooral de logbestanden van de webserver, proxyserver en/of databaseserver zijn nodig, met hieruit de relevante gedeelten waarin de HTTP-verzoeken met geïnjecteerde data te vinden zijn. Daarnaast kunnen alle afwijkende gedragingen van de computer een aanwijzing zijn, zoals onbekende meldingen in een firewall/IDS-log, trager wordende prestaties (internetverbinding), foutmeldingen of veelvuldige storingen bij specifieke webapplicaties.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Mogelijk.

Door SQL-injectie worden onverwachte gegevens ingebracht op of aangeboden aan een webserver. Er worden gegevens verstuurd aan een webserver om te worden verwerkt, om zo zonder toestemming gegevens van de website te ontfutselen. Daarnaast wordt SQL-injectie bijvoorbeeld toegepast om met valse signalen of een technische ingreep de beveiliging van een systeem te omzeilen. Meestal is bij SQL-injectie sprake van een vorm van wederrechtelijk binnendringen.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.

Een webserver aangevallen via SQL-injectie kan onbedoeld opdrachten uitvoeren die stoornis veroorzaken in een geautomatiseerd werk, bijvoorbeeld doordat onderliggende procedures (commando's) worden gestart of omdat gegevens worden aangetast.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Ja.

Door SQL-injectie kunnen gegevens worden verwijderd, gewijzigd of toegevoegd. Het is bijvoorbeeld via SQL-injectie mogelijk om gegevens aan een database toe te voegen, te veranderen of te wissen.

Worden gegevens afgetapt of afgeluisterd? Nee.

Het is wel mogelijk door SQL-injectie ongeautoriseerd gegevens op te vragen en te kopiëren, zoals toegangsgegevens van gebruikers (overnemen van gegevens).

Strafbaarheid

Het aanbieden van een kwaadaardige code gebeurt bijna altijd met opzet, bijvoorbeeld door het aanbieden van een gemanipuleerd HTTP-verzoek aan een website. De dader wil binnendringen, gegevens overnemen of schade als gevolg van vernieling veroorzaken in het computersysteem of de gegevens in het computersysteem aantasten.

Als er eerst onrechtmatig gegevens moeten worden toegevoegd aan een database om meer rechten te kunnen krijgen om verdere acties te ondernemen, is artikel 350a lid 1 Sr van toepassing. Hierbij kan tevens sprake zijn van het overnemen van gegevens nadat is binnengedrongen in het geautomatiseerde werk (artikel 138ab lid 2 Sr).

3.4 Botnets

Botnets vormen een belangrijke infrastructuur voor cybercriminelen. Door botnets kunnen cybercriminelen anoniem opereren; hun identiteit wordt verborgen (via proxies), hun IP-adres en (fysieke) locatie wordt afgeschermd en hun aanvalsmogelijkheden en -bereik worden vergroot. Botnets kunnen flexibel worden ingezet voor verspreiding van malware, versturen van spam, DDoS-aanvallen, keylogging, identiteitsdiefstal of het omleiden van internetverkeer. In deze paragraaf worden specifieke technische aspecten en verschijningsvormen van botnets beschreven.

Wat is een botnet?

Een botnet is een netwerk van geïnfecteerde computers *(bots of zombies)* die op afstand kunnen worden bediend door een cybercrimineel. Botnets zijn grootschalige en wereldwijde netwerken opgebouwd uit autonoom functionerende bots. De cybercrimineel misbruikt de rekencapaciteit en netwerkfunctionaliteit van de bots voor eigen doeleinden en gewin. De cybercrimineel die een botnet bedient wordt wel *botnet herder* genoemd. Botnet herders bieden vaak hun diensten ook aan andere criminelen aan.

De besturing vindt meestal plaats vanuit een *Command & Control-server* (C&C-server). Dit kan een legale server zijn die onder valse voorwendselen wordt gebruikt, maar het kan ook een systeem zijn waarop de botnet herder heeft ingebroken. Commando's worden gegeven via IRC (Internet Relay Chat) of HTTP.

Andere vormen van botnets zijn minder hiërarchisch en kunnen bijvoorbeeld worden bestuurd via peer-to-peer-netwerken (P2P) of door berichten geplaatst op legitieme websites (web 2.0). Via nieuwe decentrale aansturingmethoden en fast-flux-technieken, waarbij de hostnamen of IP-adressen van de C&C-servers snel wijzigen om deze te beschermen tegen uitschakelen, wordt het opsporen bemoeilijkt.

Technische verschijningsvormen en herkenbaarheid

De bots of zombies ontstaan doordat computers worden geïnfecteerd met malware die de geïnfecteerde computer deel laat uitmaken van een botnet. Deze besmetting kan plaatsvinden via virussen, besmette usb-sticks, e-mailberichten, besmette websites en downloads of social engineering. De besmetting kan in twee stappen verlopen: eerst wordt een computer geïnfecteerd, vervolgens wordt de botnet-software gedownload en geactiveerd.

Naast de al beschreven vormen van malware-herkenning kunnen geïnfecteerde computers worden opgemerkt door de soort netwerkactiviteit. Botnets bestuurd via IRC hebben een (permanente) verbinding met een C&C-server over TCP-poorten die liggen tussen 6665 tot 6669 (standaard-IRC-poorten). Met een netwerk-sniffer of in firewall-logbestanden kan dit eenvoudig worden gesignaleerd. De gebruikte datapakketten zijn meestal erg klein. De verbinding zal over het algemeen worden opgezet vanuit de bot die staat te wachten op instructies van de C&C-server.

HTTP-bestuurde bots zijn moeilijker te herkennen omdat dit verkeer over TCP-poort 80 gaat, die ook voor het normale internetverkeer wordt gebruikt. Door te kijken naar proces- en netwerkpoortkoppelingen kan worden geanalyseerd welke programma's allemaal luisteren naar poort 80. Verdachte netwerkverbindingen zijn bijvoorbeeld connecties naar sociale netwerksites zoals MSN of Twitter vanaf computers die daar geen reden toe hebben. Een rootkit zal echter nog steeds aan deze controle ontglippen.

P2P-bestuurde botnets zijn lastig te analyseren. Iedere bot is daarin zowel bot als C&C-server. Deze botnets zijn moeilijk uit te schakelen; een centrale C&C-server ontbreekt. Een enkele P2P-standaard bestaat niet. Toch kan een geïnfecteerde computer nog steeds aan de hand van verdacht netwerkverkeer worden herkend. In een P2P-botnet zal een bot veel verschillende connecties vertonen naar andere IP-adressen buiten het eigen netwerk.

Andere vormen van besturing kunnen worden herkend aan verdachte *instant messaging*-communicatie, zoals MSN of ICQ.

Benodigde gegevens voor vaststelling

Voor het vaststellen of een computer deel uitmaakt van een botnet zijn dezelfde gegevens nodig als voor malware of een Trojaans paard. Daarnaast kunnen alle afwijkende gedragingen van de computer een aanwijzing zijn, zoals onbekende meldingen in een firewall/IDS-log, trager wordende prestaties (internetverbinding), foutmeldingen of veelvuldige storingen bij specifieke applicaties.
De belangrijkste benodigde technische informatie is:

- een overzicht van de gedane constateringen en het tijdstip waaruit blijkt, of op basis waarvan wordt vermoed, dat er sprake is van een botnet-infectie;
- een technische beschrijving van de getroffen systemen;
- een lijst van geïnstalleerde programmatuur;
- een lijst van gewijzigde computerbestanden;
- een overzicht van de actieve processen in het computergeheugen;
- logbestanden;
- informatie over aanwezige firewall- en antivirusmaatregelen.

Voor het technisch onderzoek is het ook wenselijk om te beschikken over een dump van het netwerkverkeer, een overzicht van netwerkverbindingen vanaf het systeem en geïsoleerde bestanden die tot het botnet behoren. Voor de analyse kan het bovendien waardevol zijn als er een image van het schone systeem is vóórdat deze werd geïnfecteerd, en een image van het gecompromitteerde systeem.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Ja.

Op de geïnfecteerde computers, de bots, is binnengedrongen. Dit geldt zeker voor de persoon die in contact staat met de malware en deze opdrachten geeft met het doel om instructies op de computer uit te laten voeren of deze aan te sturen. Ook bij de C&C-server zal een vorm van binnendringen kunnen voorkomen als de C&C-server een misbruikt systeem is.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.

Stoornis wordt veroorzaakt wanneer de beschikbare rekencapaciteit en netwerkfunctionaliteit van de geïnfecteerde computer, die nu onderdeel is van een botnet, wordt misbruikt. Als hierdoor het geautomatiseerde werk niet of langzamer zijn eigenlijke taken kan uitvoeren, wordt een stoornis veroorzaakt.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Ja.

Gegevens op een bot worden veranderd, gewijzigd of vernield. Is een botnet een Trojaans paard, dan zal deze dit niet zonder meer doen omdat het onopgemerkt wil blijven. Wel is er altijd sprake van onrechtmatig toevoegen van gegevens aan geïnfecteerde computers.

Worden gegevens afgetapt of afgeluisterd? Ja.

Sommige botnets dienen om ingevoerde gegevens op de computer ongeautoriseerd te kunnen kopiëren, door te sturen en te misbruiken. Met name identiteits-, account/wachtwoord-, bank- en creditcardgegevens zijn doelwit. Daarnaast kunnen bots worden ingezet om het lokale netwerkverkeer af te tappen.

Strafbaarheid

Het infecteren met een Trojaans paard of andere malware valt onder art. 350a lid 1 Sr, omdat het gaat om onrechtmatig gegevens toevoegen aan een computer. Ook valt het verspreiden van malware onder art. 350a lid 3 Sr, ongeacht of daadwerkelijk een computer is geïnfecteerd en onderdeel van een botnet wordt.

Als gegevens worden afgeluisterd die worden overgedragen binnen het computersysteem (input van toetsenbord naar computer) of binnen het computer- of telecommunicatienetwerk waarmee de geïnfecteerde computer is verbonden, is dit strafbaar onder artikel 139c, eerste lid Sr, het aftappen en/of opnemen van gegevens.

Het wederrechtelijk op afstand bedienen en het laten uitvoeren van instructies op een geïnfecteerde computer is strafbaar gesteld als binnendringen in een geautomatiseerd werk (art. 138ab lid 1 Sr). Als het botnet wordt gebruikt voor het overnemen of verzamelen van gegevens, is sprake van een misdrijf op grond van artikel 138ab lid 2 Sr. Als de bot wordt gebruikt als springplank om verder te hacken op een ander systeem van een ander slachtoffer, is sprake van een misdrijf op grond van artikel 138ab lid 3 Sr.

3.5 Denial of Service

Een *DoS-aanval* wordt regelmatig ingezet uit baloriheid of wraak of als actiemiddel in (gecoördineerde) digitale protesten en zelfs rellen. De gevolgen en schade kunnen aanzienlijk zijn, afhankelijk van de diensten die als gevolg (tijdelijk) niet beschikbaar zijn.
Deze paragraaf beschrijft verschillende technische aspecten van (distributed) denial-of-service-aanvallen, in het bijzonder aanvallen die via een computernetwerk verlopen.

Wat is een DoS?

Bij een DoS-aanval wordt een computer- of netwerksysteem dusdanig zwaar belast of gemanipuleerd, dat dit systeem uitgeschakeld wordt of dat een aangeboden (internet)dienst niet meer beschikbaar is voor legitieme gebruikers. Denial of service kan ook ontstaan door stelselmatig foutieve gegevens aan te bieden, waardoor de beveiligingsinstellingen van een systeem zelf ervoor zorgen dat het systeem preventief wordt geblokkeerd om verdere schade te voorkomen. Bijvoorbeeld door bewust foute wachtwoorden aan te bieden kan een gebruikersaccount na een aantal keer worden geblokkeerd. Ook Network Intrusion Prevention Systems kunnen worden misleid om zo zelf de netwerkverbinding af te sluiten.

Wat is een DDoS?

Hoewel een DoS-aanval vanaf een computernetwerk kan worden geïnitieerd vanaf een enkel systeem, worden de meeste aanvallen tegenwoordig gecoördineerd vanaf meerdere systemen tegelijkertijd. Dit zijn zogenoemde *Distributed Denial of Service-aanvallen* (DDoS). De computersystemen die de DDoS-aanval uitvoeren zijn vaak misbruikte systemen van onschuldige slachtoffers in een botnet. De botnet herder geeft aan de geïnfecteerde systemen (bots) de opdracht om een bepaald doelwit aan te vallen.

Bij digitale protestacties komt het ook voor dat sympathisanten hun computer bewust aanbieden om te worden opgenomen in een netwerk van waaruit DDoS-aanvallen worden afgevuurd.

Het document 'Aanbevelingen ter bescherming tegen Denial of Service-aanvallen' van GOVCERT.NL geeft verschillende aanbevelingen om de weerstand tegen (D)DoS-aanvallen te verbeteren (GOVCERT.NL, 02-2005).

Technische verschijningsvormen en herkenbaarheid
Een (D)DoS-aanval wordt vaak als eerste herkend doordat een systeem traag wordt of in het geheel niet meer werkt. Zo kan het oneigenlijk gebruik van resources op een systeem leiden tot een denial of service. Een DoS is bijvoorbeeld excessief gebruik van een legitiem internet protocol, zoals het opzetten van uitzonderlijke grote hoeveelheden TCP-sessies. Een andere (onbedoelde) mogelijkheid is dat een hacker een FTP-server met publieke toegang misbruikt om illegale bestanden te plaatsen. Dit kan zoveel netwerkverkeer veroorzaken dat legitieme gebruikers geen toegang meer kunnen krijgen.

Algemene verschijningsvormen van denial of service zijn:
- een netwerk overspoelen met dataverkeer;
- connecties tussen twee systemen verbreken;
- een gebruiker de toegang tot een systeem weigeren;
- een service op een systeem onderbreken.

Denial of service komt in vele vormen voor. Een aantal basiselementen zijn:
1. Consumptie van schaarse, gelimiteerde resources;
2. Flooding (dichtslibben van netwerkverbindingen);
3. Vernieling of beschadiging van configuraties;
4. Fysieke vernieling of beschadiging van systemen.

1. Consumptie van schaarse, gelimiteerde resources
Een computersysteem functioneert door gebruik te maken van resources zoals rekencapaciteit (CPU), netwerkbandbreedte, (disk-)opslag- of geheugencapaciteit. Een aanvaller kan misbruik maken van de resources op het systeem, waardoor het zelf hier onvoldoende over kan beschikken. Het gevolg is dat het systeem crasht of niet meer bereikbaar is.

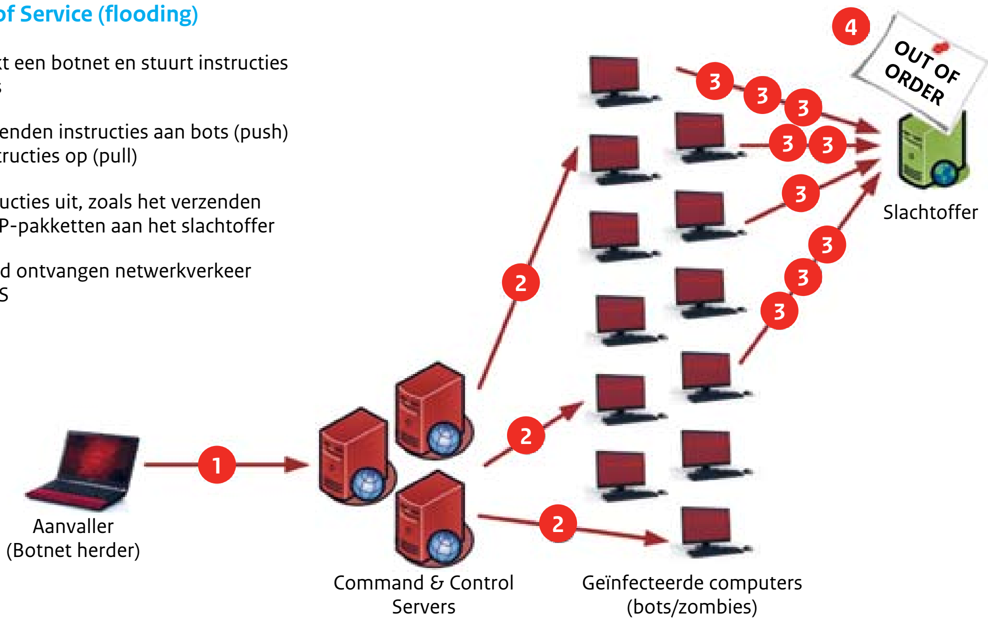
Het misbruiken van resources kan het gevolg zijn van aanvallen over het netwerk. Deze kunnen ook ontstaan door lokaal misbruik van resources via aanwezige malware. Het is zelfs mogelijk dat een deel van de resources op 'normale wijze' worden gebruikt door een aanvaller als onderdeel van een botnet. Bijvoorbeeld als er ongeldige instructies aan het doelsysteem worden gegeven zodat een buffer overflow ontstaat.

2. Flooding
Vrijwel alle computersystemen zijn afhankelijk van, of leveren hun diensten via, een computer- of telecommunicatienetwerk. Bij flooding worden deze verbindingen overspoeld met dataverkeer zodat de netwerkverbindingen dichtslibben. Normaal legitiem dataverkeer kan het systeem niet meer bereiken en komt dus niet of onvoldoende snel meer door. De meeste moderne computernetwerken en besturingssystemen zijn tegenwoordig voldoende beschermd tegen 'klassieke' vormen van flooding.

Voorbeelden waarbij netwerkverbindingen worden overspoeld of resources van een systeem via het netwerk oneigenlijk gebruikt worden:
- SYN-aanval;
- ICMP-aanvallen;
- Syslog-aanval;
- E-mail bombing;
- DNS-amplification.

Distributed Denial of Service (flooding)

1. Aanvaller gebruikt een botnet en stuurt instructies naar C&C-servers
2. C&C-servers verzenden instructies aan bots (push) of bots halen instructies op (pull)
3. Bots voeren instructies uit, zoals het verzenden van aangepaste IP-pakketten aan het slachtoffer
4. Grote hoeveelheid ontvangen netwerkverkeer veroorzaakt DDoS



2.1. SYN-aanval

Een SYN-aanval of SYN-flood maakt misbruik van het TCP-synchronisatieproces dat gebruikt wordt voor het opzetten van TCP-sessies (zie 3.2.4). Bij een SYN-aanval wordt een zeer grote hoeveelheid SYN-pakketten naar een doelsysteem (host) gestuurd. De source-IP-adressen van zulke SYN-pakketten zijn vaak onherkenbaar gemaakt om de afzender te verbergen. Het aangevallen doelsysteem stuurt voor elk SYN-pakket een SYN/ACK-pakket terug en reserveert geheugen voor de verwachte TCP-communicatiesessie. Vervolgens wacht het doelsysteem op de ACK-pakketten. Deze komen echter nooit terug omdat het afzender-IP-adres niet bestaat (spoofing) of omdat het systeem op het afzender-IP-adres het SYN/ACK-pakket niet herkent.

Een grote hoeveelheid ontvangen SYN-pakketten kan ertoe leiden dat het doelsysteem geen geheugen meer beschikbaar heeft voor andere actieve processen of netwerkverbindingen op het systeem. Dit heeft tot gevolg dat het systeem onbereikbaar is, nieuwe legitieme TCP-sessies niet meer worden geïnitieerd of dat het aangevallen systeem zelfs geheel stopt met functioneren (crasht).

Een SYN-aanval is te herkennen aan deze technische eigenschappen:

- Een host ontvangt een abnormale hoeveelheid SYN-pakketten (binnen korte tijd), afkomstig van één of meerdere IP-adressen.
- Een host ervaart een toename in hoeveelheid netwerkverkeer.
- De gemiddelde pakketgrootte neemt af bij de host doordat verbindingen worden opgezet maar uiteindelijk geen data worden uitgewisseld.

2.2. ICMP-aanvallen

Een ICMP-aanval maakt misbruik van ICMP-pakketten die oorspronkelijk bedoeld zijn om diagnostische berichten tussen systemen uit te wisselen. Bij een ICMP-aanval wordt een netwerk simpelweg overspoeld met ICMP-pakketten. Een voorbeeld van een ICMP-aanval is de (ouderwetse) *smurf-aanval*, waarbij gebruik wordt gemaakt van een *directed broadcast* (gestuurde zending). Door een directed broadcast kan een ICMP-pakket worden verstuurd naar het broadcast-adres van een ander IP-netwerksegment *(subnet)*.

Een aanvaller kan in het ICMP-pakket een gespooft source-IP-adres gebruiken voor het aan te vallen doelsysteem of om de afzender te verbergen. Alle systemen (hosts) op het subnet van het broadcast-IP-adres zullen een ICMP-*echo-reply*-pakket terugsturen naar het source-IP-adres. Het gevolg is dat het source-IP-adres wordt overspoeld met een overweldigende hoeveelheid netwerkverkeer.

Een ICMP-aanval is te herkennen aan deze technische eigenschappen:

- Een host ontvangt een abnormale hoeveelheid ICMP-pakketten (binnen korte tijd), afkomstig van een of meerdere IP-adressen.
- De gemiddelde pakketgrootte neemt af bij de host;
- Openstaande connecties van de aangevallen host worden onderbroken.
- De netwerkrouter die het aangevallen subnet verbindt met andere netwerken (zoals het internet) ontvangt ICMP-echo-request-pakketten van een of meerdere systemen die zich buiten het eigen subnet bevinden.

2.3. DNS-amplification-aanval

Een DNS-amplification-aanval is een distributed denial of service waarbij *recursive DNS name servers* worden misbruikt door vervalste (spoofed) netwerkpakketten. Recursieve DNS-servers zijn nodig voor het functioneren van het internet. Recursieve DNS-servers accepteren verzoeken van andere systemen om IP-adressen op te zoeken. Deze verzoeken worden doorgestuurd naar andere DNS-systemen, die het gevraagde antwoord wel kunnen geven of het gevonden antwoord terugsturen naar de afzender.

Bij een DNS-amplification-aanval neemt de omvang van het datapakket enorm toe na het verzonden DNS-antwoord of door de doorverwijzing naar een ander DNS-systeem. Hierdoor degraderen de beschikbare netwerkbandbreedte en de capaciteit van het DNS-systeem.
De originele DNS-verzoeken van de aanvaller bestaan uit enkele kleine datapakketten, het antwoord kan wel een factor 73 groter zijn. Als gevolg van de aanval ontvangt het slachtoffer (wiens IP-adres is vervalst in het DNS-verzoek) een grote hoeveelheid datapakketten die afkomstig zijn van legitieme DNS-servers. De identiteit van de aanvaller blijft afgeschermd.
Eventueel kan ook de DNS-service zelf (tijdelijk) niet meer functioneren en zullen de domeinen en hostnames die via deze DNS-server worden gekoppeld aan IP-adressen, niet meer eenvoudig te bereiken zijn voor gebruikers (Randal Vaughn, 17-03-2006).

3. Vernieling of beschadiging van configuraties

Systemen die niet goed zijn geconfigureerd kunnen niet goed functioneren. Hackers kunnen configuraties van systemen beschadigen of vernielen waardoor het systeem niet meer kan functioneren. De methodieken van vernieling of beschadiging variëren heel sterk en kunnen daarom onmogelijk allemaal worden beschreven. Veel voorkomende vormen zijn het aanpassen van host-tabellen (lokale koppelingen van logische hostnames naar IP-adressen) of het wijzigen of besmetten met valse informatie van routingstabellen (bijvoorbeeld waar zich verschillende subnetten bevinden en hoe netwerkdatapakketten daarnaar verzonden worden).

4. Fysieke vernieling of beschadiging van systemen
Uiteraard zal een (opzettelijke) fysieke beschadiging of loskoppeling van het computernetwerk ook tot onbeschikbaarheid van het systeem kunnen leiden en dus een denial of service veroorzaken. Echter worden deze niet meer onder de noemer van cybercrime in enge zin beschouwd.

Benodigde gegevens voor vaststelling
Voor het vaststellen van een netwerk-gebaseerde (D)DoS is de belangrijkste benodigde technische informatie:
- een overzicht van de gedane constateringen en het tijdstip waaruit blijkt, of op basis waarvan wordt vermoed, dat er sprake is van een (D)DoS-aanval;
- een technische beschrijving van de getroffen systemen;
- een netwerkoverzichtstekening;
- logbestanden van de verschillende netwerkcomponenten waarlangs de aanval heeft plaatsgevonden, zoals routers, proxies en firewalls;
- logbestanden van de getroffen systemen;
- informatie over aanwezige firewall- en antivirus-maatregelen.

Met name de begin- en eindtijd(en), source-IP-adressen, destination-IP-adres, een overzicht van de hoeveelheid netwerkverkeer en (netwerk)connecties in de tijd, gebruikte netwerkpoorten en netwerkdatapakketten gebruikt voor de aanval zijn waardevol.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling
Wordt er binnengedrongen? Nee.
Bij een (D)DoS wordt het aangevallen systeem overbelast, waardoor mogelijk gegevens beschadigd of vernietigd worden. Voor een (D)DoS aanval wordt niet getracht binnen te dringen op het doelsysteem. Uiteraard is er wel sprake van binnendringen bij het via een C&C-server aansturen van de zombiesystemen in een botnet die gebruikt worden om de daadwerkelijke (D)DoS-aanval uit te voeren.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Ja.
Het geautomatiseerde werk wordt (in ieder geval tijdelijk) onbruikbaar gemaakt voor zijn oorspronkelijke doel. Daarnaast kan er ook vernieling of beschadiging optreden.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Nee.
Bij een (D)DoS-aanval kunnen als gevolg gegevens gewijzigd of vernield worden of resulteert de aanval in het vastlopen van het getroffen systeem (system crash). Dit is echter een gevolg van de DoS-aanval en niet van de handeling zelf.

Worden gegevens afgetapt of afgeluisterd? Nee.
Een (D)DoS-aanval neemt geen gegevens over en luistert geen dataverkeer af van het aangevallen doelsysteem.

Strafbaarheid
Een (D)DoS-aanval is in eerste instantie strafbaar onder artikel 138b Sr. Een (D)DoS kan tevens leiden tot beschadiging van gegevens verwerkt of opgeslagen door het geautomatiseerde werk, wat strafbaar is op grond van artikel 350a Sr.

Als de (D)DoS-aanval een stoornis in de gang of werking veroorzaakt bij computers of netwerken met een publieke functie, waarbij ook sprake is van een openbaar belang (stoornis in de uitvoering van een nutsdienst of openbaar telecommunicatienetwerk of telecommunicatiedienst), van gemeen gevaar voor goederen of diensten of levensgevaar, is dit ook strafbaar onder artikel 161sexies.

3.6 Social engineering

3.6.1 Phishing
Phishing is een vorm van (internet)fraude waarbij cybercrime wordt gecombineerd met technieken om mensen te verleiden tot het afstaan van persoonlijke gegevens (social engineering). Bij het ontfutselen van persoonlijke informatie (naam, geboortedatum, BSN, bank- en creditcardgegevens, inlogcodes) kunnen verschillende verschijningsvormen van cybercrime een rol spelen. De techniek die daarmee gemoeid is wordt in deze paragraaf beschreven.

Wat is phishing?
Phishing is een verzamelbegrip voor activiteiten die tot doel hebben bepaalde persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie wordt gebruikt voor verkrijgen van geld (bijvoorbeeld via een creditcard) of voor het stelen van iemands identiteit. In het laatste geval zijn gegevens als BSN, adressen en geboortedatum nodig. Soms wordt ook het ongemerkt installeren van Trojaanse paarden, zoals een keylogger, onder phishing geschaard. Zo'n keylogger slaat de toetsaanslagen van het slachtoffer op en geven deze aan een derde partij. De toetsaanslagen bevatten (de toegang tot) e-mailadressen, wachtwoorden, creditcardnummers en dergelijke.

Een *phisher* maakt meestal gebruik van een nagemaakte website van een bij het slachtoffer bekende organisatie en verleidt mensen om op deze website privé-gegevens in te voeren. *Phishing-scam* is bijvoorbeeld het in bulk verzenden van vervalste of besmette e-mailberichten of het lokken van mensen via populistische filmpjes of aantrekkelijke aanbiedingen. Bekende doelwitten zijn banken, online winkels en veilinghuizen.

Het succes van phishing is gebaseerd op techniek en vertrouwen, gecombineerd met een schaalvergroting die door het internet mogelijk wordt gemaakt. Phishing bestaat al een aantal jaar en komt steeds weer 'sterker' terug. De professionaliteit van de *phishers* neemt toe, zodat de phishingpogingen voor een leek steeds moeilijker van echt te onderscheiden zijn.

Phishing kent inmiddels veel verschijningsvormen. *Smishing* is een vorm van phishing via sms-berichten. Slachtoffers worden in een sms'je overgehaald om een betaald telefoonnummer te bellen of een bepaalde (kwaadaardige) website te bezoeken.

Vishing (of *spear-vishing*) is een variant van phishing waarbij het slachtoffer telefonisch wordt benaderd en niet via e-mail of websites (social engineering). Het slachtoffer wordt gebeld door een geautomatiseerd voice-message-systeem dat om persoonlijke gegevens vraagt en deze registreert. Vishing komt ook gecombineerd met phishing of Smishing voor: het slachtoffer ontvangt een e-mail of sms'je met het verzoek telefonisch contact op te nemen.

Technische verschijningsvormen en herkenbaarheid
Phishing speelt in op patronen in het gedrag van mensen. Gebruik van e-mail is een ingeburgerde manier van communiceren. Mensen worden direct benaderd via een vervalst e-mailbericht, dat op een vertrouwenwekkende manier is opgesteld. Technisch bekeken zijn dergelijke berichten niet anders dan normale e-mailberichten. Alleen uit de tekstuele inhoud blijkt dat het om een vervalst e-mailbericht gaat.
Andere vormen van phishing zijn computerinbraak op websites, open proxies/mail relays, spoofing, trojans en botnets. Ook het misleiden door aangepaste webadressen te tonen *(URL obfuscation)* wordt frequent toegepast (Ollmann, 2007).

De eerste uitdaging voor de phisher is om voorzieningen te creëren die nodig zijn voor de phishing-scam. Zo moeten e-mailberichten of websites worden nagemaakt. Daarnaast moet de vervalste website ergens worden geplaatst zonder dat hierbij de ware locatie of identiteit van de aanvaller te traceren is.
Ook de aftocht van de phishing-activiteit moet worden afgedekt, op een zodanige manier dat vertrouwelijke gegevens worden verzameld zonder zelf te worden ontdekt. Er moeten één of meerdere locaties *(dropzones)* worden gecreeerd waar de verzamelde gegevens kunnen worden opgeslagen, zodat de phisher er op een later tijdstip veilig gebruik van kan maken.

Kenmerken voor phishing zijn:
- onverwachte verzoeken tot het invullen van vertrouwelijke gegevens;
- verzoeken tot afstaan van vreemde combinaties van (persoonlijke) gegevens;
- de tekst bevat vreemde zinsconstructies of veel spelfouten;[48]
- e-mail afkomstig van onbekende afzender/organisatie;
- e-mail afkomstig van bekende personen met een ongebruikelijk onderwerp;
- e-mail-afzender (from) en -ontvanger (to) adressen zijn gelijk;
- e-mail met een antwoord (reply) e-mailadres naar een (gratis) openbare e-mail service, zoals Hotmail of Gmail;
- e-mail met verwijzingen (links) naar bekende bestandstypen (zoals .exe) maar met dubbele extensies;[49]
- een URL in de getoonde tekst (e-mail) komt niet overeen met de werkelijke URL;
- ontvangst van (veel) gelijksoortige spam-e-mailberichten.

Onderstaand staan voorbeelden hoe technieken als computerinbraak, web proxies, spoofing en botnets worden ingezet door phishers.

Computerinbraak
Bij de voorbereiding van en tijdens een phishing-scam kan op verschillende momenten sprake zijn van computerinbraak (hacking) om zo de benodigde voorzieningen voor het hosten van bijvoorbeeld nagemaakte websites of locaties voor het opslaan van de verzamelde gegevens te creëren. Phishers verbergen hun nepwebsite bijvoorbeeld op een bestaande bonafide webserver waarop is ingebroken. De door een phisher verzamelde gegevens worden meestal opgeslagen op een andere computer dan degene waarop de nepwebsite zich bevindt (drop zone). Ook hier zal vrijwel altijd misbruik worden gemaakt van gecompromitteerde systemen.

Phishers zullen *backdoors* willen installeren op gecompromitteerde systemen om zichzelf op een later tijdstip weer toegang te verschaffen. Op geïnfecteerde computers kan een rootkit worden aangebracht om te dienen als een open proxy/mail relay.

Open webproxy/open mail relay
De phisher kan tijdens zijn activiteiten misbruik maken van open webproxies of open mail relays om op die manier minder traceerbaar te zijn. De open mail relay verspreidt bijvoorbeeld e-mailberichten waarbij slachtoffers naar een nepwebsite worden geleid. Deze manier van e-mailen

48. Buitenlandse phishing-scams gebruiken vaak automatische vertaalprogramma's.
49. Windows platformen verbergen standaard de extensie van bekende bestandtypen en tonen alleen de bestandsnaam. Een uitvoerbaar bestand met als naam afbeelding.jpg.exe zal worden getoond als afbeelding.jpg en daardoor lijken op een verwijzing naar een normaal plaatje. Bij het openen van de link start in werkelijkheid echter de uitvoerbare programmacode waardoor het systeem wordt geïnfecteerd.

vertoont alle kenmerken van spam. Daarnaast kan een phisher via een open proxy verzamelde gegevens van slachtoffers van de nepwebsite af halen om de kans op detectie te verkleinen.

Spoofing

Bij alle vormen van een phishing-scam komt spoofing voor. Het doel van de phisher is om slachtoffers te misleiden en ze ertoe te verleiden persoonlijke gegevens op een nepwebsite af te geven. Hiervoor worden deze methoden toegepast:

- Het adres van de afzender van het e-mailbericht is vervalst om de e-mail legitiem te laten lijken.
- In het e-mailbericht zijn technieken gebruikt om te verhullen dat hyperlinks niet verwijzen naar de website van de echte organisatie maar naar de nepwebsite.
- De hyperlinks die naar de nepwebsite verwijzen gebruiken technieken om in de webbrowser van het slachtoffer te verhullen dat deze zich op de nepwebsite bevindt.
- De nepwebsite is zo opgezet dat deze in alle opzichten legitiem lijkt. Zo kan er gebruik zijn gemaakt van een beveiligde HTTPS-verbinding of van links naar de echte website als onderdeel van de nepwebsite.

Trojaans paard

Phishing kan ook plaatsvinden door direct met Trojaanse paarden (keyloggers) op geïnfecteerde computers gegevens af te luisteren en door te sturen naar een verborgen verzamelpunt. Hiervoor onderschept een phisher de vertrouwelijke communicatie tussen het slachtoffer en de legitieme website (man-in-the-middle). De phisher hoeft dan geen nepwebsite meer te maken, het verspreiden van de benodigde malware is voldoende. Phishing-aanvallen in combinatie met een man-in-the-middle-aanval, eventueel weggewerkt in verborgen bestanden van de webbrowser, leiden er toe dat zelfs transacties beveiligd met sterke authenticatie (two-factor) kunnen worden omzeild.

Botnets

Een botnet herder heeft meestal volledige controle over de geïnfecteerde computers. Hiermee kan een phisher het botnet inzetten om bijvoorbeeld door keyloggers vertrouwelijke gegevens te verzamelen. Een andere mogelijkheid is het netwerkverkeer met specifieke websites om te leiden via een systeem. De phisher verzamelt de vertrouwelijke gegevens.

Een cybercrimineel kan echter ook de verbinding omleiden naar een nepwebsite, de gegevens afvangen, deze meteen aanpassen om dan weer aan te bieden bij de legitieme echte website. Op deze manier kan de aanvaller direct transacties aanpassen en voordeel proberen te behalen.

Benodigde gegevens voor vaststelling

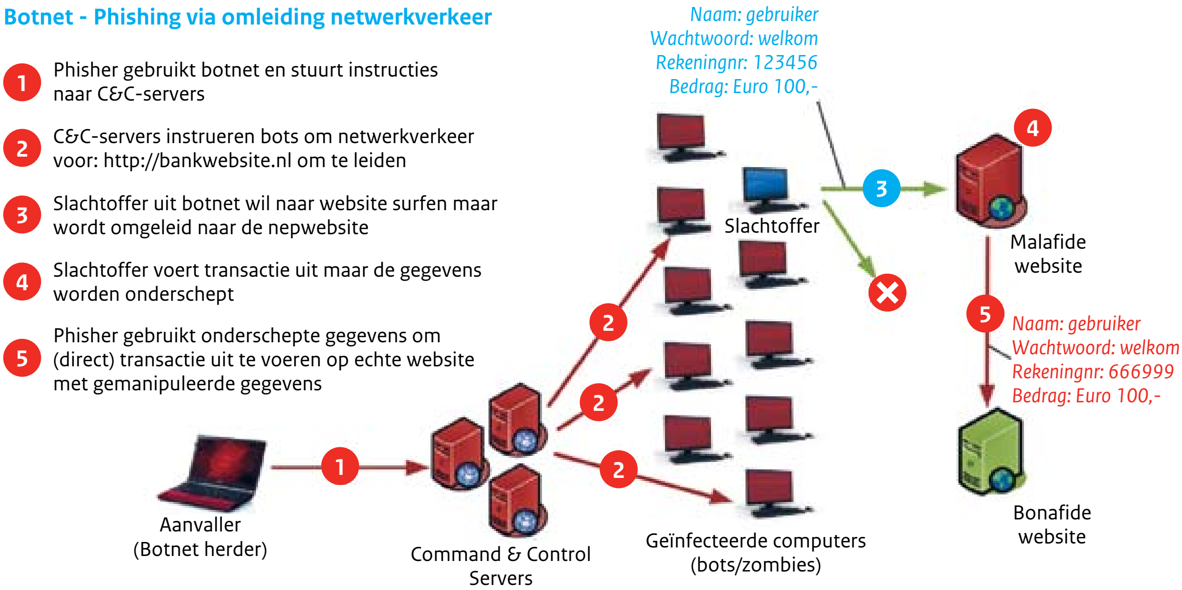
Alle afwijkende gedragingen van de computer kunnen een aanwijzing zijn, zoals onbekende meldingen in een firewall/IDS-log, trager wordende prestaties (internetverbinding), foutmeldingen of veelvuldige storingen bij specifieke webapplicaties. Voor het vaststellen van phishing is de belangrijkste benodigde informatie:

- naar welke informatie wordt 'ge-phished'?
- wat is het gevolg of mogelijke schade hiervan?
- de vervalste e-mailberichten;
- source-IP-adressen;
- e-mailadres van de afzender;
- een historie van bezochte websites of geopende links (URL's).

Daarnaast zijn logbestanden en overige informatie zoals die voor het vaststellen van malware.

Bijlage F geeft een uitgebreid overzicht van benodigde

Botnet - Phishing via omleiding netwerkverkeer



(technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Mogelijk.
Of wordt binnengedrongen is sterk afhankelijk van de gebruikte techniek. Wanneer alleen een vervalst e-mailbericht is ontvangen of de gebruiker is door eigen toedoen besmet geraakt met een Trojaans paard, is er niet binnengedrongen. Als het slachtoffer de link naar de phishing malware opent of op andere wijze deze activeert, is er sprake van binnendringen. Zeker als de phisher gebruik maakt van keyloggers of andere malware en hierbij direct contact heeft met de geïnfecteerde computers, is binnengedrongen (zie ook malware en Trojaanse paarden). Bij servers die misbruikt worden om nepwebsites te faciliteren of om gegevens te verzamelen is ook sprake van binnendringen.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.
Een phisher zal zoveel mogelijk onopgemerkt willen blijven. Het veroorzaken van een stoornis is duidelijk niet het doel. Hoewel het slachtoffer wordt omgeleid naar een nepwebsite is de werking meestal niet verstoord. Dit geldt ook wanneer de communicatie wordt onderschept of aangepast.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Mogelijk.
Hoewel gegevens kunnen worden vernield of gewijzigd, zijn de meeste phishing-aanvallen gericht op het aftappen van gegevens. Als een man-in-the-middle- of een botnettechniek wordt gebruikt waarbij de communicatie of het netwerkverkeer wordt onderschept en aangepast, dan is er wel sprake van het veranderen van gegevens. Bij sommige van deze technieken kan ook sprake zijn van onrechtmatig toevoegen van gegevens aan een computer.

Worden gegevens afgetapt of afgeluisterd? Mogelijk.
Het doel van iedere phishing-scam is vertrouwelijke gegevens te verkrijgen om daarmee fraude of oplichting te plegen. Dergelijke gegevens kunnen worden opgevangen door een computer te infecteren met malware en het slachtoffer te verleiden om gegevens in te voeren. Tijdens deze handeling worden de gegevens gekopieerd.
De malware op een besmette computer kan ook zijn ingericht om af te wachten totdat vertrouwelijk gegevens ergens worden ingevoerd of het slachtoffer wordt omgeleid via een malafide website. Bij de meeste van deze technieken is er geen sprake van het aftappen van ‘stromende’ *(streaming)* gegevens.

Strafbaarheid

Het met behulp van bijvoorbeeld een valse naam of hoedanigheid en bedrog iemand bewegen tot het ter beschikking stellen van gegevens, is strafbaar als oplichting onder artikel 326 Sr. Dit is het geval als een dader een listig verzoek uitstuurt en een slachtoffer er vervolgens op ingaat door gegevens aan te leveren. Als niemand reageert op een phishing-aanval, is er sprake van een strafbare poging tot oplichting, tenzij de aanval een volstrekt ondeugdelijk middel is (art. 45 jo. 326 Sr).

Phishing-aanvallen waarbij Trojaanse paarden zijn gebruikt zijn strafbaar als computervredebreuk (art. 138ab lid 1 Sr) en voor het overnemen van gegevens (art. 138ab lid 2 Sr) of het aftappen ervan (art. 139c Sr). Eventueel is, als wederrechtelijk verkregen gegevens zijn opgeslagen op een medium zodanig dat de aanvaller erover kan beschikken en deze voorhanden heeft, zoals op een harddisk in een (eigen) webserver, dit strafbaar onder artikel 139e lid 1 Sr. Zodra deze gegevens opzettelijk aan een ander bekend worden gemaakt, zoals bij het doorverkopen van gestolen identiteits- of creditcardgegevens, is deze activiteit strafbaar onder artikel 139e lid 2 Sr.

Als de gegevens verkregen via phishing worden gebruikt om een bankpas te vervalsen, is dit een misdrijf onder artikel 232 Sr. Dit artikel stelt het opzettelijk vervalsen van een betaalpas of een drager van identiteitsgegevens, bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties langs geautomatiseerde weg, strafbaar.

Phishing kan ook worden aangepakt via het merkenrecht.[50] Een merk is een teken om producten of diensten van een onderneming te onderscheiden. In de praktijk wordt 99% van de merken geregistreerd als woord- of beeldmerk (logo). In sommige gevallen kunnen kleuren of vormen ook een merk zijn. Producenten en bedrijven gebruiken het merk om aan te geven dat het van hen afkomstig is, om onderscheid aan te brengen met andere merken/producten en/of om een boodschap door te geven aan de consument. Na registratie mogen anderen het merk niet gebruiken zonder toestemming van de houder. Zij mogen ook geen vergelijkbare naam voeren, wanneer deze verwarring geeft met het beschermde merk. Bij een phishing-aanval wordt nu juist zo identiek mogelijk een website of andere kenmerken van een organisatie overgenomen om slachtoffers te misleiden.

3.7 E-mail-gerelateerde verschijningsvormen

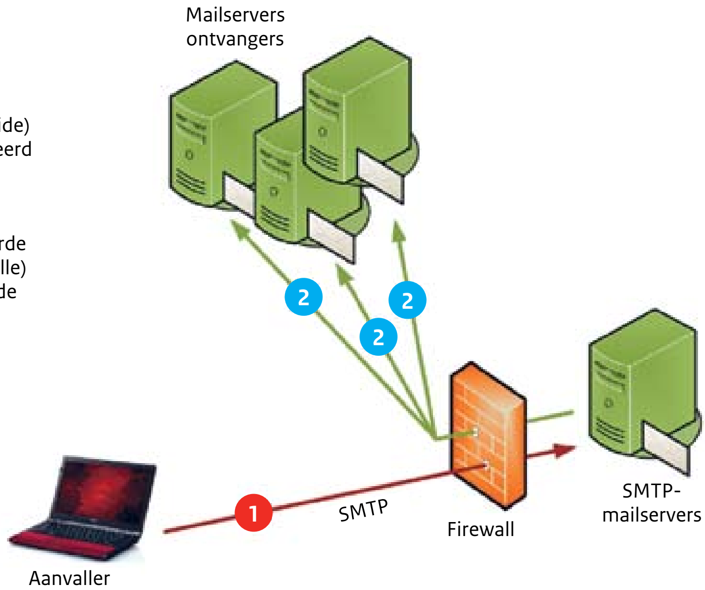
Misbruik maken van e-mailservers of slachtoffers lokken via e-mail zijn slechts enkele voorbeelden waarbij e-mail een rol speelt in cybercrime.
In deze paragraaf worden twee verschijningsvormen beschreven, mail relay en spam, waarvoor e-mailsystemen worden misbruikt.

50. In Nederland is het merkenrecht geregeld in het Benelux Verdrag inzake de Intellectuele Eigendom (BVIE). De merkbescherming geldt dus ook in België en Luxemburg. Daarnaast is de Europese en internationale regelgeving voor het merkenrecht van belang.

Open mail relay

1 Aanvaller stuurt SMTP-e-mailbericht naar (bonafide) mailserver maar met een bestemming gespecificeerd voor een ander e-maildomein

2 De (bonafide) mailserver herkent de gespecificeerde bestemming niet als zijnde voor hem en stuurt (alle) e-mailberichten door naar de mailserver(s) voor de gespecificeerde bestemming(en)



3.7.1 Misbruik van mail relay

Wat is mail relay?

Een *mail relay* is een e-mail-proxy-server die zich bevindt tussen de computer van een gebruiker en het systeem dat men wil benaderen. Via een open mail relay server kan een derde partij netwerkverkeer aanbieden aan andere computers, die de computer van de derde partij niet als oorspronkelijke afzender van het netwerkverkeer zien. Een open mail relay staat verbindingen van willekeurige gebruikers (IP-adressen) toe om e-mail naar anderen te versturen. Voor spam wordt op grote schaal misbruik gemaakt van open mail relay.

In essentie is een mail relay een foutief geconfigureerde server. Bij een open mail relay gaat het specifiek om e-mail-verkeer, verzonden over de SMTP-netwerkpoort 25 (Simple Mail Transfer Protocol).

Het gebruiken van een open mail relay voor illegale doel-einden kan ertoe leiden dat de mailserver niet of tijdelijk niet meer beschikbaar is voor normale doeleinden. Dit komt voor wanneer grote hoeveelheden e-mail worden verstuurd, zodat de rechtmatige gebruikers van de server dit niet meer kunnen. In dat geval is sprake van een denial of service.
Een open mail relay server kan op een zwarte lijst van inter-net service providers worden geplaatst (*blacklisting*). E-mail afkomstig van systemen op een zwarte lijst worden door veel ISP's of bedrijven niet meer geaccepteerd. De recht-matige eigenaar van het systeem kan zodoende effectief geen e-mail meer versturen.

51. Via de website http://www.abuse.net/relay.html kan een systeem direct vanaf het internet worden getest.

Technische verschijningsvormen en herkenbaarheid

Een open mail relay accepteert en stuurt e-mail van buiten-af door naar andere externe ontvangers. Normaal zullen e-mailservers alleen netwerkverkeer van buiten (van derden) naar binnen accepteren om via door hun beheerde domeinen e-mail te kunnen ontvangen. Zodra een server e-mail van derden naar derden afhandelt, is er sprake van een open mail relay.

Met enkele eenvoudige testen kan worden geverifieerd of een server als open mail relay misbruikt kan worden.[51]
Dit is het geval als (een combinatie van) de volgende soorten e-mail wordt geaccepteerd en verstuurd. De voorbeelden in deze lijst zijn slechts een deel van de mogelijkheden:

- mail waarvan het *from-* en *to-*adres hetzelfde zijn;
- mail waarvan het afzenderdomein niet bestaat;
- mail die vanuit het domein *local host* wordt gestuurd;
- mail zonder afzenderdomein;
- mail zonder afzenderadres;
- mail gestuurd als afkomstig van de ontvangende mailserver;
- mail met het IP-adres van de verzendende server tussen vierkante haakjes (in plaats van ronde);
- mail die gebruikmaakt van een doorverwijzing door het gebruik van het %-teken. Bijvoorbeeld *ontvanger%server.com@relayserver.com* wordt doorgestuurd naar *ontvanger@relayserver.com*;
- mail met het ontvangstadres tussen dubbele aanhalings-tekens;
- mail met het ontvangstadres in inverse notatie. Bijvoorbeeld *@relayserver.com:ontvanger@server.com* wordt doorgestuurd naar *ontvanger@server.com*;
- mail met het ontvangstadres in inverse notatie (variant). Bijvoorbeeld server.com!ontvanger wordt doorgestuurd *naar ontvanger@server.com*.

Benodigde gegevens voor vaststelling

Voor het vaststellen van misbruik van een systeem als open mail relay is de belangrijkste benodigde technische informatie:

- een overzicht van de gedane constateringen en het tijdstip waaruit blijkt, of op basis waarvan wordt vermoed, dat er sprake is van een cyberincident;
- e-mailberichten en/of de headers daarvan;
- een technische beschrijving van het netwerk;
- een overzicht van de misbruikte servers;
- de lokale beveiligings- en netwerklogbestanden;
- informatie over firewalls en andere beveiligingsmaatregelen.

Wanneer er sprake is van een open mail relay zijn de e-mailheaders en het complete e-mailbericht belangrijk. Uit de e-mail-headers kan worden opgemaakt welke mailserver is gebruikt als relay. Deze gegevens kunnen ook gedeeltelijk uit logbestanden van de ontvangende mailserver worden gehaald. Bij voorkeur is er ook informatie beschikbaar over de gebruikte (SMTP-)mailcommando's en een overzicht van e-mailservers die het bericht hebben ontvangen. Hieruit kan de gebruikte methode worden afgeleid.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Mogelijk.

In veel gevallen is een open mail relay een foutief geconfigureerde server, er zijn dus geen adequate beveiligingsmaatregelen genomen om misbruik van de server te voorkomen. Maar ook als het misbruikte systeem geen afdoende basisbeveiliging heeft, blijft het misbruik een vorm van binnendringen, hoewel misschien moeilijk als zodanig te kwalificeren. Men mag echter veronderstellen dat de eigenaar van een mailserver deze alleen bedoeld heeft om te gebruiken voor de eigen maildomeinen. Het opzettelijk aanbieden van andere maildomeinen om e-mail door te sturen, kan worden opgevat als het aanbieden van e-mail onder een valse hoedanigheid.

Er is altijd sprake van binnendringen als de open-mail-relay-toepassing ontstaat als malware met opzet op een computer is geïnstalleerd door een kwaadwillende.

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Mogelijk.

Afhankelijk van de hoeveelheid netwerkverkeer dat door open mail relay wordt verstuurd, kan er stoornis in een geautomatiseerd werk optreden.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Nee.

Een open mail relay stuurt in feite alleen aangeboden e-mailberichten door. Er is meestal geen invloed op de bestaande of verwerkte gegevens in het systeem.

Worden gegevens afgetapt of afgeluisterd? Nee.

De kwaadwillende misbruikt het systeem maar valt dit niet aan. Zonder verder binnen te dringen in het systeem zullen over het algemeen geen gegevens worden afgetapt.

Strafbaarheid

Degene die opzettelijk en wederrechtelijk gebruikmaakt van een open mail relay is strafbaar op grond van artikel 138ab lid 1 sub b Sr. Er wordt met behulp van een technische ingreep, een vals signaal of een valse hoedanigheid binnengedrongen in een e-mailserver. Het doorbreken van de beveiliging is niet vereist.
Wel moet de indringer uit de omstandigheden kunnen opmaken dat het niet de bedoeling was om het systeem als zodanig te gebruiken. Dit kan ook op andere manieren dan met beveiligingsmaatregelen duidelijk zijn gemaakt. Als er schade ontstaat aan bedrijfsnetwerken of -servers kan dit eventueel civielrechtelijk worden verhaald.

Als de persoon de mailserver misbruikt en hierdoor een stoornis veroorzaakt in de uitvoering van een nutsdienst of een openbaar telecommunicatienetwerk of telecommunicatiedienst, of met gemeen gevaar voor goederen, of levensgevaar, is hij strafbaar op grond van artikel 161sexies of 161sexies Sr. Hierbij moet dan wel worden aangetoond dat bijvoorbeeld spam verstuurd wordt waardoor de werking van een openbaar netwerk (internet) wordt bemoeilijkt.

3.7.2 Spam

Wat is spam?

Spam is grootschalige ongevraagde berichtgeving, zoals e-mail, sms of andere berichten van commerciële, ideële of charitatieve aard. Spam in de vorm van e-mail wordt vrijwel zonder uitzondering in zeer grote hoeveelheden verstuurd. Bij het versturen van de e-mail worden vaak verkeerd geconfigureerde (open) mailservers van derde partijen of botnets gebruikt, waarbij de gecompromitteerde systemen van (particuliere) gebruikers als proxy worden ingezet.

Spam wordt niet alleen verstuurd als ongevraagde reclame maar ook om malware te verspreiden of als een phishing-aanval.

Technische verschijningsvormen en herkenbaarheid

Er is geen eenduidig technisch onderscheid te maken tussen spam en normaal, legitiem e-mailverkeer. De ontvangende persoon bepaalt of iets als spam beschouwd wordt wanneer het ongevraagd is en van commerciële, ideële of charitatieve aard. Er is een aantal kenmerken waaraan spam te herkennen is:

- verdachte woordpatronen, thema's en semantiek;
- verdachte code en hyperlinks in het e-mailbericht;

- een ongeldig afzendadres. Spam wordt vaak (maar niet altijd) verstuurd met een niet-bestaand of ongeldig afzendadres of afzenddomein;
- ongeldige received-headers. Om detectie moeilijk te maken, worden in veel spam extra received-regels toegevoegd of worden bestaande regels herschreven. Meestal zijn deze regels wel als ongeldig te herkennen.

Spam verstuurd vanaf een geldig e-mailadres van een 'andere partij' (een gespooft e-mailadres) kan een DoS-aanval tot gevolg hebben voor de echte eigenaar ervan.

Benodigde gegevens voor vaststelling

Voor het vaststellen van spam is de belangrijkste benodigde technische informatie:

- het complete oorspronkelijke e-mailbericht in zijn originele staat (platte tekst);
- e-mailberichten en/of de headers ervan;
- het source-IP-adres;
- logbestanden van de e-mailserver;
- informatie over de gebruikte e-mail- en beveiligings-systemen.

Uit de e-mailheaders kan worden opgemaakt welke mail-server is gebruikt als relay. Deze gegevens kunnen ook gedeeltelijk uit logbestanden van de ontvangende mail-server worden gehaald.

Bijlage F geeft een uitgebreid overzicht van benodigde (technische) gegevens voor het vaststellen en het doen van aangifte.

Strafbaarstelling

Wordt er binnengedrongen? Nee.

Bij spam wordt slechts een e-mail gestuurd die op de computer van de ontvanger terechtkomt. Zelfs dat is niet noodzakelijk als bijvoorbeeld een webmailomgeving wordt gebruikt. Natuurlijk is het wel zo dat, als voor de verzending van de spam gekaapte e-mailadressen, een open e-mail server of een botnet worden ingezet, op die gecompromitteerde systemen sprake is van binnendringen (zie ook botnets).

Wordt stoornis in het geautomatiseerde werk veroorzaakt? Nee.

Spam is in principe (volgens de technische specificaties van het SMTP-protocol) e-mail die gebruikmaakt van normale mailtechnieken. Het sturen van e-mail in grote hoeveelheden kan echter verstoring veroorzaken in de werking of in het gebruik van het geautomatiseerde werk of bij (tussenliggende) mailservers; deze moeten extreem veel netwerkverkeer verwerken. De juiste werking wordt dan belemmerd omdat de netwerkcapaciteit ontoereikend is of omdat een mailbox vol raakt.

Overigens kan spam ook worden misbruikt voor het verspreiden van malware in bijlagen *(malicious attachments)*. Dat betekent strafbaarheid voor het verspreiden van malware.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd? Nee.

Spam heeft geen invloed op de integriteit van bestaande gegevens. Dit geldt voor zowel de gegevens op de mail-server als de gegevens op de computer die het bericht uiteindelijk ontvangt. Wel kan er sprake zijn van het toevoegen van gegevens, al zal dit, bij verspreiding via normale e-mailkanalen, als zodanig meestal niet een onrechtmatige vorm van toevoeging zijn.

Worden gegevens afgetapt of afgeluisterd? Nee.

Spamberichten zijn gewone e-mailberichten.

Strafbaarheid

Spam is als zodanig niet strafbaar gesteld volgens de Nederlandse strafwet. De wetgever vindt het sturen van spam niet strafwaardig, behalve als door het toedoen van het verzenden van spam opzettelijk de toegang tot een geautomatiseerd werk wordt belemmerd; dan is dit strafbaar onder artikel 138b Sr. Artikel 138b Sr is van toepassing op openbare en niet-openbare (dus particuliere) computer-systemen. Wanneer als gevolg van spam stoornis in de gang of werking van geautomatiseerde werken optreedt, kan spam ook strafbaar zijn op grond van de artikelen 161sexies en 161septies Sr (computersabotage). Voorwaarde daarbij is dat met het systeem een publieke dienst wordt verleend.

Onder artikel 11.7 van de Telecommunicatiewet kan de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) het spamverbod bestuursrechtelijk handhaven en boetes op leggen.

HOOFDSTUK 4

Incidentopvolging en -afhandeling

In dit hoofdstuk worden aanwijzingen gegeven voor de organisatie van en te volgen stappen bij incidentopvolging en -afhandeling. Hoe moet men omgaan met en reageren op beveiligingsincidenten? Daarnaast worden tips voor de communicatie over een incident gegeven, voor het omgaan met de pers en met personen in een incidentopvolgingsteam.

Incidentopvolging is het geheel van acties rondom een incident dat optreedt. Incidentafhandeling omvat de herstel- en uitwijkacties om te kunnen terugkeren naar de normale situatie. Dit hoofdstuk legt de nadruk op de wijze van opvolging en minder op de herstelacties. Incidentafhandeling wordt vaak gezien als onderdeel van de bedrijfs-continuïteitsplannen van een organisatie (business continuity management (BCM)). Incidentafhandeling wordt daarom niet uitgebreid behandeld in deze handleiding.

Absolute beveiliging bestaat niet. Beveiligingsincidenten zullen zich altijd voordoen. Incidentopvolging en -afhandelingsprocessen zijn dan ook een vast onderdeel van het omgaan met informatie en informatiebeveiliging.

4.1 Organisatie en stappen van incidentopvolging

Deze handleiding volgt een generiek model voor de organisatie en aanpak van incidentopvolging. Deze aanpak onderscheidt zes stappen, te weten voorbereiding, detectie, insluiting, stoppen, herstel, evaluatie (Schultz E., 2002). Bedenk echter dat een cyberincident, en zeker een gerichte cyberaanval, niet altijd netjes lineair deze stappen zal volgen. Een goede organisatie voor incidentopvolging, herstelprocedures, training en oefening met het omgaan met incidenten zijn dan ook essentieel ter voorbereiding op onverwachte situaties.

Voorbereiding
- Maatregelen
- Procedures
- Risico-analyse
- Organisatie
- Personeel
- Middelen

Detectie
- IDS
- Meldprocedure
- Initiële response
- Diagnose
- Rapportage
- Aangifte

Insluiting
- Instrueer gebruikers
- Overleg met autoriteiten
- Schadebeperking
- Informeer betrokkenen over gevolgen

Stoppen
- Oorzaak elimineren
- Voorkom herhaling

Herstel
- Verificatie backup-media
- Repareren
- Patchen
- Opheffen tijdelijke maatregelen

Evaluatie
- Vastleggen
- Borgen van ervaringen
- Aanpassen maatregelen
- Verbeteren procedures

De genoemde stappen zijn in de paragrafen hierna kort beschreven.

4.1.1 Voorbereiding

De eerste belangrijke stap is de voorbereiding. Om incidentopvolging uit te kunnen voeren, moeten zaken zoals beveiligingsmaatregelen, procedures, beschikbaarheid van middelen en personeel zijn geregeld. Wanneer een organisatie zijn (informatie)beveiliging op orde heeft, is de manier waarop wordt omgegaan met (cyber-)veiligheidsincidenten vastgelegd in beleid en procedures, zoals een 'incident- en kwetsbaarhedenbeleid'.

Procedures

Aandachtspunten voor een incident- en kwetsbaarhedenbeleid, uitgewerkt in procedures en werkinstructies, zijn:

- Procedures voor het melden van incidenten of kwetsbaarheden door eigen medewerkers, klanten, gebruikers en externen;
- Procedures voor het verlenen van toegang tot bedrijfsruimtes, apparatuur en bedrijfsinformatie aan externen, zoals functionarissen van de politie, beveiligingsadviesbureaus of een particulier recherchebureau;
- Procedures voor het uitschakelen van apparatuur en het uitwijken naar noodvoorzieningen. Neem hierbij regels voor het veiligstellen van digitale sporen in acht;
- Procedures voor het afgeven van apparatuur of andere goederen voor onderzoek aan autoriteiten of een particulier recherchebureau;
- Procedures voor de omgang met eventuele bewijsmiddelen, de opslag en het vastleggen van de bewijslastketen;
- Procedures voor het bepalen wanneer, waarom en hoe wordt overgeschakeld naar uitwijkvoorzieningen. Houd er rekening mee dat moet kunnen worden vastgesteld of uitwijkvoorzieningen nog integer zijn, en niet zijn geïnfecteerd of gecompromitteerd;
- Procedures voor de wijze van prioritering tussen verschillende beveiligingsincidenten en herstelactiviteiten;
- Procedures voor de afwegingen om imagoschade te voorkomen of te beperken. Het is hierbij belangrijk om de afwegingen expliciet te maken.

Risicomanagement

Incidentopvolging betekent ook omgaan met risico's en effecten. Een belangrijke rol daarbij is weggelegd voor risicoanalyses. Door vóóraf de afhankelijkheden, kwetsbaarheden en mogelijke soorten van incidenten te bepalen, kunnen de acties tijdens incidentopvolging effectief en efficiënt helpen sturen. Weten welke bedrijfsprocessen en middelen aanwezig zijn, weten welke kritisch of alleen maar handig zijn, en weten wat de effecten zijn op de bedrijfsprocessen en de organisatie, is essentiële informatie om op te treden tijdens een calamiteit. Bovendien helpt een risicoanalyse te bepalen welke risico's wel en welke niet acceptabel zijn voor de organisatie. Met deze inzichten kunnen de schaars beschikbare capaciteit van specialisten, beslissers en (technische) middelen optimaal worden ingezet bij de afhandeling van beveiligingsincidenten.

Organisatie van incidentopvolging

Het proces van incidentopvolging en crisisbeheersing werkt het beste als dit niet ad hoc maar gestructureerd plaatsvindt, ondersteund door en geborgd in de organisatie. Aandachtspunten zijn:

- Zorg dat er duidelijkheid bestaat over wie de verantwoording draagt, dan wel taken en bevoegdheden heeft bij de afhandeling van een beveiligingsincident. Zorg ervoor dat de betreffende personen het mandaat van de directie hebben om bepaalde beslissingen te nemen, ook als deze beslissingen op andere afdelingen betrekking hebben.
- Leg naast bevoegdheden ook de beperkingen bij incidentenopvolging vast. Welke besluiten en acties zijn niet toegestaan om te nemen en te worden uitgevoerd door een incidentopvolgingsteam?
- Zorg voor voldoende gekwalificeerd personeel en train deze in het omgaan met beveiligingsincidenten.
- Stel een mediabeleid vast: hoe wordt bij een incident omgegaan met de pers? Leg hierbij de verantwoordelijkheden vast en zorg ervoor dat zowel technische als niet-technische mensen bij dit proces betrokken zijn.
- Cyberincidenten komen zelden geïsoleerd voor. Ontwikkel samenwerkingsverbanden met andere organisaties, ISP's, CERT's en de autoriteiten.
- Pas het incident- en kwetsbaarhedenbeleid aan nadat zich een beveiligingsincident heeft voorgedaan. Vaak kunnen uit de evaluatie van een incident voorstellen komen voor verbetering van het beleid en de beveiligingsmaatregelen.

Daarnaast moeten bij de voorbereiding en organisatie van incidentopvolging, herstel en crisisbeheersing ook praktische zaken worden geregeld. Hierbij valt te denken aan het toezicht vanuit de directie, actualisering van kennis over de ICT-systemen, netwerken en bedrijfsprocessen, contactgegevens van (interne en externe) organisaties en personen, en beschikbaarheid van mensen en (communicatie)middelen.

4.1.2 Detectie

Voor een succesvolle herkenning en opvolging van cyberincidenten is het essentieel dat voldoende preventieve voorzieningen zijn getroffen om misbruik te voorkomen. Bovendien zijn voorzieningen en procedures noodzakelijk om misbruik van ICT-middelen überhaupt te herkennen. In deze tweede stap van het incidentopvolgingsproces is het belangrijk om de eerste diagnose te stellen en initiële reacties te bepalen.

Detectievoorzieningen

De meeste besturingssystemen, netwerkcomponenten, firewalls en antivirussoftware bieden uitgebreide logmogelijkheden. Deze staan vaak niet standaard allemaal aan. Het is natuurlijk van wezenlijk belang dat alle loggingopties vooraf ten volle worden benut. Hierbij moet een afweging worden gemaakt tussen de te leveren prestatie van het systeem, de noodzaak om op het systeem gegevens vast te leggen en de risico's die de organisatie loopt. Bedenk wel dat een digitaal sporenonderzoek ernstig wordt belemmerd als auditlog-gegevens ontbreken of van onvoldoende kwaliteit zijn. Als het beleid van de organisatie is om bij (vermoedens van) cybercrime aangifte te doen, is het belangrijk om vooraf de kans op het vinden en vastleggen van sporen zo optimaal mogelijk te faciliteren *(forensic readiness)*.

Vaak zijn de standaard-auditlog-mogelijkheden van besturingssystemen en applicaties te beperkt om detectie van geavanceerde cyberaanvallen te faciliteren. Aanvullende netwerk- en platformdetectiesystemen (zogenaamde *intrusion detection systems*, IDS) leveren een schat aan waardevolle informatie en kunnen verdacht gedrag signaleren wanneer deze zich voordoen *(real time)*. Het document 'Intrusion detection systems' beschrijft aanvullende achtergrondinformatie (GOVCERT.NL, 21-03-2008).

Enkele van de meest voor de hand liggende symptomen voor een beveiligingsincident zijn:

- mislukte aanmeldpogingen *(failed logon attempts)*;
- aanmelden met standaardaccounts of (niet-gebruikte) 'slapende' accounts;
- activiteit buiten normale werktijden;
- aanwezigheid van (nieuwe) onbekende accounts;
- aanwezigheid van onbekende bestanden of programma's
- onverklaarbare waarschuwingsmeldingen van firewall of antivirusprogramma's;
- onverklaarbare aanpassingen aan toegangsrechten van bestanden of folders;
- onverklaarbare verhoging of gebruik van privileges
- aangepaste bestanden of webpagina's;
- uitvoeren van commando's of programma's die normaal niet worden gebruikt;
- aanwezigheid van computerinbraak *(cracking)*-programma's;
- fouten in logbestanden: gaten in de tijd of ontbreken van bestanden;
- onverklaarbare wijzigingen in DNS-, netwerkrouter- of firewall-configuraties;
- trage systeemprestaties;
- onverklaarbare systeem-crashes;
- meldingen van (pogingen tot) manipulatie van personen (social engineering).

De kans op detectie van mogelijk misbruik wordt vergroot door de samenhang tussen de gegevens van alle verschillende logbestanden onderling te onderzoeken. Kan een medewerker wel lokaal aanmelden als het toegangssysteem van het gebouw meent dat de persoon afwezig is? Komt een antivirusmelding alleen of is er een patroon tussen verschillende systemen en verschillende typen verdacht gedrag waar te nemen? Een SIEM-oplossing (Security Information and Event Management) kan ondersteunen in deze fase van het proces.

Meldprocedure

In de detectiefase is het minstens zo belangrijk dat personeel, gebruikers en klanten bekend zijn met de werking van de meldingsprocedure. Waar kunnen ze constateringen over zwakke plekken of vreemd gedrag van een applicatie of website melden? Hoe wordt de melding geregistreerd en beoordeeld? Hoe kan de melding worden geverifieerd en in verband gebracht met andere mogelijke verdachte gedragingen of cyberincidenten? Wordt een melding wel onderkend als een mogelijk beveiligingsincident of blijft het liggen bij de helpdesk of klachtenservice? Zeker frequente gebruikers van applicaties en websites kunnen verdacht gedrag mogelijk waarnemen. De organisatie zal dus moeten stimuleren dat daarvan melding wordt gedaan, dat opvolging plaatsvindt en dat er wordt teruggekoppeld naar de aanmelder.

Initiële response

Wanneer een (vermoeden van) een beveiligingsincident zich voordoet, is het belangrijk niet in paniek te raken of paniek te veroorzaken. Zelfs bij zeer ernstige situaties zal dit nooit helpen om een cyberincident efficiënt en toereikend te stoppen of om het herstel te bespoedigen.
Om een incident het hoofd te bieden is het beter om bijvoorbeeld de volgende acties te starten:

- Start met het documenteren van alles wat er gebeurt en zich voordoet. Leg hierbij ook duidelijk de eigen acties vast. Wie doet wat, waar, waarmee. Leg ook vast met wie en hoe met andere personen wordt gecommuniceerd.
- Neem voldoende tijd om alle meldingen van verdacht gedrag te onderzoeken. Correleer de gegevens onderling.
- Activeer of voer de mate van *audit logging* op om het gedrag zo goed mogelijk vast te leggen. Start - indien mogelijk - ook een volledige registratie van het computernetwerkverkeer op *(dump)*.
- Maak direct reservekopieën *(backups)* van geïnfecteerde en aangevallen systemen. Maak in ieder geval (offline) kopieën van logbestanden, maar nog liever - als de tijd het toestaat - van het gehele systeem. Een aanvaller kan anders mogelijk sporen wissen en verder onderzoek belemmeren.

Een adequate initiële response en daarop volgende eerste diagnose zijn belangrijk om de juiste afwegingen in het vervolgproces te maken. Belangrijke keuzes zoals het wel of niet laten lopen van een incident, of juist de systemen uitschakelen om verdere schade te voorkomen, worden mede op de eerste bevindingen gebaseerd.

Eerste diagnose

Als een beveiligingsincident wordt gedetecteerd of gemeld, is het van groot belang dat zo vroeg mogelijk wordt vastgesteld of het noodzakelijk of wenselijk is daarvan aangifte te doen. Daarnaast is het belangrijk om de omvang van het incident vast te stellen. Dit is nodig om de wijze waarop met eventuele (digitale) sporen moet worden omgegaan te bepalen en een eventueel te starten strafrechtelijk onderzoek niet te frustreren. Bovendien helpt het stellen van een eerste diagnose de omvang van het incident te bepalen. Hierdoor kunnen de vervolgacties - in prioriteit - worden bepaald.

De fasen van eerste diagnose en het bepalen van acties voor het beperken van de schade (insluiting) kunnen elkaar in zeer korte tijd opvolgen. Afhankelijk van de ernst van een incident zal een ervaren opvolgingsteam snel de verschillende opties doornemen en afwegingen maken. Vergeet echter niet om voldoende tijd te nemen om de eerste constateringen te bespreken en te bediscussiëren, en om de gevolgen van de vervolgstappen te bespreken.

Enkele aspecten en afwegingen voor het vaststellen van de omvang van een cyberincident zijn:

- Hoeveel systemen/apparaten *(hosts of nodes)* zijn er mogelijk gecompromitteerd?
- Hoeveel en welke telecommunicatie- en computernetwerken zijn er bij betrokken?
- Hoe diep zijn de aanvallers er (mogelijk) in geslaagd binnen te dringen, tot aan welke beveiligingsschil zijn ze doorgedrongen?
- Welk niveau van gebruikersprivileges zijn gebruikt? Een ongeautoriseerd gebruik van beheerdersrechten zal de omvang van een cyberincident doen escaleren.
- Welke en hoeveel verschillende aanvalsvectoren worden er (tegelijkertijd) gevolgd?
- Welke kwetsbaarheden gebruikt de aanvaller en hoe wijdverspreid zijn deze in de organisatie en bij de verschillende systemen?
- Welk risico loopt de organisatie? Welke bedrijfsprocessen, systemen of informatie is mogelijk gecompromitteerd en ondervinden nadelige gevolgen?
- Wie zijn allemaal op de hoogte van het incident? Hoe schadelijk kan dit zijn voor de organisatie?

Rapportage

De volgende stap in de detectiefase is het rapporteren van het incident. Niet alleen moeten zo spoedig mogelijk de juiste autoriteiten (politie/openbaar ministerie) worden ingelicht of moet aangifte worden gedaan, maar moeten ook andere partijen noodzakelijk op de hoogte gebracht worden, zoals:

- de interne beveiligingsfunctionaris of Chief Information Security Officer;
- het crisisteam;
- het gehele personeel;
- communicatie en persvoorlichting;
- de juridische afdeling;

- autoriteiten;
- een (extern) incidentopvolgingsteam (CERT);
- de internet service provider;
- systeembeheerders of security officers van klanten en relaties;
- klanten en gebruikers.

Bij voorkeur wordt vastgelegd
- welke informatie door wie mag worden doorgegeven;
- de snelheid waarmee gegevens over een incident moeten worden doorgegeven;
- de manier waarop deze gegevens worden doorgegeven: telefonisch, per (versleutelde) e-mail, op papier, in persoon.

Een classificatieschema voor informatie en een beleid over het uitwisselen van gevoelige informatie kan hierbij helpen (NAVI, juni 2009). Het is bovendien een goede voorbereiding om te weten wat de mogelijke (juridische) consequenties zijn als een beveiligingsincident niet, of niet tijdig, wordt gemeld.

Als aangifte wordt gedaan, zullen de autoriteiten in deze fase tegelijkertijd een strafrechtelijk onderzoek kunnen instellen. Dit onderzoek zal zeer waarschijnlijk starten met een technisch onderzoek. Hoofdstuk 5 gaat verder in op de verschillende aspecten die hierbij een rol spelen.

4.1.3 Insluiting

Het doel van insluiting in het proces van incidentopvolging is om de omvang en impact te beperken. Nadat is bevestigd dat er sprake is van een incident, kunnen passende acties worden uitgezet. Soms kan dit eenvoudig en snel. Stel dat veel mislukte aanmeldpogingen op een gebruikersaccount worden uitgeprobeerd, dan kan eenvoudig de desbetreffende account (tijdelijk) worden geblokkeerd. Maar blijkt dit een beheerdersaccount of service-account te zijn, dan gaat dat niet zonder meer. Het is daarom van belang om de stappen in de insluitingsfase weloverwogen uit te voeren.

Rol van gebruikers

Ook de gewone gebruiker heeft een belangrijke rol. Zij zijn vaak de eerste personen die vreemd gedrag kunnen opmerken. Aan de andere kant kunnen ze ook juist overreageren op (vermoedens) van een incident en daarmee meer schade veroorzaken.

Gebruikers kunnen daarom worden geïnstrueerd om:
- systemen niet uit te zetten of los te koppelen van het netwerk zonder eerst melding te maken van een incident en te overleggen met de verantwoordelijke (beveiligings-) functionaris, manager of helpdesk;
- alle vermoedens van beveiligingsincidenten te melden conform een bedrijfsbeleid en procedures;
- alle vreemde gebeurtenissen te blijven volgen en te documenteren totdat deskundige hulp ter plaatse is;
- geen aanpassingen te maken aan het systeem of applicaties;
- niet te praten met de pers, externe relaties of klanten behalve met toestemming van het management en de beveiligingsfunctionaris.

De schade beperken

Een volgende stap is het beperken van de omvang van het incident en de schadelijke gevolgen. Hierbij kunnen zeer uiteenlopende strategieën worden gevolgd. Hoe en wanneer deze afwegingen worden gemaakt is sterk afhankelijk van de specifieke situatie en de risico's die de organisatie bereid is te nemen. Enkele aspecten die de besluitvorming beïnvloeden zijn bijvoorbeeld hoeveel reputatieschade ontstaat, de financiële schade, schadeclaims of het niet nakomen van (wettelijke) verplichtingen. Gebruik bij de besluitvorming de resultaten van eerdere risicoanalyses om te bepalen of het acceptabel is om juist wel of geen risico te nemen in de wijze en tijdsplanning voor het treffen van acties.

Enkele mogelijke insluitende maatregelen zijn:
- uitschakelen van het systeem *(shutdown);*
- loskoppelen van het computernetwerk;
- aanpassen van firewall en netwerkrouter-configuraties *(firewall rules);*
- blokkeren van gebruikersaccounts;
- wijzigen van alle wachtwoorden;
- installeren van afleidingssystemen *(honeypots);*
- tijdelijke stopzetten van services (zoals FTP, webdiensten, e-mail).

Als een aangevallen systeem gevoelige of geclassificeerde informatie bevat, is de keuze om het systeem direct uit te zetten waarschijnlijk gemakkelijk gemaakt. Echter als een aanval zich lijkt te verspreiden via e-mail, is het misschien nog niet zo eenvoudig om te besluiten om het e-mailsysteem volledig uit te schakelen. Bovendien kan juist een schadebeperkende actie de kans voor het behouden van digitale sporen of op het volgen van de aanvaller, drastisch doen afnemen.

Volg bij de schadebeperkende acties weer een duidelijke procedure. Blijf hierbij alle uitgevoerde acties documenteren, inclusief wie, wat, waar en wanneer iets heeft gedaan.

Opnieuw is het belangrijk om gebruikers en al eerder geïnformeerde functionarissen en instanties op de hoogte te houden van de meest significante ontwikkelingen en getroffen insluitingacties. Adviseer gebruikers en klanten bovendien hoe om te gaan met het mogelijke verlies van gegevens, wachtwoorden of het uitlekken van gevoelige informatie.

In deze insluitingsfase kan bovendien sprake zijn dat de autoriteiten tegelijkertijd al een technisch onderzoek zijn gestart. Als geen aangifte is gedaan, kan in deze fase een eigen forensisch of rechercheonderzoek worden gestart. Het veiligstellen van de zogenaamde plaats veiligheidsinbreuk (PVI) en het verzamelen van gegevens kan op gespannen voet staan met het belang om de schade snel te beperken.

Als een strafrechtelijke procedure wordt gevolgd, is het cruciaal om alle verdere acties in deze en alle volgende incidentopvolgingsfasen af te stemmen met de autoriteiten (politie en Openbaar Ministerie).

4.1.4 Stoppen

De volgende fase, stoppen, heeft als doel om de oorzaak van een incident weg te nemen en om het voortduren of herhalen van een incident te voorkomen. Bij eenvoudige virussen is het bijvoorbeeld mogelijk dat het antivirusprogramma in staat is om een virus te verwijderen. Maar een Trojaans paard dat een 'achterdeur' heeft geplaatst ergens in het besturingssysteem zal moeilijker te verwijderen zijn. Een volledige herinstallatie en formattering van het systeem kan zijn vereist als de besmetting bestond uit extreem kwaadaardige malware of wanneer het systeem onderdeel uitmaakte van een gerichte cyberaanval.

Bijlage G geeft een overzicht van enkele controles die kunnen worden uitgevoerd op verschillende platformen.

Een zorgvuldige procedure is ook in deze fase van de incidentopvolging vereist om voldoende zekerheid te kunnen geven of de oorzaak van een incident is weggenomen. Een gehaaste of ondoordachte aanpak kan resulteren dat het incident zich herhaalt of dat bijvoorbeeld belangrijk forensische digitale sporen worden gewist.

Als onderdeel van deze fase kan een melding worden gedaan aan de systeembeheerder van het domein waarvandaan een aanvaller lijkt te komen. Een meldpunt voor het doorgeven van incidenten is verplicht voor aanbieders van internetdiensten.[52] Veel bedrijven en websitebeheerders hebben bijvoorbeeld een e-mailadres waarop beveiligingsincidenten kunnen worden gemeld (meestal onder een e-mailadres als *abuse@...*).[53] Ook kan aan een internet service provider, via de autoriteiten of NCSC, worden verzocht om een bepaald domein of systeem uit te schakelen *(Notice and Take down)*. Een officier van justitie of NCSC kan een beheerder of ISP echter niet verplichten omstreden informatie op het internet ontoegankelijk te maken of geheel te verwijderen.[54]

In het kader van insluiting en stoppen van een cyberincident wordt het afgeraden om actief onderzoek te doen naar of aan de (externe) systemen waarvandaan de aanval mogelijk lijkt te ontspringen. Actief onderzoek kan bijvoorbeeld bestaan uit zelf een poortscan uitvoeren of testen of een systeem als open proxy of e-mail-relay functioneert. Het is moeilijk aan te tonen dat de aanval echt van een betreffend systeem afkomstig is. Er kan dus zomaar een onschuldig systeem, en daarmee een persoon of organisatie, worden aangevallen. Bovendien is het rechercheren naar derden een opsporingstaak en dus voorbehouden aan de autoriteiten.

4.1.5 Herstel

Als een cyberincident is gestopt, is de volgende stap om de ICT-systemen en dienstverlening weer te herstellen tot hun normale status en niveau. De stop- en herstelfases zijn nauw met elkaar verbonden en gaan vaak in elkaar over.

Om systemen efficiënt te herstellen, kan een herstelstrategie worden gevolgd. Daarbij hoeven de systemen alleen binnen een vastgestelde tijd tot een bepaald percentage van het oorspronkelijke niveau te worden hersteld. In een eerder opgestelde herstelanalyse kunnen de benodigde herstelmiddelen (capaciteiten), een hersteltijd en de kosten voor herstel worden aangegeven. Voor ieder bedrijfsproces zal vaak een *Recovery Time Objective* (RTO) en *Recovery Point Objective* (RPO) zijn gespecificeerd. De Recovery Time Objective is de tijd die beschikbaar is om alle hersteltaken (inclusief reconstructie) van verloren gegane gegevens uit te voeren. De RPO is het punt in de tijd tot welke de gegevens hersteld moeten kunnen worden.

Bij het herstel is het essentieel dat de integriteit van de gebruikte media is gegarandeerd. Ook de reservekopieën (backups) kunnen dezelfde fouten en malware bevatten. Het herinstalleren van systemen moet daarom gebeuren vanaf bekende en geteste installatiemedia. Het terugzetten van reservekopieën moet gebeuren vanaf schone (malwarevrije) media. Zeker als een cyberincident zich over een langere periode heeft voorgedaan, of als een aanvaller gedurende een lange periode toegang tot de systemen heeft gehad, bestaat er een serieus gevaar dat ook de backup-media zijn gecompromitteerd!

Systemen kunnen niet worden hersteld van gespiegelde of redundante systeemconfiguraties (zoals in *mirror sites*,

52. Er geldt een verplicht misbruik-contact-veld voor objecten in de APNIC Whois-database om efficiënt rapporten over misbruik aan de juiste netwerkcontactpersoon te doen toekomen.
53. Abuse-e-mailadressen zijn te vinden in de RIPE database.
54. Als het conceptwetsvoorstel 'Versterking bestrijding computercriminaliteit' wordt aangenomen, worden twee nieuwe artikelen toegevoegd aan het Wetboek van Strafvordering: art. 125p en 125q. Deze zien toe op een vordering van de officier van justitie. Deze kan dan van een aanbieder van een communicatiedienst of van degene die de beschikkingsmacht heeft over een geautomatiseerd werk, vorderen om onverwijld alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit nodig is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.

RAID disk configuraties en dergelijke). Deze bieden wel bescherming tegen hardware-storingen maar zijn qua data elkaars gelijke. Gespiegelde systemen of media zijn dus ook besmet.

Is het systeem hersteld, dan moeten, voordat het weer in gebruik wordt genomen en op een netwerk aangesloten, alle laatste programma-aanpassingen zijn geïnstalleerd (patches). Ook alle andere systemen moeten zo snel mogelijk worden gecontroleerd op de laatste beveiligings-instellingen en aanpassingen.

In de insluitingsfase kunnen tijdelijke maatregelen zijn getroffen om bepaalde typen netwerkverkeer te blokkeren. Nadat voldoende is getest en de herstelde systemen mogen worden geactiveerd, kunnen de tijdelijke maatregelen weer worden opgeheven.

Net als in alle fasen van incidentopvolging blijft het belangrijk om alle handelingen te documenteren en om de significante stappen te communiceren met de betrokken functionarissen, gebruikers en autoriteiten.

4.1.6 Evaluatie

De laatste stap, de evaluatie, dient om de ervaringen opgedaan bij het afhandelen van een beveiligingsincident te borgen. Het doel is om herhaling te voorkomen en om eventuele hiaten in procedures te verbeteren.
Voor de evaluatie kunnen de verslagen en logboeken worden gebruikt die tijdens de incidentopvolging zijn bijgehouden.

Punten om te evalueren zijn onder meer de tijdspanne waarbinnen de opvolging plaatsvond, de afwegingen die zijn gemaakt, de criteria die zijn gehanteerd in de besluitvorming en de effectiviteit van maatregelen die zijn getroffen. Daarnaast helpt het documenteren van de ervaringen om toekomstige incidenten sneller te herkennen en af te handelen. De gedocumenteerde ervaringen zijn ook geschikt als trainingsmateriaal.

4.2 Omgaan met de pers

Niet zelden wordt een groot deel van de schade die een organisatie ondervindt van een cyberincident, veroorzaakt door verlies van imago, reputatie en vertrouwen in de organisatie en de geleverde diensten. In het ideale geval beschikt de organisatie over een communicatieafdeling en een persvoorlichter die adequaat kan omgaan met de pers. Overleg en communicatie met de buitenwereld, in het bijzonder met de pers, moet vooraf zijn goedgekeurd door het verantwoordelijke management of de directie.

Deze handleiding gaat niet verder in op de wijze van communiceren over incidenten maar wil wel enkele aandachtpunten meegeven:

- Bereid een interview voor.
- Probeer zoveel mogelijk informatie over een interview vooraf te verzamelen.
- Zet de belangrijkste punten die de organisatie wil vertellen op een rij.
- Anticipeer vooraf op mogelijke lastige vragen en bereid de antwoorden voor.
- Maak tijdens het interview zo snel mogelijk contact met de interviewer.
- Gebruik korte heldere zinnen.
- Vermijd moeilijke technische toelichtingen.
- Stuur het gesprek naar de punten die de organisatie wil maken.
- Wordt niet afgeleid of geïntimideerd door de entourage van de pers.
- Wees diplomatiek maar vertel altijd de waarheid.
- Geef toe als een antwoord niet bekend is.
- Let op houding en non-verbale communicatie.
- Breek een interview af als dit nodig lijkt.
- Vraag om verslaggeving van het interview vóór publicatie te mogen inzien.

Enkele vragen die kunnen worden verwacht zijn:
- Wat is er gebeurd?
- Welke schade is ondervonden?
- Wat was de oorzaak?
- Wat heeft u er aan gedaan?
- Kan het nog een keer gebeuren?
- Wat kunnen anderen er aan doen?
- Wordt schade door u gecompenseerd?

4.3 Incidentopvolgingsteam

Het omgaan met cyberincidenten is niet een puur technische aangelegenheid. Zoals de hiervoor beschreven stappen duidelijk maken, vereisen het managen van risico's, communiceren met betrokken partijen, coördineren met autoriteiten en aansturen van onderzoeks- en herstelteams verschillende vaardigheden en kennis. Zeker bij grootschalige, publiek- of politiek-gevoelige incidenten wordt de nodige druk gelegd op het crisisteam van de organisatie.

De borging van incidentopvolging in de organisatie vereist dat de teamleider direct kan rapporteren aan de top van het management of de directie. De teamleider zelf hoeft daarom niet zozeer over diepgaande technische kennis en vaardigheden te beschikken. In plaats daarvan is het voor een teamleider belangrijker om over voldoende management- en advieskwaliteiten te beschikken. De teamleider moet daarnaast vooral de procedures bewaken, kennis hebben van de juridische aspecten en de coördinatie met (externe) partijen en autoriteiten kunnen uitvoeren.

De teamleden van een incidentopvolgingsteam moeten uiteraard over uitstekende technische vaardigheden en kennis beschikken. Maar minstens zo belangrijk is het om te kunnen communiceren met andere technici. Voor het uitvoeren van veel van de handelingen zijn uitgebreide beheerdersrechten op de computer- en netwerksystemen nodig. Dat vereist dat leden van een incidentopvolgingsteam ook systeembeheerder zijn, of ten minste bevoegd om de medewerking van systeembeheerders te kunnen eisen. Teamleden komen zeer waarschijnlijk ook in aanraking met gevoelige informatie. Leden van incidentopvolgingsteams worden dan ook vaak onderworpen aan een antecedentenonderzoek en expliciet gewezen op een geheimhoudingsplicht.

Alle teamleden moeten over voldoende persoonlijke en communicatieve vaardigheden beschikken en teamspelers zijn.

HOOFDSTUK 5

Onderzoeken van incidenten

Hoe ga je om met elektronisch verkregen materiaal als bewijsmiddel? In dit hoofdstuk staan ook aandachtspunten bij (forensisch) recherche-onderzoek. De informatie is bedoeld om personen betrokken bij een onderzoek naar een cyberincident voldoende achtergrondinformatie te geven om vast te stellen of zij bevoegd zijn een onderzoek te verrichten. Daarnaast schetst dit hoofdstuk de voornaamste kaders en verplichtingen van een digitaal onderzoek en het veiligstellen van digitale sporen.

5.1 Rechtsmacht - formeel strafrecht

Is een bepaalde handeling in Nederland strafbaar, dan volgt de vraag of de Nederlandse rechter bevoegd is om te oordelen over de strafzaak. Deze vraag betreft de rechtsmacht van Nederland, ook wel jurisdictie genoemd. De grenzen van deze rechtsmacht worden beheerst door de regels van internationaal recht, die stellen dat *jurisdictie* gebaseerd kan worden op twee verschillende grondslagen. Enerzijds gaat het om de exclusieve rechtsmacht van een staat over het eigen grondgebied, anderzijds betreft het de rechtsmacht van een staat over zijn onderdanen.

De term jurisdictie heeft in dit kader alleen betrekking op de rechtsmacht om personen te vervolgen. Dit moet duidelijk worden onderscheiden van de bevoegdheden die een staat heeft voor opsporingshandelingen en de feitelijke arrestatie van verdachten.

De eerste basisregel bij het vaststellen van jurisdictie is dat er voldoende verband moet zijn tussen het strafbare feit en de staat die stelt rechtsmacht te hebben. In principe is niet vereist dat het gaat om een fysiek verband. Bij cybercrime zal een dergelijk verband namelijk vaak ontbreken.

Voorbeeld: een persoon uit land A kan, via een (telecommunicatie) infrastructuur in land B, zich toegang verschaffen tot een computersysteem in land C en hieruit kennis verzamelen of deze gebruiken als springplank om vervolgens schade te veroorzaken in land D. Het bewijzen van een fysieke aanwezigheid van de persoon in landen B, C en D is in dit geval niet vereist. Maar als in voornoemd voorbeeld "land B" Nederland blijkt te zijn, kan er ook rechtsmacht geclaimd worden.

Dit is alleen de 'lichtste' vorm van de betrokkenheid van een land volgens het Nederlands rechtssysteem.

5.1.1 Bevoegdheid Nederlandse rechter

Territoriale jurisdictie

In een aantal internationale verdragen is de eerste grondslag voor jurisdictie nader uitgewerkt: het territorialiteitsbeginsel. Volgens deze internationale rechtsregel heeft een staat volledige rechtsmacht over zijn *territoir* (grondgebied), de bijbehorende territoriale zee en de luchtkolom daarboven, alsmede over vaartuigen en luchtvaartuigen die de vlag van de betreffende staat voeren.

In Nederland is de strafrechtelijke territoriale jurisdictie geregeld in art. 2 en 3 Sr. Deze bestaat uit:

1. Het objectieve territorialiteitsbeginsel: Nederland kan jurisdictie claimen indien de gevolgen van de handeling optreden in Nederland.
2. Het subjectieve territorialiteitsbeginsel: Nederland heeft rechtsmacht indien de handeling is uitgevoerd in Nederland.

Het territorialiteitsbeginsel houdt dus in dat iedereen die zich in Nederland schuldig maakt aan een strafbaar feit (misdrijf en/of overtreding) een straf kan krijgen opgelegd.

Personele jurisdictie

De aanpak van internationale computercriminaliteit berust op meer beginselen dan alleen de territoriale rechtsmacht. De tweede grondslag voor jurisdictie is de rechtsmacht die een staat mag uitoefenen over personen op basis van hun nationaliteit. De mogelijkheden daarvoor zijn:

- Het actieve nationaliteitsbeginsel: criminele jurisdictie van de Nederlandse staat over zijn onderdanen, zoals bepaald in art. 5 Sr. Dit artikel is ook van toepassing op een beperkt aantal strafbare feiten die door Nederlanders buiten Nederland zijn begaan. Bovendien geeft dit artikel de Nederlandse strafrechter de bevoegdheid om te oordelen over alle misdrijven die door een Nederlander in het buitenland zijn gepleegd, voor zover deze feiten in beide landen strafbaar zijn. Lid 1 sub 4 van dit artikel regelt bovendien de jurisdictie voor de specifieke misdrijven genoemd in art. 138ab, 138b, 139c, 139d, 161sexies, 350 en 350a Sr.
- Het passieve nationaliteitsbeginsel of personaliteitsbeginsel: criminele jurisdictie over strafbare feiten die buiten het territoir van de staat worden gepleegd tegen één van haar onderdanen. Nederland kent dit controversiële beginsel niet.
- Het beschermingsbeginsel: de jurisdictie over strafbare feiten die door een niet-onderdaan in het buitenland zijn begaan, gericht tegen de veiligheid of essentiële belangen van de Nederlandse staat (art. 4 Wetboek van Strafrecht).
- Het universaliteitsbeginsel: jurisdictie over strafbare feiten die in principe geen verband houden met Nederland, maar waarvoor een internationaalrechtelijke machtiging of verplichting tot berechting bestaat. Het gaat dan vooral om ernstige feiten, waarbij de bevoegde staten hun rechtsmacht niet kunnen of willen gebruiken voor vervolging.

Het personaliteitsbeginsel houdt dus in dat iedere Nederlander die zich, waar dan ook ter wereld, schuldig maakt aan met name genoemde misdrijven een straf kan krijgen opgelegd. Hiertoe behoren dus ook verschillende vormen van cybercrime in enge zin.

5.1.2 De internationale dimensie

Evenals Nederland onderschrijven veel landen het territorialiteitsbeginsel voor de vervolging van strafbare feiten op internet. Internet beschikt echter niet over (zichtbare) territoriale grenzen. Dit betekent dat meerdere landen bevoegd kunnen zijn voor opsporing en vervolging van hetzelfde feit. De gevolgen van een bepaalde vorm van cybercrime kunnen zich immers in meerdere landen voordoen.

Wanneer Nederland over rechtsmacht beschikt en men in het buitenland bewijsmateriaal wil vergaren voor opsporing van het strafbare feit, dan kan dit met een rechtshulpverzoek. Omgekeerd geldt, dat ook buitenlandse opsporingsinstanties op basis van internationale afspraken Nederland om rechtshulp kunnen vragen. Of de gevraagde rechtshulp daadwerkelijk wordt geboden hangt af van de vraag of er sprake is van zogenaamde dubbele strafbaarheid. Dubbele strafbaarheid houdt in dat zowel in het verzoekende als in het verzochte land sprake is van een strafbaar feit.

Internationale rechtshulpverzoeken voor cybercrime worden door de National High Tech Crime Unit van het KLPD beoordeeld en in overleg met het Landelijk Parket doorverwezen naar een opsporingsinstantie zoals de regionale politie of de FIOD/ECD. Ook handelt het NHTCU zelf rechtshulpverzoeken af.

5.1.3 Uitlevering van verdachten

Er is geen algemene regel die een staat verplicht tot uitleve-ring van een verdachte. Evenmin is er een regel die uitlevering in zijn algemeenheid verbiedt. Uitleveringsverplichtingen tussen staten kunnen daarom alleen ontstaan als zij deze in verdragen vastleggen.
Voor Nederland is hierbij vooral het Europees Uitleveringsverdrag van 1957 van belang. Daarin wordt bepaald dat uitlevering slechts verplicht is als een feit strafbaar is in zowel het uitleverende land als in het land waaraan de verdachte wordt uitgeleverd. Dit is de zogenoemde dubbele criminaliteitseis. Ook bepaalt het verdrag dat de verdachte na uitlevering alleen mag worden berecht voor het feit waarvoor hij is uitgeleverd.

Er zijn enkele belangrijke uitzonderingen op deze regels. Zo mag uitlevering worden geweigerd als het risico bestaat dat de aanvragende staat bij een veroordeling de doodstraf zal opleggen, of wanneer de reële vrees bestaat dat de verdachte vervolgd zal worden wegens ras, geloof of politieke gezindheid. Een staat kan te allen tijde de uitlevering weigeren van één van zijn eigen onderdanen.

5.1.4 Doorzoeking en inbeslagneming

Bij het onderzoeken van cyberincidenten kan het nodig zijn om computersystemen of apparatuur veilig te stellen voor onderzoek. Mogelijk is het zelfs nodig om apparatuur of andere voorwerpen, zoals documenten, in beslag te nemen. Deze paragraaf gaat kort in op enkele uitgangspunten in het formeel strafrecht.

Bevoegde onderzoekers

Een strafrechtelijk onderzoek uitvoeren en een procesverbaal opmaken kan alleen worden gedaan door een algemeen opsporingsambtenaar (OA) en de volgende functionarissen:

- Officieren van Justitie;
- rechter-commissarissen;
- ambtenaren van politie aangesteld voor politietaken;
- vrijwilligers van politie aangesteld voor politietaken;
- bijzondere ambtenaren van politie;
- opsporingsambtenaren van andere opsporingsinstanties (zoals FIOD/ECD).

Een (strafrechtelijk) onderzoek kan ook worden verricht door een buitengewoon opsporingsambtenaar (BOA). Daartoe moet deze bevoegd zijn verklaard in een akte van benoeming of op grond van bijzondere wetgeving of verordening.

Particulier onderzoek

Onderzoek naar een beveiligingsincident kan ook door, of in opdracht van, de eigenaar van de computersystemen worden gedaan. Van deze systemen vermoedt men dat deze zijn betrokken bij een misdrijf. De eigenaar mag ook onderzoek doen als het om een mogelijke inbreuk op de bedrijfsrichtlijnen gaat. De eigenaar, bijvoorbeeld de directie van het bedrijf, kan de systeembeheerder opdracht geven om een systeem te onderzoeken. Een eigenaar of systeembeheerder mag niet zonder meer gaan 'vissen' naar eventuele sporen (Zwan, 2009).

De eigenaar kan het onderzoek laten uitvoeren door een derde partij. Voor het verrichten van recherchewerkzaamheden is vergunning van de minister van Veiligheid en Justitie nodig. Een ingehuurde particuliere onderzoeker heeft geen extra bevoegdheden maar opereert vanuit de juridische bevoegdheid van de eigenaar en opdrachtgever.

Doorzoeking

In een strafrechtelijk onderzoek kunnen computers worden onderzocht en gegevens worden gekopieerd. Het Wetboek van Strafvordering stelt, naast de normale doorzoekingbevoegdheden, regels vast voor het doorzoeken van geautomatiseerde werken en gegevensdragers. Het doorzoeken van een computer in een netwerk mag op afstand plaatsvinden als dit redelijkerwijs nodig is om de waarheid aan de dag te brengen (art. 125j, lid 1 Sv). Hierbij moet het onderzoek zich beperken tot geautomatiseerde werken (netwerklocaties) waar de normale gebruikers van de doorzochte computer rechtmatig toegang toe hebben, vanaf de plaats (computer) waar de doorzoeking plaatsvindt (art. 125j, lid2 Sv).

Er bestaat overigens ook een mogelijkheid tot "doorzoeking ter vastlegging van gegevens" (art. 125i Sv). Hierbij worden plaatsen doorzocht om gegevens vast te leggen (te kopiëren) die op die plaats op een gegevensdrager zijn opgeslagen. Er wordt dus niets in beslag genomen. Veelal vindt de uitvoering van deze bevoegdheid op locatie plaats.

Inbeslagname

In het belang van een onderzoek kan het nodig zijn om computersystemen of gegevensdragers veilig te stellen voor verder onderzoek of als bewijs. Bevoegde opsporingsambtenaren kunnen voorwerpen in beslag nemen.

Inbeslagname is de beschikking krijgen of gaan houden (reeds onder zich maar nu houden als bewijs) van voorwerpen. Vatbaar voor inbeslagname (art. 94 Sv) zijn voorwerpen die:

- nodig zijn om de waarheid aan het licht te brengen;
- verbeurd zijn verklaard, bijvoorbeeld door diefstal of heling verkregen;
- onttrokken zijn aan het maatschappelijke verkeer (in strijd met de wet);
- geschikt zijn om wederrechtelijk voordeel aan te tonen.

Een systeembeheerder of een ingehuurde particulier onderzoeker kunnen in het kader van een onderzoek apparatuur en informatiedragers meenemen en veilig stellen. Een burger, dus ook een particulier onderzoeker, mag alleen voorwerpen in beslag nemen die een verdachte bij zich draagt en zo voor het grijpen zijn. Een burger mag niet fouilleren en geen onderzoek aan lichaam of kleding verrichten.

5.1.5 Opsporingsmethoden

Opsporingstaken zijn voorbehouden aan de autoriteiten. De politie heeft verschillende opsporingsmethoden om digitaal bewijsmateriaal te vergaren. Deze handleiding geeft slechts een beknopt overzicht hiervan.

De autoriteiten mogen, naast fysieke goederen zoals documenten, cd-rom's, usb-sticks en computerapparatuur, ook elektronische gegevens in beslag nemen, bijvoorbeeld tijdens een huiszoeking. Daarnaast kan de politie een eigenaar bevelen een kopie van bijvoorbeeld de harde schijf van een computer af te staan. Ook is de politie bevoegd om te eisen dat versleutelde gegevensdragers of computerbestanden worden ontsleuteld. Een dergelijk bevel mag niet aan een verdachte worden gegeven. Een verdachte is niet verplicht hieraan mee te werken en kan een bevel tot afgifte of ontsleuteling negeren.[55] Een ISP of systeembeheerder die toevallig over een wachtwoord van versleutelde bestanden van een verdacht beschikt, kan wel worden gedwongen deze af te staan (art. 125k Sv).

Opsporingsdiensten kunnen een internet service provider verplichten om al het dataverkeer van een verdachte op te nemen (aftappen). Zo kunnen e-mail, chatsessies en bezochte websites worden nagetrokken. Ook kunnen de persoonsgegevens van het IP-adres van een abonnee door de politie worden gevorderd.

55. Geldt ook voor personen met verschoningsrecht.

5.1.6 Bewijsmiddelen

Boek II, Titel VI, derde afdeling van het Wetboek van Strafvordering behelst de bepalingen (artikelen 338 t/m 344a Sv) over het strafrechtelijk bewijsrecht. De belangrijkste onderdelen van deze bepalingen worden hieronder opgesomd. Noodzakelijk voor het aannemen van het bewijs door de rechter is dat de bewijsmiddelen wettig en overtuigend zijn.

Wettige bewijsmiddelen zijn (limitatief) (art. 339 Sv):

1. eigen waarneming van de rechter;
2. verklaringen van de verdachte;
3. verklaringen van een getuige;
4. verklaringen van een deskundige;
5. schriftelijke bescheiden.

Schriftelijke bescheiden in het bovenvermelde zijn (limitatief) (art. 344 lid 1 Sv):

1. beslissingen door colleges en personen met rechtspraak belast;
2. processen-verbaal en andere geschriften, in wettelijke vorm opgemaakt door daartoe bevoegde colleges, en behelzende hun mededeling van feiten en omstandigheden, door hen zelf waargenomen of ondervonden (artikel 344 lid 1 onder 2 Sv);
3. geschriften opgemaakt door openbare colleges of ambtenaren, betreffende onderwerpen behorende tot de onder hun beheer gestelde dienst en bestemd om tot bewijs van enig feit of enige omstandigheid te dienen;
4. verslagen van deskundigen;
5. alle andere geschriften, doch deze kunnen alleen gelden in verband met de inhoud van andere bewijsmiddelen.

Eisen aan het bewijs

Het bewijs moet rechtmatig zijn verkregen en voldoen aan bewijsminimumregels. Is dat niet het geval is, dan kan bewijsuitsluiting volgen. In beginsel moet het bewijs steunen op meer dan één wettig bewijsmiddel.
Op deze regel wordt een uitzondering gemaakt voor het proces-verbaal van een opsporingsambtenaar, dat een geschrift is in de zin van het hiervoor aangegeven tweede punt. Het is echter niet zo dat elk feit kan worden bewezen op grond van een enkel proces-verbaal van een opsporingsambtenaar. In de praktijk zal dit slechts van toepassing zijn als het gaat om simpele, op heterdaad geconstateerde overtredingen. In andere gevallen zal de rechter zich immers minder snel overtuigd achten.

Het bewijs moet de rechter kunnen overtuigen. Er mag geen onredelijke twijfel over het bewijsmateriaal bestaan. Voor het bewijs mag (bijvoorbeeld) geen gebruik worden gemaakt van:

- meningen of gissingen;
- verklaringen van medeverdachten (volgens de wet zijn dat enkel degenen die samen met de verdachte op dezelfde aanklacht, in dezelfde instantie, tegelijk terecht staan).

De verklaring van een medeverdachte kan alleen meewerken aan het bewijs wanneer die medeverdachte als getuige is gehoord;
- bewijsmateriaal waarvan de verdediging gemotiveerd aanvoert dat het onbetrouwbaar is, zonder dat er een motivering door de rechter tegenover staat.

Hierdoor is onrechtmatig verkregen bewijs niet altijd onbruikbaar en rechtmatig verkregen bewijs niet altijd bruikbaar. Iets is bewijs als de rechter het accepteert als bewijs. Gemotiveerde verweren van de verdediging over de betrouwbaarheid van bewijsmateriaal moeten door de rechter gemotiveerd worden verworpen. Gebeurt dat niet, dan kan het bewijsmateriaal niet worden gebruikt en met zich meebrengen dat een bewezenverklaring onvoldoende is gemotiveerd. Zulke verweren kunnen betrekking hebben op de betrouwbaarheid van een verklaring, van een ingeschakelde deskundige of diens toegepaste onderzoeksmethode of de onzorgvuldige hantering van een (onderzoeks)methode.

Ook kan de betrouwbaarheid van de uitkomst van een (elektronische) meting of elektronische informatie gemotiveerd worden betwist, als gevolg waarvan de rechter er onder bepaalde omstandigheden geen gebruik van mag maken.[56]

Bewijskracht van elektronische gegevens

Uit het voorgaande blijkt dat (elektronische) gegevens als zodanig niet in de opsomming van wettige bewijsmiddelen zijn opgenomen. De gegevens zullen daarom in een procesverbaal of ander geschrift moeten worden opgenomen om voor het bewijs in een strafzaak te kunnen worden gebruikt. Een in de wettelijke vorm door een bevoegd ambtenaar opgemaakt proces-verbaal over diens waarneming van gegevens van een computer of gegevensdrager, zou in beginsel kunnen gelden als schriftelijk bewijs in de zin van art. 344 lid 1 onder punt 2 Sv. Andere geschriften, zoals de gegevens uit een computer of gegevensdrager, zouden kunnen gelden als bewijs in de zin van art. 344 lid 1 onder punt 5 Sv (Zwan, 2009).

Voor de waardering van elektronisch bewijs is van belang hoe betrouwbaar de waargenomen gegevens worden geacht. Bovendien zal de (forensisch) onderzoeker de integriteit van de onderzochte gegevens gedurende het hele onderzoek te allen tijde moeten kunnen aantonen *(evidence trail)*.

Elektronische bewijsmiddelen zijn helaas makkelijk te vervalsen. Een datum of tijdstip waarop een computerbestand is aangemaakt of gewijzigd, kan eenvoudig worden aangepast. Misschien is een computerbestand zonder medeweten van de eigenaar op het systeem geplaatst door een kwaadwillende. Een rechter bepaalt hoeveel waarde wordt toegekend aan het gepresenteerde bewijsmateriaal. Hebben datum en tijdstip van een verzonden e-mailbericht betrekking op een onafhankelijk logbestand van de internetprovider, dan is het aannemelijk dat het e-mailbericht ook daadwerkelijk is verzonden op dat tijdstip. Een e-mailbericht op de computer van een verdachte zonder sporen (van verzending) op mailservers is moeilijker aan te voeren als solide bewijs.

5.2 Modus operandi en rolverdeling

Deze paragraaf met voorbeelden van daders en hun modus operandi dient om de verschillende vormen van cybercrime beter te kunnen herkennen, de wijze van incidentopvolging beter in te schatten, en gerichter te kunnen zoeken naar digitale sporen.
Heeft een organisatie te maken met zero-day exploits, ingezet om de systemen van een organisatie te verstoren, dan is de reactie anders dan wanneer de organisatie slachtoffer is van een computervirus dat veel voorkomt. Om de juiste beveiligingsmaatregelen te kiezen moet men ook een beeld hebben van het door de dader gewenste verloop van een aanval. Deze handleiding beperkt zich tot een overzicht van enkele daderprofielen die specifiek ICT-middelen inzetten of tot doelwit maken, zoals een *scriptkiddie*, een *hacktivist* of hacker.[57]

Misbruik van ICT en internet wordt steeds laagdrempeliger. Cybercrime neemt in alle sectoren van de samenleving toe. Iedereen kan er mee worden geconfronteerd. Cybercrime internationaliseert verder, is in ontwikkeling en steeds vaker zijn criminele organisaties erbij betrokken. ICT maakt tegenwoordig deel uit van de *modus operandi* van criminelen. Cybercrime kenmerkt zich onder meer door het anonieme karakter, het massaal en snel kunnen verrichten van handelingen, het gebrek aan (lands)grenzen en de dynamiek van de cyberwereld.

Een algemeen model dat de verschillende stappen in een cyberaanval laat zien, bestaat uit de fasen voorbereiding, toegang verschaffen, uitvoeren van acties, aftocht en genot. In werkelijkheid zal een computercrimineel natuurlijk niet zo bewust calculerend te werk gaan. Eenvoudig manipuleerbare systemen - het laag hangende fruit - worden snel en direct geëxploiteerd als dat mogelijk voordeel kan opleveren.

De fases bestaan uit de volgende activiteiten:

56. Zie in dit verband arrest HR 12 maart 1996, NJ 1996, 511
57. Een bekende indeling in klassen is de hackertaxonomie van Rogers (2006) of Lovet (2007). Een indeling van mogelijke daders is echter nooit zo zwart-wit en bovendien deels achterhaald.

Voorbereiding
- Selecteren doelwit
- Openbare informatie verzamelen
- Blogs en social networks
- Verkennen, observatie (scanning, DNS)
- Middelen aanschaffen
- Gegevens aanschaffen (omkoping)

Toegang verschaffen
- Plannen van uitvoering
- Netwerk scanning
- Identificeer systemen/personen
- Sturen malware, exploits
- Social engineering
- Scannen/sniffen van binnenuit
- Aanvalsplan bijstellen

Acties
- Binnendringen (onbeschermde) systemen
- Installeren malware/backdoors
- Stelen van data
- Aanpassen gegevens, sabotage, manipulatie
- Misbruiken in andere cyberaanval

Aftocht
- Verzamelen buit
- Terugzenden gegevens
- Wissen logbestanden

Genot
- Publiciteit
- Doorverkopen
- Aanschaf van (luxe) goederen

Het feitelijk getoonde gedrag van de dader in elke fase is sterk afhankelijk van het type dader, zijn doelstellingen, motivatie en hulpmiddelen, het doelwit en de omstandigheden dat het doelwit bereikbaar en 'zichtbaar' is in cyberspace. De toegangsverschaffing markeert meestal het operationele startpunt van de onbevoegde handeling, hoewel verschillende voorbereidingshandelingen op zich al strafbaar kunnen zijn.

Daders kunnen gegevens kopiëren of aanpassen, of rootkits en backdoors installeren om op een later tijdstip weer toegang te hebben. De meeste daders hebben baat bij een veilige aftocht. De buit zal op een bepaalde manier onopgemerkt bij de dader moeten aankomen, wil die hiervan gebruik gaan maken.

Vaak moeten tijdens de aftocht verkregen gegevens worden gezonden naar een systeem van de aanvaller. Dit hoeft niet een eigen systeem van de aanvaller te zijn, het kan ook een misbruikt systeem van een ander slachtoffer zijn. Een dader kan bij de aftocht proberen sporen te verbergen door logbestanden te wissen of andere schade aanrichten. De dader wil uiteraard van zijn daad genieten, bijvoorbeeld door publiciteit of roem, de aanschaf van goederen of doorverkopen van de buit aan een criminele handelspartner.

Meer achtergronden over de verschillende modus operandi en rolverdeling in de criminaliteitsketen kan worden gevonden in de 'Criminaliteitsbeeldanalyse Hightech crime' van het KLPD (KLPD Dienst Nationale Recherche, 2009). Aanvulling over het profiel van verschillende daders staat in de studie van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Veiligheid en Justitie (Hulst, 2008) of de 'Verkenning cybercrime in Nederland 2009' (Leukfeldt E.R., 2010).

5.2.1 Scriptkiddie

Een *scriptkiddie* (computervandaal) is een persoon die zich zonder kennis van zaken misdraagt op ICT-systemen. Voor ICT-systemen die goed up-to-date zijn gehouden komen ze meestal kennis en kunde te kort om daadwerkelijk een groot gevaar te vormen. Een scriptkiddie heeft slechts beperkte kennis van de onderliggende technieken en bedient zich van hulpmiddelen die door anderen zijn bedacht en ontwikkeld. De stereotype scriptkiddie is een mannelijke puber, in het bezit van een krachtige computer en een snelle internetverbinding. Scriptkiddies handelen vaak vanuit een baldadige motivatie en voor de 'kick'. Zij zijn zich meestal niet bewust van de gevolgen van hun handelen of hebben weinig van doen met andere (internet)gebruikers. Scriptkiddies veroorzaken veel overlast en zijn de oorzaak van veel *abuse*-meldingen op het internet.

5.2.2 Hacker

Een hacker (computercrimineel) is iemand die inbreekt in computersystemen. In sommige technisch georiënteerde subculturen wordt een hacker gezien als iemand met goede vaardigheden zonder criminele bijbedoelingen. Een hacker is een persoon die geniet van de intellectuele uitdaging om op een creatieve, onorthodoxe manier aan technische beperkingen te ontsnappen. Een hacker hoeft niet per se iets met computers te doen.
De meeste hackers zijn intelligente mensen met een expliciete behoefte aan kennisverrijking. Ze zijn creatief en kunnen zelf software ontwikkelen. Een hacker kent een programmeertaal of -omgeving zo goed dat hij zonder zichtbare moeite een programma kan schrijven, een technologie bedenkt, ontwerpt, uitwerkt, implementeert, test, en verbetert. Een hacker kan ook onconventionele maar adequate oplossingen bedenken tegen lekken, fouten en problemen met de beschikbare middelen.

Kwaadwillende hackers *(black-hat)* opereren steeds vaker met criminele bedoelingen en raken steeds meer betrokken bij criminele organisaties. Een (black-hat) hacker krijgt een kick als het lukt om (ongeoorloofd) toegang te hebben tot een ICT-systeem.[58]

5.2.3 Botnet herder

Een *botnet herder* is een computercrimineel die tijd en moeite steekt in het onderhouden en uitbreiden van illegale netwerken van zombie-computers (botnets). Botnet herders beperken zich regelmatig tot illegaal binnendringen van de computersystemen. Ze verkopen of verhuren vervolgens hun botnet aan criminelen die deze inzetten voor andere vormen van internetgerelateerde criminaliteit, zoals spam versturen, gegevens verzamelen of DDoS-aanvallen uitvoeren.

5.2.4 Hacktivist

Een *hacktivist* (computeractivist) is iemand die protesteert via (openbare) ICT-voorzieningen. Hacktivisme is een term die staat voor computergeoriënteerde activistische handelingen, zoals een politieke machthebber ondermijnen, meestal vanuit ethische motieven. De term is een samenvoeging van de begrippen computerinbraak en activisme. De bekendste vorm van hacktivisme is het wijzigen van websites *(defacen)*. Een andere vorm van hacktivisme is het organiseren van (volgens de geldende opvattingen) subversieve krachten om de vrijheid van meningsuiting te kunnen afdwingen. Daarbij wordt gebruik gemaakt van publieke netwerken, zoals het internet en sociale netwerken, en besloten netwerken zoals Freenet.

5.2.5 (Ex-)medewerker/insider

Een (gefrustreerde) medewerker of ex-medewerker, waaronder eigen of ingehuurd personeel of in dienst van toeleveranciers, kan de belangen van de organisatie schaden door fysieke, financiële of imagoschade aan te richten. Bovendien kan een medewerker, zonder rancuneuze bijbedoelingen, uit zijn op eigen (financieel) gewin. Medewerkers die de organisatie verlaten kunnen ook een bedreiging zijn. Zij nemen bijvoorbeeld gevoelige informatie mee om aan een nieuwe werkgever te kunnen tonen wat ze hebben gedaan. Ook kan een medewerker van mening zijn dat hij het werk heeft gecreëerd en dus recht heeft op een kopie, of zelfs het bronbestand. In enkele gevallen hebben wraakzuchtige medewerkers bij het verlaten van het bedrijf malware achtergelaten om later toegang tot de systemen te krijgen.

Acties van medewerkers zijn over het algemeen moeilijk te voorkomen, omdat de medewerker kennis heeft van het bedrijf, de procedures en de installaties. Daarbij heeft de (ex-)medewerker vaak toegang tot cruciale objecten of gevoelige bedrijfsinformatie.

5.3 Technisch onderzoek

Het (digitaal) forensisch onderzoek laat zich beschrijven als een gestructureerd onderzoek naar illegale activiteiten volgens bewezen methoden, waarbij informatie op elektronische middelen wordt verzameld, veiliggesteld, geanalyseerd en gepresenteerd op een juridisch verantwoorde wijze in dienst van de rechtspraak. Het gaat hier dus om objectieve waarheidsvinding van wat is gebeurd, waar, wanneer, waarmee (hoe), met welk gevolg en door wie. Een forensisch onderzoek beantwoordt normaliter geen vragen waarom iemand iets heeft gedaan en stelt ook nimmer een schuld vast.

Ga nooit zelf onderzoek verrichten en kom niet aan mogelijk te onderzoeken voorwerpen (fysieke en digitaal) als een strafrechtelijk onderzoek nodig is. Schakel in dat geval direct de autoriteiten (politie) in. Schakel bij twijfel deskundige hulp in, bijvoorbeeld van een particulier recherchebureau, zoals voor het begeleiden van het onderzoek of het verrichten van forensische werkzaamheden.

De meeste regionale politiekorpsen hebben een Bureau Digitale Expertise (BDE). Deze bureaus ondersteunen lokaal bij de ICT-aspecten van vrijwel alle typen van opsporingsonderzoek. Digitale rechercheurs onderzoeken bijvoorbeeld in beslag genomen computers, laptops, mobiele telefoons, smartphones en digitale fotocamera's op sporen die een misdrijf kunnen helpen oplossen.

Het op de volgende pagina afgebeelde onderzoeksmodel kent fasen voor de voorbereiding, het veiligstellen van sporen, het analyseren en het presenteren van de resultaten. De resultaten moeten kunnen worden gebruikt in een civiele of strafrechtelijke procedure (Zwan, 2009).

5.3.1 Voorbereiding

De forensisch onderzoeker moet zich onder meer afvragen hoe om te gaan met het incident, waar digitale sporen kunnen worden aangetroffen, wie allemaal een rol speelt, wie beslissingen mag nemen, waar de verantwoordelijkheden liggen en wat de juridische kaders zijn. Daarnaast moet bekeken worden of er überhaupt sprake is van wederrechtelijk handelen en opzet, hoewel deze vaststelling ook na het (initiële) onderzoek mag plaatsvinden.

De onderzoeker moet ook vaststellen of hij bevoegd is om onderzoek te verrichten en of toestemming van de eigenaar is verkregen. Bij vermoeden van een beveiligingsincident op bijvoorbeeld een website van een bedrijf, die is ondergebracht op een webserver bij een internet service provider en die gedeeld wordt met anderen, kan niet zonder meer onderzoek worden verricht. In dit voorbeeld is het bedrijf

58. Het onderscheid tussen hackers en crackers is ondertussen achterhaald. In deze handleiding wordt met de term 'hacker' zonder verdere toevoegingen, de kwaadwillende computercrimineel bedoeld.

Voorbereiding
- Formeer onderzoeksteam
- Benoem onderzoeksleider
- Toestemming voor onderzoek
- Communicatie
- Forensic Toolkit

Acquisitie
- Veiligstellen PVI
- Veiligstellen digitale sporen
- Identificeer
- Verpakken
- Transporteren

Analyse
- Dataverificatie
- Logging
- Onderzoek strategie
- Data reductie
- Analyseer

Rapportage
- Rapport
- Evaluatie
- Presentatie
- Verdediging

slechts eigenaar van de website maar niet van de webserver of de telecommunicatienetwerken. Voor een volledig onderzoek zal dus toestemming van de internet service provider nodig zijn.

Een onderzoeksstrategie moet worden bepaald en met de opdrachtgever worden besproken en goedgekeurd. Ook kan het noodzakelijk zijn om in dit stadium de ondernemingsraad te informeren over het onderzoek. Het plan moet aandacht besteden aan de in te zetten onderzoeksmiddelen en een afweging geven waaruit blijkt dat deze voldoen aan de principes voor proportionaliteit (evenredigheid van doel en middelen) en subsidiariteit (gematigdheid bij de inzet van middelen en methoden).

5.3.2 Veiligstellen van digitale sporen

Bij de meeste cyberincidenten beperkt het onderzoek zich tot de plaats veiligheidsinbreuk (PVI) in enge zin. Dat wil zeggen de plaats waar het (vermoedelijke) feit daadwerkelijk is gepleegd, beperkt in omvang. Er wordt alleen technisch onderzoek verricht op enkele betrokken netwerk- en computersystemen of -apparatuur. De eerste diagnose van mogelijke omvang en soort cyberincident en een begrip van de verschillende modus operandi en verschijningsvormen van cybercrime kunnen helpen om plaatsen te identificeren waar (digitale) sporen kunnen worden aangetroffen.

Iedere stap in het onderzoek, door zijn wisselwerking met de omgeving, zal invloed hebben op het te onderzoeken materiaal.[59] Een eerste vraagstuk dient zich aan wanneer besloten moet worden hoe het materiaal veilig te stellen. Stel dat het een desktopcomputer betreft. Zet men het systeem uit en neemt deze mee, of moet het systeem aan blijven staan zoals het werd aangetroffen en als zodanig onderzocht worden? Tenslotte staan gegevens niet alleen op de harde schijf maar ook in tijdelijke werkgeheugens of buffers.

De vluchtigheid van de gegevens is een uitdaging voor de onderzoeker, maar ook de enorme diversiteit aan computerapparatuur en programmatuur. Windows, Unix, Linux, Apple en vele andere besturingssystemen kunnen worden aangetroffen met evenzoveel verschillende bestandstructuren en media. Denk hierbij aan computers, mobiele telefoons, usb-sticks, dvd's, navigatiesystemen, e-mailservers, printservers enzovoorts. Problemen of belemmeringen kunnen ontstaan bij de toegangsbeveiliging, encryptie van gegevensdragers of het onderbreken of verstoren van een actief systeem.

Een bijzondere uitdaging bij het veiligstellen van digitale sporen ontstaat wanneer een aanvaller nog actief blijkt te zijn. Ontdekt de hacker tijdens zijn activiteiten dat het systeem wordt onderzocht, dan wordt het veiligstellen van sporen een zeer onalledaagse klus, zelfs voor experts.

Bij veiligstelling kunnen apparatuur, gegevensdragers of andere goederen in beslag worden genomen. Is inbeslagname niet mogelijk, bijvoorbeeld omdat het systeem niet gemist kan worden of omdat het onderzoek nog heimelijk plaatsvindt, kan ter plaatse een forensische kloon (image) van de betreffende media, bijvoorbeeld de harde schijf, worden gemaakt. Ook als apparatuur wél wordt meegenomen van de PVI kan de onderzoeker besluiten om eerst de gegevens op een harde schijf veilig te stellen door het maken van een forensische kopie.[60]

Het is van essentieel belang dat vanaf het allereerste moment van onderzoek de integriteit en betrouwbaarheid van de (technische) materialen die worden veiliggesteld, wordt gewaarborgd en kan worden aangetoond. De diversiteit aan vindplaatsen plaatst de onderzoeker voor een uitdaging om aantoonbaar te maken dat de verkregen informatie uit het onderzoek een correcte representatie is van de werkelijk aangetroffen gegevens. De bewijslast-

59. Locard's Exchange Theory.
60. Een forensische kopie of image is een exacte bit-voor-bit kopie van het origineel, bijvoorbeeld een harde schijf. Hiermee worden dus ook alle verborgen gegevens en vrije ruimte op de gegevensdrager (slack space en free space) gekloond. De kopie wordt normaal gemaakt op een schoon nieuw medium. Tijdens het maken van het forensisch kopie moet het origineel beveiligd zijn tegen schrijven/modificeren. Hiervoor wordt vaak gebruik gemaakt van speciale hardware zodat er geen twijfel kan bestaan over de integriteit van het origineel.

keten *(chain of evidence)* moet onafhankelijk kunnen worden gecontroleerd.

In ieder onderzoek, ook wanneer het geen strafrechtelijk onderzoek betreft, is het documenteren van iedere stap in het proces en het handhaven van de integriteit van de bewijsmiddelen essentieel. De bewijslastketen mag niet worden onderbroken. Op ieder moment in het proces moet duidelijk en onomstotelijk kunnen worden gemaakt waar een bepaald digitaal spoor is aangetroffen en dat deze na het veiligstellen niet meer is gewijzigd. Uiteindelijk moeten bewijsmiddelen zelfs tot na een eventuele strafrechtelijke proces of een civiele procedure worden bewaard. Dit vergt dus een strikte naleving van procedures en werkinstructie, want een onderzoek en de daarop volgende procedures kunnen over een periode van jaren zijn verspreid.

Om de integriteit van bewijsmiddelen in iedere stap van het proces te kunnen controleren, worden hiervan controlewaarden bepaald. Met deze zogenoemde checksum of hash-waarden kan te allen tijde op een later tijdstip op een onafhankelijke wijze de integriteit van het origineel worden vastgesteld. Verandert er iets in de toestand waarin een bewijsmiddel destijds op een PVI in beslag is genomen, dan kan dat via de checksum worden aangetoond en opgespoord. Van forensische kopieën worden dan ook altijd de hash-waarden bepaald en krijgen digitale sporen en bestanden een digitale handtekening.[61]

De aanbeveling is dan ook om van tevoren een stappenplan te maken voor het veiligstellen van digitale sporen. Vermeld daarbij altijd wie, hoe, wat, waar, wanneer en waarmee die sporen worden veiliggesteld.

Bijlage H geeft een algemeen stappenplan voor het veiligstellen van digitale sporen, zodat de systeembeheerder of verantwoordelijk manager een algemeen beeld krijgt wat er allemaal bij komt kijken. In dit stappenplan is geen rekening gehouden met onderzoeken van vluchtige gegevens die mogelijk aanwezig zijn in het computergeheugen.

Voor meer achtergrondinformatie kan bijvoorbeeld de handleiding ‘Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations’ worden geraadpleegd (U.S. Department of Justice, 2009).

Andere sporen
Vooral in strafrechtelijke onderzoeken, afhankelijk van het vermoeden wat voor cybercrime er is gepleegd, zal ook gezocht worden naar andere sporen. Een onderzoek naar de PVI of op de plaats delict (PD) in ruime zin kan aanvullende aanwijzingen opleveren.
Een onderzoek PVI in ruime zin behelst bijvoorbeeld ook de omgeving en de omstandigheden waarin het computersysteem of apparaat is aangetroffen. Misschien moet een ruimte worden afgezet om vernietiging van fysieke sporen te voorkomen. Zo kunnen materiële sporen (indrukken/afdrukken, stoffen en voorwerpen), immateriële sporen (niet-tastbare, zoals de wijze waarop iets ligt) of dactyloscopische sporen (vingerafdrukken) bijdragen aan de waarheidsvinding.

5.3.3 Analyse
Vrijwel iedere analyse begint met het beperken van de hoeveelheid te onderzoeken data. Dit gebeurt op basis van vaste procedures en met behulp van steekwoorden. De onderzoeker bepaalt de strategie op basis van wat de aangever heeft gemeld bij de aangifte, of van wat de opdrachtgever aan een particulier recherchebureau heeft gevraagd te onderzoeken. Slim gekozen steekwoorden helpen om de te analyseren data in omvang terug te brengen. Zo wordt gericht gezocht naar relevante e-mailberichten, webhistorie en documenten. Daarnaast wordt de filestructuur van de media altijd doorzocht.

Ook tijdens de analysefase is het belangrijk dat iedere stap in het onderzoek wordt gedocumenteerd. Tenminste alle behandeling van originele bewijsmiddelen moet zijn vastgelegd. Maar ook handelingen om sporen te vinden moeten worden verantwoord. De meest gespecialiseerde geautomatiseerde forensische hulpmiddelen bieden hiervoor logboekopties.

Een digitaal forensisch onderzoek zal normaliter nooit worden uitgevoerd aan of op de originele apparatuur of gegevensdragers. Om de bewijslastketen te handhaven wordt van gegevensdragers de hash-waarde berekend en een forensisch identieke kopie gemaakt. Door van het gekloonde exemplaar ook een hash-waarde te berekenen, kan worden vastgesteld of origineel en kopie identiek zijn. Onafhankelijk van elkaar moet dus exact dezelfde hash-waarde kunnen worden bepaald.
Soms zijn er uitzonderingssituaties waarin het digitaal forensisch onderzoek niet anders kan plaatsvinden dan op de originele apparatuur of gegevens. Dit kan noodzakelijk zijn wanneer *RAID-configuraties* met ‘exotische’ controllers of extreem grote opslagmedia worden aangetroffen. De forensische middelen zijn dan mogelijk niet toereikend om kopieën te maken. Er wordt dan ter plaatste onderzoek verricht *(LIVE-forensics)*.

Het technisch onderzoek concentreert zich in eerste instantie op de inhoud van aangetroffen harde schijven, andere gegevensdragers, logbestanden en systeembestanden (*core dumps* of *memory dumps*). De analyse zelf wordt uitgevoerd op beveiligde forensische klonen *(images)* van de betreffende media, zoals hierboven omschreven.

61. Op dit moment geldt SHA-256 als de facto methode om hash-waarden te berekenen.

Bij een digitaal forensisch onderzoek worden vaak grote hoeveelheden gegevens verzameld van de PVI. Een standaard harddisk in een desktop- of laptopcomputer kan al snel honderden gigabyte groot zijn. Onderzoek aan servers of netwerk gekoppelde opslagmedia levert een veelvoud hiervan op. De onderzoeksstrategie moet hierop zijn afgestemd. Zonder efficiënte onderzoeksmethode en gespecialiseerde geautomatiseerde hulpmiddelen is een analyse weinig zinvol. Cruciale digitale sporen worden over het hoofd gezien of simpelweg niet gevonden in de brij van digitale gegevens.

5.3.4 Traceren van de aanvaller

Bij (vermoedens van) een netwerk-cyberaanval moet worden vastgesteld welke IP-adressen bij de aanval zijn betrokken om de identiteit van de mogelijke dader(s) te achterhalen. Daarvoor wordt het spoor teruggevolgd naar een fysiek apparaat (tracing). Hiervoor moeten *DHCP-databases* worden geanalyseerd, MAC-adressen worden opgespoord of informatie worden opgevraagd bij een ISP. Het technisch onderzoek draagt daarmee bij aan de insluitingfase van de incidentopvolging; op basis van de verkregen informatie kunnen gerichte (tijdelijke) beveiligingsmaatregelen worden getroffen.

Het verrichten van naspeuringen buiten het eigen bedrijfsnetwerk kan anderen attenderen of zelfs alarmeren. Bovendien kunnen er juridische beperkingen gelden of mogen bepaalde handelingen alleen worden verricht door de autoriteiten.

5.4 Het rechercheonderzoek

Een (digitaal) forensisch (technisch) onderzoek kan worden ondersteund door of onderdeel zijn van een uitgebreider rechercheonderzoek. Het technisch onderzoek wordt dan aangevuld met getuigenverklaringen, andere gedragingen worden onderzocht en betrokkenen kunnen worden geconfronteerd met de aangetroffen sporen. Het rechercheonderzoek is bedoeld om de dader(s) op te sporen en het motief te achterhalen. Maar rechercheren blijft een proces van objectieve waarheidsvinding.

Een rechercheonderzoek bestaat bijvoorbeeld uit onderzoek van open en gesloten bronnen, gesprekken, buurtonderzoek en waarneming. Het is raadzaam om dergelijke interviews zorgvuldig te plannen, bij voorkeur pas na afronding van het eerste technisch onderzoek. Bij een rechercheonderzoek is de opdrachtgever een belangrijke eerste bron van informatie. Deze kan dienstroosters, sleutelprocedures, een personeelslijst, het bedrijfsreglement en dergelijke verstrekken. De te onderzoeken groep van betrokken personen wordt daarmee al beperkt.

Uitvoering van recherche- en technisch onderzoek is voorbehouden aan bevoegde autoriteiten, dus de politie of andere aangewezen buitengewone opsporingsambtenaren. Zelfstandig uitgevoerd recherche- en technisch onderzoek zijn meestal niet toelaatbaar in een eventuele strafrechtzaak.

Net als bij andere rechercheonderzoeken moeten de onderzoeksmiddelen voor cybercrime voldoen aan de principes van proportionaliteit en subsidiariteit:

- Proportionaliteit: er dient een evenredigheid te zijn tussen het beoogde doel en de geschonden rechtsbelangen van personen (evenredigheid van doel en middelen).
- Subsidiariteit: er dient een gematigdheid te worden gevolgd bij de inzet van middelen en methoden; men kiest altijd het minst ingrijpende middel.

Het technisch en rechercheonderzoek hebben ten doel het verzamelen van materiaal dat als bewijs kan dienen in een gerechtelijke procedure. Een onderzoek maakt in meer of mindere mate inbreuk op grondrechten van de onderzochte perso(o)n(en). Het handelen van organisaties, systeembeheerders en particuliere onderzoeksbureaus moet dus zorgvuldig gebeuren en in overeenstemming zijn met wat in het maatschappelijk verkeer mag worden verwacht. Daarom is bij ieder onderzoek de bescherming van privacy en persoonlijke levenssfeer van betrokken personen belangrijk. De uitvoerende onderzoekers en organisaties moeten de Wet bescherming persoonsgegevens volgen.

5.5 Bescherming van persoonsgegevens bij onderzoeken

Deze paragraaf geeft op hoofdlijnen een uiteenzetting over de Wet bescherming persoonsgegevens (Wbp), voor zover relevant bij het onderzoeken van cyberincidenten. Vooral op welke wijze persoonsgegevens worden verzameld wordt beschreven. Daarvoor worden zowel de verwerking van persoonsgegevens van eigen werknemers als van externen van wie wordt vermoed dat ze een bepaalde vorm van cybercrime hebben gepleegd, behandeld.

In bijlage I is een aantal stappenschema’s opgenomen voor de naleving van de Wbp.

5.5.1 Reikwijdte Wbp

De Wbp is van toepassing op iedere verwerking van persoonsgegevens. In de Wbp staat een rechtmatige en zorgvuldige omgang met persoonsgegevens voorop. De reikwijdte van de Wbp wordt onder meer bepaald door een tweetal definities uit deze wet, ‘persoonsgegevens’ en ‘verwerken’.

Onder een persoonsgegeven wordt verstaan: “elk gegeven betreffende een geïdentificeerd of identificeerbare natuurlijke persoon”.
Dus ook bij een combinatie van gegevens die leiden tot

een identificeerbaar persoon is er sprake van een persoonsgegeven. Wanneer zonder onevenredige inspanning de identiteit van de persoon kan worden vastgesteld, is er sprake van persoonsgegevens.

Onder verwerken wordt verstaan: “elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken (...) of vernietigen van persoonsgegevens”.

5.5.2 IP-adres als persoonsgegeven

Voor cybercrime is een IP-adres in principe een persoonsgegeven. Daarom zijn bij de verzameling, opslag en verwerking van IP-adressen de rechten en plichten volgens de Wbp van toepassing. Op Europees niveau lijkt eenzelfde lijn gevolgd te worden. Is de identiteit van een persoon herleidbaar op basis van diens IP-adres, dan zal in beginsel worden aangenomen dat het gaat om een beschermd persoonsgegeven.

Een recente uitspraak van het College Bescherming Persoonsgegevens (CBP) over de toelaatbaarheid van een zogenoemde *IP-checker* onderstreepte dit. Het CBP stelde in deze zaak dat het IP-adres weliswaar niet altijd door eenieder herleidbaar is tot een individueel persoon, maar dat het toch een persoonsgegeven is, omdat een derde - bijvoorbeeld de internetprovider - eenvoudig de identiteit van de gebruiker kan achterhalen. Hetzelfde geldt voor een bedrijf, dat op basis van interne gegevens makkelijk kan achterhalen welke werknemer bij het betreffende IP-adres hoort.

Een IP-adres hoeft niet altijd als een beschermd persoonsgegeven te worden aangemerkt. Zo zijn groepen van IP-adressen die gekoppeld zijn aan het land van herkomst, geen persoonsgegevens.[62] Een dergelijke koppeling geeft beheerders van webpagina’s de mogelijkheid om hun websites zó in te stellen, dat de gepresenteerde informatie automatisch in de taal van de gebruiker wordt weergegeven. Aangezien deze koppeling van IP-adressen aan de voertaal van de gebruiker niet tot gevolg heeft dat de identiteit van deze persoon direct herleidbaar is, worden deze gegevens niet beschouwd als beschermde persoonsgegevens.

5.5.3 Doelbinding en rechtmatige grondslag

De Wbp kent het beginsel van doelbinding, waardoor de verantwoordelijke voor de verwerking de persoonsgegevens slechts voor bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mag verwerken. Daarnaast mogen de persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met het doel of de doeleinden waarvoor ze zijn verkregen (art. 7 en 9 Wbp). Het principe van doelbinding betekent dat, voordat persoonsgegevens worden verwerkt, de verantwoordelijke voor de gegevensverwerking de plicht heeft concrete doeleinden voor de verwerking(en) te formuleren.

Naast het beginsel van doelbinding geldt dat het doel ook gerechtvaardigd moet zijn. Wannéér er sprake is van een gerechtvaardigd doel, is limitatief omschreven in artikel 8 van de Wbp:

a. ondubbelzinnige toestemming van betrokkenen;
b. noodzakelijk voor de uitoefening van een overeenkomst;
c. noodzakelijk voor het nakomen van een wettelijke verplichting;
d. noodzakelijk ter vrijwaring van een vitaal belang;
e. noodzakelijk voor een goede vervulling van een publiekrechtelijke taak;
f. noodzakelijk voor de behartiging van het gerechtvaardigde belang.

Alleen als de verwerking van persoonsgegevens op één van deze gronden kan worden gebaseerd, is het gerechtvaardigd.

5.5.4 Melding bij CBP

De verantwoordelijke voor de verwerking van persoonsgegevens is in principe verplicht de verwerkingen van persoonsgegevens te melden bij het College bescherming persoonsgegevens (CBP) voordat met de verwerking wordt gestart, tenzij het zogenoemde Vrijstellingsbesluit van toepassing is (Besluit Wbp, 07-05-2001). Voorkomende verwerkingen van persoonsgegevens waarvan het bestaan algemeen bekend mag worden verondersteld en waarvan inbreuk op de privacy onwaarschijnlijk wordt geacht, zijn in het besluit vrijgesteld van melding bij het CBP.

Op basis van dit uitgangspunt moet een particulier recherchebureau zijn aangemeld bij het CBP, want in principe kan bij ieder uitgevoerd onderzoek de verwerking van persoonsgegevens plaatsvinden.

5.5.5 Informatieplicht en rechten betrokkenen

De verantwoordelijke voor de verwerking van de persoonsgegevens is verplicht de betrokkene te informeren over het feit dat er gegevens over hem worden vastgelegd. De betrokkene moet worden geïnformeerd over (art. 33 en 34 Wbp):

- welke persoonsgegevens over hem worden verwerkt;
- met welk doel deze gegevens worden verwerkt;
- wie de ontvangers zijn van zijn persoonsgegevens;
- welke rechten hij kan uitoefenen tegen het feit dat er persoonsgegevens van hem worden verwerkt.

De informatie van de betrokkene mag plaatsvinden (art. 34 lid 1 Wbp):

a. op het moment van vastlegging van hem betreffende gegevens, of

62. Uitspraak CBP 19 maart 2001, kenmerk z2000-0340

b. wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.

Tijdens een rechercheonderzoek is het onwenselijk om de betrokkene in een vroegtijdig stadium te alarmeren. Onder art. 34 lid 1 sub b is het mogelijk om het informeren uit te stellen tot het onderzoeksrapport voor het eerst wordt over-handigd aan de opdrachtgever. Eventueel kan opschorting van de informatieplicht plaatsvinden op grond van de opsporing van strafrechtelijke feiten (art. 43 sub b en d Wbp).

Naast het recht om geïnformeerd te worden heeft degene van wie persoonsgegevens worden verwerkt recht op inlichtingen, inzage, correctie en verzet. De informatieplicht van de verantwoordelijke voor de gegevensbescherming is dus ook een recht van de betrokkene.

5.5.6 Beveiliging van persoonsgegevens

De verantwoordelijke voor de gegevensverwerking is op basis van de Wbp verplicht de persoonsgegevens ook te beveiligen. De Wbp spreekt van “passende technische en organisatorische maatregelen” tegen verlies of tegen enige vorm van onrechtmatige verwerking (art. 13 Wbp). Het begrip ‘passend’ impliceert enerzijds dat de beveiliging in overeenstemming moet zijn met de stand van de techniek, anderzijds dat de proportionaliteitseis geldt. De proportionaliteitseis houdt in dat hoe gevoeliger de gegevens zijn, des te zwaarder de eisen die kunnen worden gesteld aan de gegevensbeveiliging. Het CBP heeft richtlijnen opgesteld in de brochure ‘Beveiliging van persoonsgegevens’ (Blarkom G.W. van, 04-2001).

Voor de verwerking van persoonsgegevens bij een rechercheonderzoek naar een cyberincident kan het beste een zo hoog mogelijke beveiliging worden nageleefd. Maatregelen moeten ten minste voldoen aan het niveau van Wbp risicoklasse II. Systemen waarop de verwerking plaatsvindt moeten zijn versleuteld (encryptie) en voorzien van sterke toegangscontrole (authenticatie met token en wachtwoord/pincode/certificaat). Bestanden voor het onderzoek kunnen bovendien het beste ook nog eens apart worden versleuteld.

5.6 Volgen van werknemers bij vermoeden van cybercrime

Verschillende vormen van cybercrime kunnen (bewust of onbewust) worden veroorzaakt door het computergebruik van eigen medewerkers. Door het oneigenlijk gebruik van het bedrijfsnetwerk, e-mail- of internetfaciliteiten kan het bedrijf schuldig zijn aan het inbreken op websites van anderen, het zich op een ongeoorloofde wijze toegang verschaffen tot afgeschermde informatie of het verspreiden van virussen. Werkgevers kunnen overgaan tot het monitoren van het gebruik van de bedrijfsnetwerken en de gegevens hierover vastleggen om beveiligingsrisico’s te beheersen.

Een werkgever en een werknemer moeten zich ten opzichte van elkaar gedragen als een goed werkgever en een goed werknemer (art. 7:611 Bw). Een werknemer heeft op zijn werkplek bovendien recht op bescherming van zijn privacy. In deze paragraaf wordt uitgelegd hoe een werkgever het computergebruik van zijn medewerkers rechtmatig kan volgen zonder in strijd met de Wbp te handelen.

5.6.1 Gedragscode internet en e-mail

De Wbp stelt dat betrokkenen zijn geïnformeerd over de persoonsgegevens die een verantwoordelijke voor de gegevensverwerking van hen tot zijn beschikking heeft, met welk doel deze gegevens worden verwerkt, dat de gegevensverwerking gerechtvaardigd is en dat de betrokkenen weten welke rechten zij tegen deze gegevensverwerking kunnen uitoefenen. Zonder medeweten van betrokkenen is verwerken van persoonsgegevens niet toegestaan. Wenst een werkgever over te gaan tot monitoren van zijn bedrijfsnetwerk met het doel beveiligingsrisico’s te beperken, dan zal hij op grond van de Wbp maatregelen moeten treffen.

Door monitoren en volgen van het netwerkverkeer op het bedrijfsnetwerk worden gedragingen van werknemers op het internet en het e-mailgebruik inzichtelijk gemaakt. Ook al is het doel van deze controle het minimaliseren van beveiligingsrisico’s, die kunnen ontstaan als gevolg van het handelen van werknemers, betekent dit nog niet dat het gedrag van de werknemers continu mag worden gevolgd. Het stelselmatig volgen of waarnemen van activiteiten van een persoon waarbij inbreuk op de persoonlijke levenssfeer optreedt, is een opsporingstaak en daarmee voorbehouden aan bevoegde autoriteiten (Zwan, 2009).

De werkgever kan wel systematische steekproeven houden. Via een systematische steekproef kunnen medewerkers onder de Wbp worden gevolgd, mits de werkgever zijn werknemers informeert over het gebruikte volgsysteem. De werkgever geeft zijn medewerkers informatie over:
- het toegestane internet- en e-mailgebruik en het feit dat dit internet- en e-mailgebruik door de werkgever wordt gecontroleerd;
- het doel van de gegevensverwerking;
- de consequenties van het niet naleven van de afspraken over het toegestane internet- en e-mailgebruik;
- welke maatregelen worden getroffen - en wanneer - als afspraken over het internet- en e-mailgebruik niet worden nageleefd.

Om aan deze informatieplicht te voldoen adviseert het CBP een ‘Gedragscode Internet en e-mailgebruik’ op te stellen (Terstegge J.H.J., 04-2002). In een gedragscode kan de werkgever de werknemers ook wijzen op de rechten die de werknemers kunnen uitoefenen en dat de gegevens, als een redelijk vermoeden bestaat van het plegen van een strafbaar feit, kunnen worden gebruikt voor het doen van aangifte.

Om de privacy van de werknemers te beschermen kan de monitoring het beste zijn geautomatiseerd, dient men alleen gegevens op te slaan van geanonimiseerd netwerkverkeer en moet de controle worden beperkt tot een eenduidig doel.

5.6.2 Vermoeden van strafbare gedraging

Als na controle via systematische steekproeven het vermoeden bestaat dat een bepaalde werknemer zich schuldig maakt aan het plegen van een strafbaar feit of onrechtmatig het bedrijfscomputernetwerk gebruikt, kan de werkgever de medewerker onderwerpen aan een nader onderzoek. Hierover hoeft de werkgever de betreffende werknemer niet in te lichten. De Wbp voorziet in de uitzondering op de informatieplicht voor de voorkoming, opsporing en vervolging van strafbare feiten (art. 43 sub b Wbp).

Het vermoeden van een strafbare gedraging rechtvaardigt het voor langere tijd volgen van de medewerker door de werkgever. De werkgever heeft dus *niet* de plicht om de betreffende werknemer te informeren over het feit dat er op basis van het vermoeden een nadere controle wordt uitgevoerd. Het is echter wel aan te bevelen in een gedragscode op te nemen dat, zodra er een vermoeden van een onrechtmatige gedraging bestaat, de desbetreffende werknemer voor een bepaalde periode continu kan worden gevolgd.

Bij een vermoeden van een strafbare gedraging kan de werkgever ook het beginsel van de verenigbare doeleinden als niet toepasbaar verklaren. Dit betekent dat, als de verwerking van persoonsgegevens van werknemers verzameld voor minimalisering van beveiligingsrisico's worden gebruikt voor het opsporen van een strafbaar feit, dit niet in strijd is met de Wbp. Beide verschillende doeleinden zouden onverenigbaar zijn.
Tot slot houdt de uitzonderingsbepaling (art. 43 Wbp) in dat de werkgever geen gehoor hoeft te geven als de werknemer een verzoek om inlichtingen of inzage indient.

5.6.3 Rol Ondernemingsraad

Op basis van de Wet op de Ondernemingsraden (WOR) heeft de werkgever instemming van de ondernemingsraad (OR) nodig om maatregelen te kunnen treffen voor gebruik van en omgang met persoonsgegevens (Wet op de Ondernemingsraden, 28-01-1971). Het instemmingsrecht van de OR is ook van toepassing als de werkgever wenst over te gaan op het controleren van het gedrag van zijn werknemers (art. 27 lid 1 sub k en l WOR). Wordt de regeling voor de controle van het computergebruik zonder goedkeuring van de OR door de werkgever doorgevoerd, dan kan de OR deze regeling nietig verklaren (art. 27 lid 5 WOR).

5.7 Vastleggen gegevens externen

In de vorige paragraaf draaide het om het volgen van werknemers om de beveiligingsrisico's, ontstaan als gevolg van oneigenlijk gebruik van het bedrijfsnetwerk door eigen werknemers, te beperken. Beveiligingsrisico's kunnen natuurlijk ook van buitenaf ontstaan.

Als een organisatie persoonsgegevens van externen verwerkt, bijvoorbeeld van websitebezoekers, is de verantwoordelijke van de organisatie ook verplicht om de beginselen en randvoorwaarden van de Wbp te respecteren. Dit betekent dus dat er sprake moet zijn van een concreet en gerechtvaardigd doel voor de verwerking en dat de verwerking in principe ook gemeld moet worden bij het CBP. Vervolgens moeten de externen worden geïnformeerd over het doel van de gegevensverwerking, of de gegevens worden doorgegeven aan derden en over de rechten die in het kader van de Wbp kunnen worden uitgeoefend. Een privacy-statement op de website, goed zichtbaar, of vermeld op een inlogscherm, voldoet aan de eis.

Onder artikel 8 van de Wbp mogen persoonsgegevens van externen niet zonder meer worden verwerkt. Dit betekent dat bijvoorbeeld IP-adressen van websitebezoekers niet zomaar mogen worden vastgelegd omdat die IP-adressen worden aangemerkt als een persoonsgegeven. Deze bepaling staat op gespannen voet met de behoefte om alle websitebezoekers te registeren in logbestanden om misbruik te kunnen opsporen. Zolang er een redelijk belang is, zoals het voorkomen van aanvallen op (de werking van) de website of het (bedrijfs)netwerk, is het vastleggen toegestaan. Alleen als de gehanteerde bewaartermijn en toegang tot de logbestanden in acht wordt genomen.

Worden er gegevens verwerkt om een vorm van cybercrime te herkennen en eventueel aangifte daarvan te doen, dan verdient het aanbeveling om dit expliciet in het privacystatement op te nemen. Dit valt onder de plicht om de betrokkene te informeren over gegevensverstrekking aan derden.
Ook hier geldt dat alleen als de organisatie de persoonsgegevens inderdaad verwerkt als gevolg van verdenking van een strafbaar feit, het beginsel van de verenigbare doeleinden, de plicht om de betrokkenen te informeren en het recht op inlichtingen buiten toepassing kan worden verklaard door de verantwoordelijke van de gegevensverwerking.

5.8 Rapportage

Ieder (formeel) technisch en/of rechercheonderzoek naar een cyberincident moet worden gedocumenteerd volgens deze richtlijnen:

- Bouw een rapport logisch en structureel op.
- Geef feiten chronologisch weer.
- Stel het op in onvoltooid verleden of voltooid tegenwoordige tijd.
- Vermeld hoe het is geconstateerd (ik zag, hoorde, proefde, voelde, rook).
- Neem de toestand van de opstal op, de wijze van binnentreden, de aangetroffen situatie.
- Neem een testimonium de auditu (getuigenverklaring van horen zeggen) op. Voorzie deze verklaring van:
  - het gegeven dat de verklaring in volledige vrijheid is afgelegd;
  - personalia;
  - rol of functie van de persoon;
  - de eigen bewoordingen van betrokkene;
  - hoe constatering is gedaan;
  - dagtekening;
  - ondertekening.

Voor rechtsgeldigheid van de onderzoeksresultaten en de verklaringen van betrokkenen is het belangrijk dat de rapportage snel en persoonlijk door de onderzoeker wordt opgemaakt, is voorzien van een dagtekening en ondertekening van de onderzoeker. Is het een verklaring van een betrokkene, dan moet deze in eigen bewoordingen en vrijwillig door de betrokkene te zijn opgesteld.

Zelf opgestelde rapportages zijn geen bewijsmiddel. In een strafrechtelijke zaak kan het alleen dienen als indirect bewijsmiddel en alleen na acceptatie door de rechter.

HOOFDSTUK 6

Aangifte doen

Welke mogelijkheden voor incidentopvolging heeft een organisatie als zij vermoedt of constateert dat zich een bepaalde vorm van cybercrime heeft voorgedaan? Dit hoofdstuk gaat in op het doen van aangifte en wat daaraan voorafgaat.

6.1 Omgaan met een beveiligingsincident

Is een organisatie slachtoffer van cybercrime, dan moet de organisatie besluiten hoe hiermee wordt omgegaan. De organisatie is daar zelf verantwoordelijk voor. Aangifte is slechts één van de mogelijke acties. Er kan ook worden volstaan met alleen het doen van een melding of het starten van een civiele procedure. Vaak vinden slachtoffers van cybercrime het nodig alleen de schade te beperken en te herstellen en de beveiligingsmaatregelen aan te scherpen.

Er zijn vijf mogelijkheden waarop organisaties met een beveiligingsincident kunnen omgaan:
1. herstellen van de schade en aanscherpen van beveiligingsmaatregelen;
2. doen van melding;
3. strafrechtelijke procedure (aangifte doen);
4. civielrechtelijke procedure;
5. disciplinaire procedure.

De genoemde mogelijkheden sluiten elkaar niet uit. In veel gevallen is een combinatie van stappen mogelijk. De volgorde waarin de stappen worden uitgevoerd is essentieel voor de effectiviteit van de aanpak. Men wil nog digitale sporen kunnen vinden of opsporing en vervolging succesvol afronden.

NCSC adviseert om in geval van cybercrime altijd aangifte te doen. Schakel voor strafrechtelijke procedures direct de autoriteiten (politie) in. Bij twijfel kunt u deskundige hulp inschakelen, bijvoorbeeld van een beveiligingsadviesbureau of een particulier recherchebureau, om het onderzoek te begeleiden of het beveiligingsincident op te volgen.

6.1.1 Herstellen van schade

In veel gevallen kiest een organisatie ervoor om haar beveiligingsmaatregelen aan te scherpen, in combinatie met herstel van de schade. Als wordt overgegaan tot het herstel van de schade, is de kans groot dat gegevens, die noodzakelijk zijn om de cybercrime vast te stellen en/of noodzakelijk zijn voor een strafproces, worden gewist.
Te snel besluiten tot herstellen van de schade kan een strafrechtelijke of civielrechtelijke procedure belemmeren of zelfs onmogelijk maken.

6.1.2 Doen van melding

Bedrijven kunnen ervoor kiezen om alleen melding te doen. Het melden van cybercrime levert een substantiële bijdrage aan het inzichtelijk maken van cybercrime.
De meldingen leveren ook een bijdrage aan de beleidsformulering van diverse (overheids)instanties.
Van een melding wordt geen proces-verbaal opgemaakt. Toch kunnen politie en Openbaar Ministerie besluiten zelf tot onderzoek en vervolging over te gaan.

Voor aanbieders van openbare communicatienetwerken of openbaar beschikbare elektronische communicatiediensten (internet service providers) geldt een meldplicht vanuit de Europese Unie-richtlijn 2009/140/EG om de bevoegde nationale regelgevende instantie in kennis te stellen van elke inbreuk op de veiligheid of elk verlies van integriteit die een belangrijke impact had op de exploitatie van netwerken of diensten.

Daarnaast geldt een meldplicht vanuit de EU-richtlijn 2009/136/EG voor aanbieders van openbare elektronische communicatiediensten om, zodra een inbreuk van persoonsgegevens optreedt, de bevoegde nationale instantie zonder onnodige vertraging daarvan in kennis te stellen. Heeft de inbreuk ongunstige gevolgen voor de persoonsgegevens en persoonlijke levenssfeer van een abonnee of een individuele persoon, dan stelt de aanbieder ook de bedoelde abonnee of individuele persoon onmiddellijk van de inbreuk in kennis.
Een betrokken abonnee of individuele persoon op de hoogte stellen is niet vereist wanneer de aanbieder, tot voldoening van de bevoegde instantie, heeft aangetoond dat hij de gepaste technische beschermingsmaatregelen heeft genomen en dat deze maatregelen (encryptie) werden toegepast op de data die bij de beveiligingsinbreuk betrokken waren.
Er is vooralsnog geen nationale algemene meldplicht voor ernstige datalekken.

6.1.3 Strafrechtelijke procedure (aangifte doen)

Wenst een organisatie dat een opsporingsonderzoek plaatsvindt, dan moet aangifte worden gedaan bij de plaatselijke politie. Een aangifte is een juridisch formele melding van een strafbaar feit aan de politie. De politie maakt hiervan een proces-verbaal op. De beslissing of er daarna ook daadwerkelijk vervolging wordt ingesteld ligt bij het Openbaar Ministerie en zal worden bepaald door de Officier van Justitie.

Bij het doen van aangifte volgt een strafrechtelijke procedure waarbij mogelijk gegevens over de zaak openbaar worden. Bovendien wordt apparatuur waarop digitale sporen staan uitgeschakeld voor onderzoek. Eventueel worden deze apparaten voor geruime tijd in beslag genomen. Het is belangrijk dat een organisatie zich dit realiseert en is voorbereid op het ondersteunen van onderzoeken, bijvoorbeeld door te kunnen uitwijken naar schaduwsystemen.

Als besloten wordt om aangifte te doen, dan is het voor opsporing van groot belang dat gegevens niet worden gewijzigd of aangepast. Dit kan opsporing aanzienlijk bemoeilijken, vertragen of zelfs onmogelijk maken. Bij aangifte kan de politie al met een eerste concreet advies komen.

6.1.4 Civielrechtelijke procedure

Wil de organisatie de schade vergoed krijgen en beschikt zij over de identiteit van de dader, dan kan de organisatie kiezen voor een civielrechtelijke procedure.[63] Voor een civiele procedure wordt het technisch onderzoek uitgevoerd onder eigen verantwoordelijkheid, met inachtneming van de wettelijke kaders, en eventueel met ondersteuning van een particulier recherchebureau of security-specialisten uit de private sector.

Wordt gekozen voor een civielrechtelijke procedure - in plaats van aangifte doen bij de politie - dan zal de zaak eveneens in de openbaarheid kunnen komen. Echter de kans dat apparatuur langdurig niet beschikbaar is gedurende het onderzoek is kleiner. Bovendien behoudt de organisatie meer grip op het verloop van de procedure.

6.1.5 Disciplinaire procedure

Als blijkt dat het beveiligingsincident is veroorzaakt door een eigen medewerker, kan de organisatie kiezen voor een interne disciplinaire procedure. Voor een interne procedure is het raadzaam om het technische en eventueel recherche-onderzoek, met inachtneming van de wettelijke kaders, te laten uitvoeren door een particulier recherchebureau. Hiermee wordt de onafhankelijkheid van het onderzoek gewaarborgd, omdat een recherchebureau gebonden is aan bepaalde richtlijnen.

Wanneer het incidentonderzoek leidt tot achterhalen van de identiteit van de dader en de organisatie wenst op te treden, kunnen disciplinaire maatregelen worden opgelegd of ontslag worden aangezegd, afhankelijk van de zwaarte van het incident. Eén en ander moet wel zijn vastgelegd in het bedrijfsreglement en moet met instemming van de ondernemingsraad plaatsvinden. Bovendien bestaat altijd de kans dat de betrokken persoon zelf een civielrechtelijke procedure begint tegen de organisatie.

6.2 Het doen van aangifte

Wanneer een persoon of organisatie constateert of vermoedt dat zich een bepaalde verschijningsvorm van cybercrime heeft voorgedaan en deze is aangemerkt als een strafbaar feit, kan aangifte worden gedaan. Uiteraard moet voor het doen van aangifte informatie beschikbaar zijn in de vorm van gegevens, op basis waarvan een opsporingsonderzoek door opsporingsambtenaren ingesteld kan worden. Deze gegevens moeten informatie geven over het soort delict, wanneer en waar dit is gepleegd en met eventuele aanwijzing van een dader of daders.

De bepalingen voor het doen van aangiften (en klachten) staan in het Wetboek van Strafvordering, Titel I, art. 160 e.v. De bepalingen omvatten niet alleen regels over de vraag wie er aangifte kan doen of wie een aangifte kan opnemen, maar ook dat men in sommige gevallen verplicht is om aangifte te doen. Daarnaast wordt in het wetboek beschreven hoe een aangifte moet worden opgenomen (art. 163 t/m 166a Sv).

Deze paragraaf geeft beknopt weer wie aangifte kan doen en op welke wijze dit kan gebeuren. Vervolgens wordt beschreven welke informatie met betrekking tot cybercrime nodig is om succesvol aangifte te kunnen doen. Daarna wordt beschreven bij welke opsporingsambtenaren aangifte kan worden gedaan en welke plichten en bevoegdheden zij hebben.

6.2.1 Verplichting en bevoegdheid

Iedereen die kennis draagt van een strafbaar feit is volgens artikel 161 van het Wetboek van Strafvordering bevoegd tot het doen van aangifte.

In sommige gevallen is men zelfs verplicht om aangifte te doen. Dit is het geval bij sommige, met name genoemde, ernstige misdrijven (art. 160 Sv). Dit zijn geen misdrijven van cybercrime in enge zin. Wanneer ICT-voorzieningen worden misbruikt en hierbij vermoedens van een, met name genoemd, ernstig delict bestaat, geldt wél de verplichting tot het doen van aangifte.[64]

6.2.2 Volgorde bij aangifte doen

Wanneer aangifte wordt gedaan van cybercrime volgt de politie hierbij een procedure die bestaat uit het opnemen van de aangifte, een vervolggesprek, een technisch onderzoek en een prioritering (zie volgende pagina). De daadwerkelijke stappen die worden doorlopen kunnen hiervan afwijken afhankelijk van de situatie, noodzakelijkheid, beschikbaarheid bij de politie of andere reden.

Bij de opname van de aangifte zal aan de aangever om diverse gegevens van het gepleegde feit worden gevraagd, of de eigenaar en/of benadeelde wanneer deze een ander is dan de aangever. De initieel aangeleverde informatie wordt door de politie meegewogen in de beoordeling of de zaak in behandeling wordt genomen *(case screening)*.

Bijlage F geeft een overzicht van de algemene en technische gegevens die nodig zijn voor het vaststellen van het feit en het doen van de aangifte. Daarnaast kan om een beschrijving van de gebeurtenissen en om technische achtergrondinformatie gevraagd worden.

De aangifte

Aangifte doet u in uw eigen woorden. Voor het politieonderzoek is het van groot belang dat ook de kleinste details in de aangifte staan. De aangifte wordt in eerste instantie opgenomen door een opsporingsambtenaar, werkzaam binnen de basispolitiezorg. De aangever komt dus op het politiebureau aangifte doen. Deze opsporings-

63. De eis voor schadevergoeding kan ook worden gevoegd in het strafproces, of het strafvonnis kan worden afgewacht waarna de zaak voor schadevergoeding wordt voorgelegd aan een civiele rechter.

64. De verplichting tot het doen van aangifte geldt voor de artikelen 92-110 van het Wetboek van Strafrecht, in Titel VII van het Tweede Boek van dat Wetboek, voor zover daardoor levensgevaar is veroorzaakt, of in de artikelen 287 tot en met 294 en 296 van dat wetboek, van mensenroof of van verkrachting.

ambtenaar, de verbalisant, heeft algemene basiskennis, maar zeer waarschijnlijk geen technisch inhoudelijke kennis. De verbalisant neemt een summiere aangifte op, zonder alle technische details. Hierbij noteert de verbalisant slechts het verhaal van de aangever zonder in te gaan op technische details.

Bij het opnemen van de aangifte zal om informatie worden gevraagd die gebaseerd is op de wettekst en dus op de elementen van het strafbare feit, zoals:

- Betreft het een aangifte tegen een particulier of een bedrijf?
- Zijn er beveiligingsmaatregelen genomen?
- Wat is de geschatte schade (uren in geld, immateriële schade) en wat zijn de herstelkosten?
- Een beschrijving van de (technische) situatie
- Is er al een verdachte bekend?

Na het opnemen van de aangifte stelt de verbalisant indien nodig een digitaal rechercheur van zijn district/regio op de hoogte van de aangifte. Er komen ook steeds meer situaties voor waarbij een digitaal rechercheur direct bij de aangifte betrokken is.

De verbalisant of digitaal rechercheur geeft de aangever het advies om alle mogelijk relevante gegevens (zoals logbestanden) te bewaren en om de apparatuur uit te zetten en niet te gebruiken totdat een onderzoek is afgerond. Het advies van de opsporingsambtenaar hoeft niet volledig en juist te zijn om digitale sporen veilig te stellen! U kent uw eigen systemen het beste. De aangever/eigenaar zal er zelf dus ook alert op moeten zijn om mogelijke sporen niet te wissen of aan te passen.

Vervolggesprek met aangever

Voor het verzamelen van relevante technische informatie volgt een gesprek met en/of bezoek aan de aangever door een digitaal rechercheur. Tijdens het bezoek wordt geprobeerd de informatie te krijgen die nodig is om te bepalen wat er feitelijk technisch is gebeurd.

De digitaal rechercheur wil dan de technische omgeving leren kennen, zoals de soort omgeving, de gebruikte besturingssystemen en applicaties, de netwerktopologie, koppelingen met (externe) netwerken, soorten gebruikers en de aanwezige beveiligingssystemen en -maatregelen. De rechercheur wil een beeld krijgen van de organisatie en de bedrijfsprocessen die schade hebben ondervonden van het cyberincident. Daarnaast zal om een specificatie van de ondervonden schade worden gevraagd, zoals economische schade, verlies van (gevoelige of persoons)gegevens, maatschappelijke impact of het totale verlies aan beschikbaarheid van de services (down time).

Uiteraard wil de digitaal rechercheur de plaats veiligheidsinbreuk (PVI) zien en vaststellen. Daarnaast wil de rechercheur zich een beeld vormen van de eventuele acties die al zijn uitgevoerd en handelingen die aan betrokken systemen zijn verricht. Welke systemen zijn gecompromitteerd? Wat zijn dit voor systemen, wat is hun functie? Hoe en door wie werd geconstateerd dat het systeem is gecompromitteerd?

In sommige situaties is de aanvaller nog actief op het systeem. Kan de aanvaller dan worden gevolgd? Is het mogelijk om actief te monitoren op de acties die de aanvaller uitvoert? De digitaal rechercheur zal deze mogelijkheid willen gebruiken om de identiteit van de dader te achterhalen.

De verzamelde informatie wordt toegevoegd aan de aangifte. Deze informatie wordt meegewogen in de beoordeling of de zaak verder in behandeling wordt genomen. Als wordt besloten een strafrechtelijk onderzoek te starten op grond van de gegevens volgt het feitelijke technisch onderzoek.

Technisch onderzoek

Het technisch onderzoek wordt meestal uitgevoerd door een regionaal Bureau Digitale Expertise. Daarnaast kan het onderzoek samen met of door het Team High Tech Crime van het KLPD worden gedaan. Dit wordt mede bepaald door de informatie die tot dan toe beschikbaar is en het type misdaad. De focus van het NHTCU ligt voornamelijk op de zogenaamde level 3-zaken waarbij er sprake is van georganiseerde criminaliteit, (inter)nationaal karakter, vitale infrastructuren en/of een hoge mate van inventiviteit of innovatie.

Bij het technisch onderzoek wordt onder meer onderzoek verricht op de aangetroffen gegevensdragers op de PVI.

Naast bewijsmateriaal van de aangever kan gedurende het onderzoek ook een verdachte of derde partijen, zoals een internet service provider, in beeld komen.
Paragraaf 5.3 gaat in op de uitvoering van een technisch onderzoek.

Prioritering
De kerntaak van het Openbaar Ministerie is de strafrechtelijke handhaving van de rechtsorde. Samen met de politie maakt het OM keuzes: welke zaken moeten worden aangepakt en op welke manier, en of het strafrecht het meest geëigende instrument is voor een bestuurlijke of een op preventie gerichte aanpak.

Het College van Procureurs-Generaal stelt met instemming van de Minister van Veiligheid en Justitie landelijke prioriteiten vast voor het opsporings- en vervolgingsbeleid. Prioriteiten komen bijvoorbeeld voort uit internationale afspraken of beleid. Op landelijk niveau gaat het om de aanpak van de zware, georganiseerde criminaliteit waarvan ICT-voorzieningen het doelwit zijn. Deze zaken worden afgehandeld door het Landelijk Parket. Ook gaat het om grote zaken, gericht op georganiseerde criminaliteit, waar fraude en financiële geldstromen deel van uitmaken.

Op bovenregionaal niveau gaat het om veelal traditionele vormen van criminaliteit, die met ICT via de digitale snelweg worden gepleegd. Een groot deel bestaat uit middelzware fraudezaken. Daarnaast is er een categorie niet-fraudedelicten, zoals bijvoorbeeld kinderporno, computerinbraak en/of phishing.

Op regionaal niveau gaat het de politie om zaken waarbij (lokale) ondernemingen of gewone burgers slachtoffer zijn geworden van cybercrime. Dit betekent in ieder geval dat een deel van de zaken vraagt om een lokale aanpak. Het gaat hier om de lichtere zaken die in hoge mate lokaal gebonden zijn. De lokale, regionale en landelijk vastgestelde prioriteiten spelen een grote rol bij de beoordeling van de aangifte.[65]

6.2.3 Aangifte doen: bij wie en waar?

Slachtoffers van een delict kunnen het beste zo snel mogelijk aangifte doen bij het eigen lokale politiekorps. De aangifte kan zowel mondeling als schriftelijk worden gedaan, hetzij door de aangever zelf of door iemand die door de aangever *schriftelijk* is gemachtigd.

Aangifte kan worden gedaan bij:
- de Officier van Justitie van het arrondissement waar het feit is gepleegd;
- elke (algemeen) opsporingsambtenaar;
- buitengewoon opsporingsambtenaren die hiervoor opsporingsbevoegdheid hebben verkregen.

Gebruikelijk is dat aangifte bij een algemeen opsporingsambtenaar, de politie, wordt gedaan. Politieambtenaren zijn verplicht om de aangifte op te nemen of te ontvangen, zoals in artikel 163 van het Wetboek van Strafvordering is gesteld. Normaal wordt aangifte gedaan in de plaats waar het feit heeft plaatsgevonden.

Voor het opnemen van een aangifte van cybercrime is in beginsel algemene kennis voldoende om de basisgegevens te verzamelen en vast te leggen. Voor de specifieke gegevens van de verschillende verschijningsvormen van cybercrime is meer specialistische kennis nodig. Niet iedere opsporingsambtenaar beschikt over deze kennis. Voor deze specifieke kennis kan de opsporingsambtenaar een beroep doen op ondersteuning van het personeel van de Technische Recherche, het Bureau Digitale Expertise of het Team High Tech Crime van het KLPD. Zij kunnen de lokale politie assisteren bij het in te stellen onderzoek of het zelfstandig verder uitvoeren.

In sommige politieregio's is het mogelijk om telefonisch of digitaal aangifte te doen via het internet. Dit betreft alleen enkele met name genoemde feiten. De 'cybercrime-feiten' horen daar (nog) niet bij.[66] Gelet op de complexiteit van de materie is het raadzaam om mondeling of schriftelijk in persoon aangifte te doen.

6.3 Contactgegevens

Politiekorpsen en arrondissementen
Het *algemeen* meldnummer van de Nederlandse politie is **0900-8844** (lokaal tarief). Alle politiekorpsen zijn bereikbaar via dit nummer. U kunt dit nummer gebruiken om aan te geven dat u aangifte wilt doen. U krijgt dan de informatie waar u dat het beste kunt doen.

Hebt u informatie over een misdrijf of een dader en wilt u absoluut anoniem blijven? Bel dan met Meld Misdaad Anoniem op **0800-7000**.

Op de algemene website www.politie.nl vindt u meer informatie over het regiopolitiekorps waaronder uw organisatie valt.

Op de website www.openbaarministerie.nl vindt u meer informatie over de arrondissementen. Het Landelijk Parket in Rotterdam houdt zich in het bijzonder bezig met de (internationale) georganiseerde criminaliteit en heeft een kennis- en expertisecentrum voor cybercrime, telecommunicatie en digitale opsporing: www.om.nl/onderwerpen/cybercrime.

65. http://www.om.nl/onderwerpen/cybercrime/cybercrimeartikelen/versterking_aanpak/
66. In 2010 is een initiatief gestart in de politieregio Flevoland voor het ontwikkelen van een landelijk digitaal bedrijvenloket cybercrime.

Meldingen

Het KLPD heeft een Meldpunt Cybercrime waar burgers melding kunnen maken van kinderporno en radicale en terroristische uitingen die zij op het internet tegenkomen: www.meldpuntcybercrime.nl.

Voor het melden van identiteitsfraude kunt u terecht bij het Centraal Meld- en Informatiepunt Identiteitsfraude: http://www.overheid.nl/identiteitsfraude. Het CMI zorgt dat de juiste instanties uw melding afhandelen.

Het Meldpunt Internetoplichting van de politie en het Openbaar Ministerie samen met Marktplaats.nl maakt het voor burgers mogelijk om online melding en aangifte te doen van internetoplichting: https://www.mijnpolitiebureau.nl/if.shtml.

Een klacht over spam kan worden ingediend bij de OPTA, die deze meldingen gebruikt voor handhaving van het spamverbod: www.spamklacht.nl.

Meldingen over discriminatie kunnen ook worden gedaan bij het 'Meldpunt Discriminatie Internet' van de stichting Magenta: http://www.meldpunt.nl.

Bijlagen

Literatuur

Auteurswet. 23-09-1912.
Wet van 23 september 1912, houdende nieuwe regeling van het auteursrecht. Den Haag: Koninkrijk der Nederlanden, 23-09-1912.

Besluit universele dienstverlening en eindgebruikersbelangen. 2004.
Besluit van 7 mei 2004, houdende regels met betrekking tot universele dienstverlening en eindgebruikersbelangen (Besluit universele dienstverlening en eindgebruikersbelangen). Den Haag: Koninkrijk der Nederlanden, 2004.

Besluit Wbp. 07-05-2001.
Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens. Den Haag: Ministerie van Justitie, 07-05-2001. Vrijstellingsbesluit Wbp.

Blarkom G.W. van, Borking J.J. 04-2001.
Beveiliging van persoonsgegevens. Den Haag: Registratiekamer, 04-2001. Achtergrondstudies en Verkenningen 23.

Carvey, Harlan. 2007.
Windows Forensic Analysis. s.l.: Syngress, 2007.

Council of Europe. 2001.
Convention on Cybercrime. Budapest: Council of Europe, 2001. ETS No 185.

Engelfriet, Arnoud. 2007.
De Wet Computercriminaliteit. *Ius mentis.* [Online] ICT-jurist Arnoud Engelfriet, 7 27, 2007. http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/cybercrime/.

Engelfriet, Arnoud. 2008.
Elektronisch briefgeheim: de stand van zaken. *Ius mentis.* [Online] ICT-jurist Arnoud Engelfriet, 2008. http://www.iusmentis.com.

Europese Commissie. 31 juli 2002.
Europese Richtlijn privacy en elektronische communicatie. 31 juli 2002. 2002/58/EG, PbL 201.

GOVCERT.NL. 02-2005.
Aanbevelingen ter bescherming tegen Denial of Service aanvallen. Den Haag: s.n., 02-2005.

GOVCERT.NL. 03-2009.
Beveiliging van mobiele apparatuur en gegevensdragers. Den Haag: s.n., 03-2009.

GOVCERT.NL. 28-09-2009.
Factsheet FS-2008-01 Draadloze netwerken. Den Haag: s.n., 28-09-2009.

GOVCERT.NL. 23-06-2008.
Factsheet FS-2008-05 Massale SQL injectie aanvallen. Den Haag: s.n., 23-06-2008.

GOVCERT.NL. 21-01-2011.
Factsheet FS-2010-02, Stuxnet - een geavanceerde en gerichte aanval. Den Haag: GOVCERT.NL, 21-01-2011.

GOVCERT.NL. 21-03-2008.
Intrusion Detection Systems. Den Haag: GOVCERT.NL, 21-03-2008. v1.2.

GOVCERT.NL. 30-07-2008.
Whitepaper DNS misbruik, van herkenning tot preventie. Den Haag: s.n., 30-07-2008.

GOVCERT.NL. 11-11-2009.
Whitepaper Raamwerk Beveiliging Webapplicaties. Den Haag: GOVCERT.NL, 11-11-2009.

Grondwet. 1815.
Grondwet voor het Koninkrijk der Nederlanden van 24 augustus 1815. s.l.: Koninkrijk der Nederlanden, 1815.

Helmus S.,Kool L., Smulders A., Zee, van der F. 25-9-2006.
ICT-veiligheidsbeleid in Nederland - een quickscan. Delft: TNO, 25-9-2006.

Hulst, van der, R.C., Neve, R.J.M. 2008.
High-tech crime, soorten criminaliteit en hun daders. ministerie van Jusititie. Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum, 2008. ISBN 978 90 5454 998 7.

Jörg, N. en Kelk C. 1994.
Strafrecht met mate. Arnhem: Gouda Quint b.v., 1994.

Kamerstukken 1989/90, 21551. 1989-1990.
Kamerstukken 1989-1990, 21551, nr. 3. Den Haag: Tweede Kamer der Staten-Generaal, 1989-1990.

Kamerstukken 2004/05, 26671. 2005.
Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II). Den Haag: Tweede Kamer der Staten-Generaal, 2005. Kamerstukken II 2004/05, 26671 nr.10.

KLPD Dienst Nationale Recherche. 2009.
High tech crime; Criminaliteitsbeeldanalyse. s.l.: Korps landelijke politiediensten, 2009.

Koops, Bert-Jaap. 2003/5.
De Code voor Informatiebeveiliging naar Nederlands recht. s.l.: Informatiebeveiliging 2003/5, p. 20-24., 2003/5.

Koops, Bert-Jaap. 2003.
Het Cybercrime-verdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij. s.l.: Centrum voor rechtn bestuur en informatisering, 2003. Computerrecht, 02, 115-123.

Leukfeldt E.R., Domenie M.M.L., Stol W. 2010.
Verkenning cybercrime in Nederland 2009. Den Haag: Boom Juridische uitgevers, 2010. Vol. Veiligheidsstudies.

Meulen, N.S. van der. december 2010.
Fertile Grounds: The Facilitation of Financial Identity Theft in the United States and the Netherlands. s.l.: Universiteit van Tilburg, december 2010.

NAVI. juni 2009.
Leidraad uitwisseling van gevoelige informatie. Den Haag: Nationaal Adviescentrum Vitale Infrastructuur, juni 2009. https://www.navi-online.nl/services/Proxy/kennisbank/id/303.

Nijboer, Cleiren &. 2002.
Tekst & Commentaar Strafrecht, art. 161sexies Sr. 2002. aant. 10e.

Nijboer, Cleiren &. 2002.
Tekst & Commentaar Strafrecht, art. 350 Sr. 2002. aant. 9c.

Ollmann, Gunter. 2007.
The Phishing Guide - Understanding & Preventing Phishing Attacks. s.l. : IBM Internet Security Systems, 2007.

OWASP. 2010.
Open Web Application Security Project. [Online] OWASP Foundation, 11 2010. http://www.owasp.org/index.php/Main_Page.

Randal Vaughn, Gadi Evron. 17-03-2006.
DNS Amplification Attacks. 17-03-2006.

Regeling pbr. 03-03-1999.
Regeling particuliere beveiligingsorganisaties en recherchebureaus. Den Haag: Koninkrijk der Nederlanden, 03-03-1999.

Schultz E., Shumway R. 2002.
Incident Response. A strategic guide to handling system and network security breaches. s.l.: New Riders, 2002.

Terstegge J.H.J., Lieon S. 04-2002.
Goed werken in netwerken. Regels voor controle op email en Internet-gebruik van werknemers. Den Haag: College Bescherming Persoonsgegevens, 04-2002. Achtergrondstudies en Verkenningen 21.

Tw. 19 oktober 1998.
Telecommunicatiewet. Den Haag: Koninkrijk der Nederlanden, 19 oktober 1998.

U.S. Department of Justice. 2009.
Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. s.l.: Computer Crime and Intellectual Property Section Criminal Division, 2009.

Wbp. 06-07-2000.
Wet bescherming persoonsgegevens. Den Haag: Koninkrijk der Nederlanden, 06-07-2000. Staatsblad 06-07-2000, nr 302.

Wet op de Ondernemingsraden. 28-01-1971.
Wet van 28 januari 1971, houdende nieuwe regelen omtrent de medezeggenschap van de werknemers in de onderneming door middel van ondernemingsraden. Den Haag: Koninkrijk der Nederlanden, 28-01-1971.

Wetboek van Strafrecht. 03-03-1881.
Wetboek van Strafrecht. s.l.: Koninkrijk der Nederlanden, 03-03-1881.

Wetboek van Strafvordering. 15-01-1921.
Wetboek van Strafvordering. s.l.: Koninkrijk der Nederlanden, 15-01-1921.

Wpbr. 24-10-1997.
Wet particuliere beveiligingsorganisaties en recherchebureaus. Den Haag: Koninkrijk der Nederlanden, 24-10-1997.

Zwan, E. van der. 2009.
Besnuffeld door de baas: juridische aspecten van preventief monitoren en digitaal onderzoek. Platform voor Informatiebeveiliging. 2009, Vol. november 2009.

Zwan, E. van der. 2010.
Security of Industrial Control Systems: What to Look for? ISACA Online Journal. 2010, Vol. augustus 2010.

Afkortingen

A

ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
AT	Agentschap Telecom

B

B2C	Business to consumer
BCM	Business Continuity Management
BCP	Best Current Practice
BDE	Bureau Digitale Expertise
BGP	Border Gateway Protocol
BOA	Buitengewoon opsporingsambtenaar
Bw	Burgerlijk Wetboek
BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

C

CBP	College Bescherming Persoonsgegevens
CCTV	Closed Circuit Television
CCV	Cybercrime Verdrag
CD-ROM	Compact Disk Read Only Memory
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPU	Centrale Processor Unit
COTS	Commercial Off The Shelf

D

DCS	Distributed Control System
DDoS	Distributed Denial of Service
DGET	Directoraat-Generaal Energie en Telecom
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoS	Denial of Service
DVD	Digital Video (Versatile) Disk

E

EH	Elektronische Handtekening
EL&I	Ministerie van Economische Zaken, Landbouw & Innovatie
EMS	Energy Management System
ERP	Enterprise Resource Planning

F -

G

GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communication

H

HMI	Human Machine Interface
HSDPA	High Speed Downlink Packet Access
HTTP	Hypertext Transfer Protocol

I

IB	Informatiebeveiliging
ICT	Informatie en Communicatie Technologie
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSEC	IP Security Protocol
IRC	Internet Relay Chat
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library

J -

K

KA	Kantoorautomatisering
KLPD	Korps Landelijke Politiediensten

L

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol

M

MAC	Media Access Control adres
MAN	Metropolitan Network
MES	Manufacturing Execution System
MSN	The Microsoft Network

N

NAT	Network Address Translation
NAVI	Nationaal Adviescentrum Vitale Infrastructuur
NCC	Nationaal Crisis Centrum
NCTb	Nationaal Coördinator Terrorismebestrijding
NHTCU	National High Tech Crime Unit

O

OA	Opsporingsambtenaar
OLE	Object Linking and Embedding
OM	Openbaar Ministerie
OPC	OLE for Process Control
OPTA	Onafhankelijke Post en Telecommunicatie Autoriteit
OSI	Open Systems Interconnection
OSN	Online Sociale Netwerken
OTAP	Ontwikkel-, Test-, Acceptatie- en Productieomgeving
OvJ	Officier van Justitie

P

P2P	Peer-to-peer communicatie
PA	Procesautomatisering
PAT	Port Address Translation
PCN	Process Control Network
PCS	Process Control System
PD	Plaats Delict
PDA	Personal Digital Assistant
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSTN	Public Switched Telephone Network
p-v	proces-verbaal
PVI	Plaats Veiligheid Inbreuk

Q -

R

RAID	Redundant Array of Independent Disks
RFID	Radio Frequency Identification
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RTU	Remote Terminal Unit

S

SAAS	Software as a Service
SCADA	Supervisory Control And Data Acquisition
SIEM	Security Information and Event Management
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOVI	Strategisch Overleg Vitale Infrastructuur
Sox	Sarbanes-Oxley
SPIM	Spam via instant messaging
SPIT	Spam via internettelefonie
SPOC	Single Point of Contact
SPOF	Single Point of Failure
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering

T

TCP/IP	Transmission Control Protocol / Internet Protocol
Tw	Telecommunicatiewet

U

UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
URL	Uniform Resource Locators
USB	Universal Serial Bus

V

VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst - Bijzondere Informatie
VoIP	Voice-over-IP
VPN	Virtual Private Network

W

WAN	Wide Area Network
Wbp	Wet bescherming persoonsgegevens
Weh	Wet elektronische handtekeningen
WIPS	Wireless Intrusion Detection System

X -

Y -

Z -

Overzichtstabel Cybercrime

Deze bijlage geeft een overzicht van de belangrijkste strafrechtelijke bepalingen voor verschijningsvormen van cybercrime in enge zin.

Verschijningsvorm cybercrime	138ab *lid 1*	138ab *lid 2*	138ab *lid 3*	138b	139c *lid 1*	139d	139e	161 *sexies*	161 *septies*	350a *lid 1*	350a *lid 2*	350a *lid 3*	350b *lid1*	350b *lid2*
• Malware														
Malware maken en/of verspreiden	X					X		X	X	X	X	X	X	X
Malware (Trojaanse paarden) gebruiken	X	X			X			X	X	X	X	X	X	
• Computerinbraak														
Computerinbraak (hacking)	X		X								X			
Computerinbraak vervolg-handelingen		X	X		X	X	X	X	X	X	X	X		
Portscan						X								
Spoofing/cache poisoning	X	X		X	X	X	X	X		X	X			
Sniffing					X	X	X			X				
Draadloze netwerken hacken/ misbruiken	X	X	X	X	X		X	X		X	X			
Password guessing	X			X		X								
• Website aanvallen														
Veroorzaken open relay									X				X	
Wederrechtelijk open relay gebruiken	X							X		X				
Defacing/vernielen website	X							X	X	X			X	
Defacing/doorleiden internet-verkeer	X							X	X	X				
Cross-site scripting	X	X			X	X	X	X		X			X	
SQL-injecties	X	X						X		X				
• Botnets														
Botnet bouwen en beheren	X	X	X		X					X		X		
• Denial of Service														
DDoS-aanval				X				X		X			X	
• Social Engineering														
Phishing		X			X		X							
Vishing/Smishing		X			X									
• E-mail gerelateerd														
Wederrechtelijk open mail relay gebruiken	X							X	X	X				
Spamming (met DoS tot gevolg)				X				X	X				X	

Toelichting overzichtstabel Cybercrime

Art. 138ab lid 1 Sr
Opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk *(computervredebreuk of hacken)*.

Art. 138ab lid 2 Sr
Het overnemen van opgeslagen gegevens in een geautomatiseerd werk nadat, als bedoeld in lid 1, is binnengedrongen.

Art. 138ab lid 3 Sr
Via een openbaar telecommunicatienetwerk opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk en vervolgens zichzelf of anderen bevoordelen door gebruik te maken van het geautomatiseerd werk of verder te hacken naar het geautomatiseerd werk van een derde (zoals bij een proxy of springplankeffect via een botnet).

Art. 138b Sr
Opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren door daaraan gegevens aan te bieden of toe te zenden (zoals bij Denial of Service).

Art. 139c lid 1 Sr
Opzettelijk en wederrechtelijk aftappen en/of opnemen van gegevens met behulp van een technisch hulpmiddel (aftappen of afluisteren).

Art. 139d lid 1 Sr
Plaatsen van een technisch hulpmiddel voor het wederrechtelijk opnemen of afluisteren van een geautomatiseerd werk bijvoorbeeld opname-, aftap- c.q. afluisterapparatuur *(sniffing)*.

Art. 139d lid 2 Sr
Het vervaardigen, verkopen, verwerven of anderszins ter beschikking hebben of stellen van een technisch hulpmiddel, toegangscodes of wachtwoorden met het oogmerk computerinbraak (art. 138ab), een DoS-aanval (art. 138b) of aftappen (art. 139c) te plegen (voorbereidingshandelingen of misbruik van hulpmiddelen).

Art. 139d lid 3 Sr
Het verkopen, verwerven of anderszins ter beschikking hebben of stellen van een technisch hulpmiddel, toegangscode of wachtwoord om gekwalificeerde computerinbraak (art. 138ab lid 2 of 3) te plegen.

Art. 139e Sr
Het voorhanden hebben of bekendmaken van gegevens die door wederrechtelijk afluisteren, aftappen en/of opnemen zijn verkregen.

Art. 161sexies lid 1 Sr
Opzettelijk stoornis veroorzaken in de gang of werking van een geautomatiseerd werk met een publieke functie of een werk voor de telecommunicatie, waarbij een bepaald gevolg optreedt.

Art. 161sexies lid 2 Sr
Het vervaardigen, verkopen, verwerven of anderszins ter beschikking hebben of stellen van een technisch hulpmiddel, toegangscodes of wachtwoorden met het oogmerk computersabotage (art. 161sexies lid 1) te plegen (voorbereidingshandelingen of misbruik van hulpmiddelen).

Art. 161septies Sr
Door verwijtbare nalatigheid een stoornis veroorzaken in de gang of werking van een geautomatiseerd werk met een publieke functie of een werk voor de telecommunicatie, indien een bepaald gevolg optreedt.

Art. 273d lid 1 Sr
Opzettelijk en wederrechtelijk aftappen of opnemen, beschikking hebben over, of bekend maken van, de inhoud van communicatie door een medewerker van de aanbieder van een openbaar telecommunicatienetwerk of -dienst.

Art. 273d lid 2 Sr
Opzettelijk en wederrechtelijk aftappen of opnemen, beschikking hebben over of bekend maken van de inhoud van communicatie door een medewerker van een communicatienetwerk of -dienst (zoals een bedrijfsnetwerk).

Art. 326c
Het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen (telecomfraude).

Art. 350a lid 1 Sr
Het opzettelijk en wederrechtelijk onbruikbaar maken, veranderen of toevoegen van gegevens.

Art. 350a lid 2 Sr
Hetzelfde als lid 1, na door tussenkomst van een openbaar telecommunicatienetwerk te zijn binnengedrongen in een geautomatiseerd werk, waarbij ernstige schade optreedt.

Art. 350a lid 3 Sr
Opzettelijk en wederrechtelijk ter beschikking stellen of verspreiden van gegevens die schade aanrichten door zichzelf te vermenigvuldigen (zoals computervirussen, wormen en Trojaanse paarden).

Art. 350b lid 1 Sr
Het door verwijtbare nalatigheid wederrechtelijk onbruikbaar maken, veranderen of toevoegen van gegevens, als daardoor ernstige schade ontstaat.

Art. 350b lid 2 Sr
Het door verwijtbare nalatigheid verspreiden van gegevens die schade aanrichten door zichzelf te vermenigvuldigen.

Begrippenlijst

Aanbieder van een communicatiedienst
Een aanbieder van een communicatiedienst is de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren via een geautomatiseerd werk, of die gegevens verwerkt voor een zodanige dienst of gebruikers van die dienst.

Abonnee
Een abonnee is een natuurlijke persoon of rechtspersoon die partij is bij een overeenkomst met een aanbieder van openbare elektronische communicatiediensten voor de levering van dergelijke diensten (art. 1.1 sub p Tw).

Adware
Adware is de naam voor kleine programma's die, soms zonder dat deze worden opgemerkt, op een computer worden geïnstalleerd. Adware zit vaak bij gratis software. Adware wordt gebruikt voor pop-ups van advertenties maar wordt ook gebruikt om na te gaan waar de gebruiker zoal in is geïnteresseerd op het internet. Deze informatie wordt dan periodiek gestuurd naar een leverancier die deze informatie vervolgens weer gebruikt om gerichte reclame te sturen. Adware is een vorm van spyware.

Aftappen en opnemen
De termen aftappen en opnemen hebben in de strafwet een min of meer vastomlijnde betekenis en worden gebruikt voor het onderscheppen en vastleggen van stromende (streaming) gegevens (vgl. art. 125g Sv en 139a e.v. Sr). Opnemen betekent dat de gegevens worden vastgelegd om later te worden omgezet of anderszins te worden gebruikt. Gaat het om kopiëren van bestaande, opgeslagen gegevens, dan wordt de term overnemen gebruikt.

Authenticatie
Het proces waarbij een persoon, een computer of een applicatie nagaat of een gebruiker, een computer of een applicatie daadwerkelijk is wie hij/het beweert te zijn. Bij de authenticatie wordt gecontroleerd of een opgegeven bewijs van identiteit overeenkomt met echtheidskenmerken, bijvoorbeeld het een in het systeem geregistreerde bewijs. Authenticatie is de tweede stap in een toegangscontroleproces. De eerste stap is identificatie, de derde en laatste stap is autorisatie.

Autorisatie
Het proces waarin een subject (een persoon of een proces) rechten krijgt voor het benaderen van een object (een set gegevens, een computerbestand, een systeem). De autorisatie wordt toegekend door de object- of locatie-eigenaar.

Beschikbaarheid
Een kwaliteitskenmerk voor een object of dienst voor (informatie)beveiliging. Geeft aan in hoeverre een object, (ICT-)dienst, systeem of component zonder belemmering toegankelijk is voor geautoriseerde gebruikers. De beschikbaarheid wordt in de regel als een percentage gepresenteerd, waarbij een hogere waarde een positievere uitkomst is dan een lage waarde.

Beveiligen
Onttrekken aan geweld, bedreiging, gevaar of schade door het treffen van maatregelen.

Beveiligingsincident
Een (informatie)beveiligingsincident is een enkele of serie van ongewenste of onverwachte gebeurtenissen die een significante kans maken een ramp te veroorzaken, bedrijfsprocessen te compromitteren en een bedreiging te vormen voor de veiligheid.

Beveiligingsmaatregelen
Middelen, procedures, overeenkomsten of andere voorzieningen bedoeld om risico's te verkleinen of deze weg te nemen (mitigeren). De maatregelen kunnen worden gecategoriseerd als organisatorische, personele, fysieke of technische (ICT-)maatregelen. Maatregelen verschillen in karakter doordat ze preventief (voorkomen van de dreiging), detectief (ontdekken en herkennen van de dreiging) of correctief (optreden als de dreiging zich voordoet) bedoeld zijn.

Bevoegden
Degenen die een geautoriseerde en/of functionele toegang hebben tot (onderdelen van) het bedrijf, locatie, proces, middelen of informatie.

Bewerker
Degene die in het kader van de Wbp voor de verantwoordelijke persoonsgegevens verwerkt, zonder aan diens rechtstreeks gezag te zijn onderworpen.

Bot
Een bot is een geïnfecteerde computer die op afstand (met kwade bedoelingen) bestuurd wordt. Het woord 'bot' komt van robot. Een bot voert via een programma zelfstandig 'geautomatiseerd werk' uit. Een bot kan onschuldig zijn; zoekmachines gebruiken bots om websites in kaart te brengen. Maar bots worden ook ingezet om kwaadaardige handelingen uit te voeren op computers. Zo kan een bot volledige toegang krijgen tot informatie op een computer of deze als onderdeel van een botnet gebruiken bij criminele acties tegen anderen.

Botnets
Een (grootschalige en wereldwijde) verzameling van autonoom werkende softwarerobots op zogenoemde zombiecomputers die op afstand kunnen worden bediend. De besturing vindt plaats via bijvoorbeeld IRC (Internet Relay Chat), http of peer-to-peer-netwerken. Botnets worden meestal geassocieerd met een netwerk van gecompromitteerde computers die via gedistribueerde software kunnen worden misbruikt.

Buffer overflow
Een buffer overflow is een fout in een programma of besturingssysteem die door een kwaadwillende persoon kan worden misbruikt. Buffer overflows worden vaak gebruikt om toegang te krijgen tot een computer, zonder dat de eigenaar van de computer daar iets van merkt. Ook wordt een buffer overflow gebruikt om een programma op een computer of de computer zelf vast te laten lopen.

Chatroom
Een virtuele ruimte op het internet waar mensen met elkaar communiceren.

Checksum
Een checksum (ook wel hash genoemd) is een controlereeks die gebruikt word om te controleren of een bestand of bericht is gewijzigd. Checksums worden tegenwoordig veel gebruikt om documenten of berichten digitaal te ondertekenen. Ook kunnen checksums gebruikt worden voor de controle van de integriteit van bestanden op een computersysteem.

Client-side aanvallen
Een aanvalstactiek gericht op bezoekers van een website. Door het bezoeken van een gehackte of kwaadaardige website wordt de computer van de bezoeker besmet met malware, dat daarvoor gebruik van een kwetsbaarheid van bijvoorbeeld de browser of een mediaspeler.

Codec
In de context van deze handleiding wordt met een codec een softwarecomponent bedoeld waarmee bepaalde digitale mediatypen bekeken of beluisterd worden. Omdat deze typen vaak veranderen door betere compressietechnieken of verbetering van de kwaliteit, is het niet ongebruikelijk dat de gebruiker gevraagd wordt een nieuwe codec te installeren om een bepaald fragment te zien of te beluisteren. Criminelen maken hier handig gebruik van om mensen te verleiden malware te installeren.

Command & Control-server (C&C)
Centrale computer(s) die de bots in een botnet aanstuurt.

Computercriminaliteit
Het misbruik waarbij ICT specifiek als doel én als middel worden ingezet. Computercriminaliteit is hightech crime in enge zin. Het betreft misdrijven die niet zonder tussenkomst of gebruik van computers of netwerken gepleegd kunnen worden (computervredebreuk, hacking, verspreiding van computervirussen).

Controleerbaarheid
Een kwaliteitskenmerk voor een object of dienst in het kader van de (informatie)beveiliging. Mate waarin het mogelijk is kennis te verkrijgen over de structurering (documentatie) en de werking van een object. Ook omvat het kwaliteitsaspect de mate waarin het mogelijk is vast te stellen dat het proces, de procedures en/of de verwerking van informatie in overeenstemming met de kwaliteitseisen wordt uitgevoerd.

Cookie
Een cookie is een bestandje dat door een website op de harde schijf van een bezoeker wordt geplaatst. Dit bestandje kan op een later moment door dezelfde website ook weer uitgelezen worden. Cookies worden vaak gebruikt voor identificatie van bezoekers van websites. Ze bevatten informatie als datum en tijd van bezoek en namen van bezochte pagina's.

Cross site scripting
Een aanvalstactiek waarbij het adres van een hiervoor kwetsbare website wordt misbruikt om extra informatie te tonen of programma's uit te voeren. Er zijn diverse vormen van cross site scripting waarbij complexe aanvallen mogelijk zijn.

Datalek (of data breach)
Het onopzettelijk naar buiten komen van vertrouwelijke gegevens.

Defacement
Het onbevoegd en vaak met kwaadaardige intentie vervangen of beschadigen van de inhoud van een bestaande webpagina. Vaak gebeurt dit door aanvallers die zichzelf op onrechtmatige wijze toegang hebben weten te verschaffen tot een webserver.

(Distributed) Denial of Service (DoS)
Een actie waarbij wordt geprobeerd een computer, een systeem of telecommunicatienetwerk zo te belasten of te manipuleren, dat deze wordt uitgeschakeld en niet meer beschikbaar is voor (bevoegde) gebruikers. DoS houdt in dat een computer continu 'aangevallen' wordt door bijvoorbeeld e-mail of ander netwerkverkeer.
Bij een Distributed Denial of Service-aanval (DDoS) wordt door een groot aantal computers tegelijk een gecoördineerde aanval uitgevoerd.

Digitaal Certificaat
Een set elektronische gegevens voor het identificeren van een persoon of ICT-systeem en/of een elektronische bevestiging die gegevens voor het verifiëren van een elektronische handtekening met een bepaalde persoon verbindt en de identiteit van die persoon bevestigt.

Domain Name System (DNS)
DNS is een techniek om de onpraktische IP-adressen te koppelen aan leesbare en begrijpelijke domeinnamen. Een DNS-server vertaalt niet, omdat er geen enkele logica zit in de domeinnamen en IP-adressen. DNS wordt gebruikt op het internet maar ook in bedrijfsnetwerken.

Dreiging (threat)
Een potentiële oorzaak voor het optreden van een ongewenst incident die kan leiden tot schade aan een object, systeem of de organisatie. Dreigingen kunnen worden gekwalificeerd als *zeer waarschijnlijk* (ZW), *waarschijnlijk* (W), *mogelijk* (Mo), *onwaarschijnlijk* (O) of *zeer onwaarschijnlijk* (Zo), afhankelijk van de kans van optreden.

Drive by downloads
Het ophalen van malware zonder dat de gebruiker het weet of daar zijn toestemming voor heeft gegeven, bijvoorbeeld door te klikken op een valse foutmelding of via een kwetsbaarheid in de browser, e-mail-client of besturingssysteem (zie ook > client side aanvallen).

Dropzone
Computersysteem waar gestolen gegevens (tijdelijk) worden opgeslagen.

Elektronische handtekening
Een handtekening bestaande uit elektronische gegevens die zijn vastgehecht aan, of logisch geassocieerd zijn met, andere elektronische gegevens en die wordt gebruikt als authenticatiemiddel.

Exploit
Een kwaadaardig programma of computercode waarmee misbruik kan worden gemaakt van een kwetsbaarheid in programma's of een besturingssysteem om zo niet-normaal gedrag te creëren op een computersysteem. Exploits voor bekende kwetsbaarheden zijn soms makkelijk te vinden op het internet.

Fast flux
Als de netwerk- of IP-adressen van een domeinnaam van bijvoorbeeld een phishingsite of Command & Control-botnet-server snel wijzigen om de dienst te beschermen tegen uitschakelen, wordt gesproken van de fast-flux-DNS-techniek.

Firmware
Firmware is de benaming voor software die standaard is geïnstalleerd op en meegeleverd wordt met bepaalde apparaten. De firmware is nodig om het apparaat te laten functioneren.

Fraude
Fraude is een opzettelijke handeling waarbij door het geven van een onjuiste voorstelling van zaken een gepretendeerde rechtvaardiging voor de handeling ontstaat, waarmee onrechtmatig voordeel wordt verkregen.

Geautomatiseerd werk
Geautomatiseerd werk is een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen (art. 80sexies, Sr.). Hieronder vallen computer- en netwerkapparatuur of -systemen, elektronische gegevensdragers of telecommunicatienetwerken, telefoon en fax.[67] Onder geautomatiseerde werken vallen dus 'de middelen van informatie- en communicatietechniek'.[68]

Gebeurtenis (event)
Een (informatie)beveiligingsgebeurtenis is een geïdentificeerd optreden van een object, systeem, service of (computer-) netwerk dat kan duiden op een mogelijke afwijking of overtreding van het beveiligingsbeleid, het falen van beveiligingsmaatregelen of een voorgaande relevante onbekende situatie.

Gegevens
Iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken (art. 80quinquies, Sr.). Hieronder vallen dus alle op een elektronische gegevensdrager, computer of ander geautomatiseerd werk verwerkte of opgeslagen informatie. Het begrip 'gegevens' omvat niet alleen gegevens die zijn opgeslagen in geautomatiseerde werken, maar ook de programmagegevens voor besturing van de computer.[69]

67. Cleiren & Nijboer 2002, Tekst & Commentaar Strafrecht , art. 80sexies Sr., aant. 2.
68. H. Franken, H.W.K. Kaspersen en A.H. de Wild, Recht en computer 1997, Kluwer Deventer.
69. Cleiren & Nijboer 2002, Tekst & Commentaar Strafrecht, art. 80quinquies Sr., aant. 2.

Gegevensoverdracht
In wetsartikelen wordt naast 'overdracht van gegevens' soms toegevoegd 'of andere gegevensoverdracht door een geautomatiseerd werk'.
'Overdracht van gegevens' in samenhang met het begrip 'telecommunicatie' duidt op overdracht van gegevens op afstand, tussen personen onderling, tussen personen en computers of tussen computers onderling.
De toevoeging 'of andere gegevensoverdracht door een geautomatiseerd werk' geeft aan dat ook de gegevensoverdracht 'op korte afstand' (bijvoorbeeld tussen computer en beeldscherm) onder gegevensoverdracht valt.[70]

Gelaagde maatregelen (defence in depth)
Het geheel aan op elkaar afgestemde beveiligingsmaatregelen waarbij een evenwichtige balans wordt gemaakt tussen waar deze maatregelen worden benut (organisatorisch, personeel, fysiek of (ICT-)technisch) en waar deze maatregelen preventief, detectief en correctief optreden, zodat voldoende weerstand en veerkracht bestaat tegen dreigingen.

Gevolg (impact)
Beoordeling van de omvang van de schade aan de bedrijfsvoering of de samenleving die ontstaat in relatie tot een object. Het gevolg kan kwalitatief (zoals verwachte financiële schade) of kwantitatief (hoog, middel, laag) worden uitgedrukt.
De Nationale Risicobeoordeling gebruikt de indeling *catastrofaal*, *zeer ernstig*, *ernstig*, *aanzienlijk* en *beperkt* gevolg.

Hacktivisme
Het inzetten van computers en telecommunicatienetwerken om een ideologisch of politiek doel te bereiken. Aanvallen richten zich bijvoorbeeld op het beschadigen of onbereikbaar maken van websites en internetvoorzieningen van tegenstanders.

Hash-waarde
Een hash-waarde is het resultaat van een cryptografische hash-functie. Deze zet de waarde van een invoer om in een (meestal) kleiner bereik van karaktertekens. De uitkomst is een onbegrijpelijke reeks van tekens met zeer weinig kans dat twee verschillende invoerwaarden dezelfde uitvoer geven. Bovendien is het zeer moeilijk om de oorspronkelijke invoerwaarde af te leiden. Een typische toepassing is het versleutelen van wachtwoorden of het berekenen van controlewaarden (checksums).

Hightech crime
Een paraplubegrip voor computercriminaliteit, cybercrime, cyberstalking, cyberfraude, cyberhate en cyberespionage of het anderszins misbruiken van ICT- of technisch geavanceerde middelen of het inzetten hiervan bij (zware en georganiseerde) criminaliteit.

Hoax
Een hoax is een verzonnen probleem waarover - meestal per e-mail - berichten worden verspreid. Denk bijvoorbeeld aan meldingen over niet-bestaande virussen of niet op waarheid berustende mededelingen. Bijna altijd wordt gevraagd om het e-mailbericht naar zoveel mogelijk mensen door te sturen (vergelijkbaar met een kettingbrief).

Hotfix
Fouten in programma's worden meestal in een volgende versie verholpen. Soms zijn de gevolgen van een fout zo ernstig, dat niet gewacht kan worden op het uitbrengen van een nieuwe versie. Er wordt dan een vervangend programmaonderdeel uitgebracht dat alleen de fout herstelt. Dit vervangende programmaonderdeel noemt men een hotfix.

Hotspot
Een publieke locatie (hotel, café, tankstation) waar, al dan niet tegen betaling, draadloos toegang tot het internet verkregen kan worden.

Identificatie
Het kenbaar maken van de identiteit van een subject (een persoon of een (computer)proces). De identiteit wordt gebruikt om de toegang van het subject tot een object te beheersen. Identificatie kan op verschillende manieren plaatsvinden, bijvoorbeeld via een inlogscherm, biometrisch kenmerk of een smartcard.

Informatiebeveiliging
Het proces van vaststellen van de vereiste kwaliteit van informatie(-systemen) in termen van vertrouwelijkheid, beschikbaarheid, integriteit, onweerlegbaarheid en controleerbaarheid, maar ook het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende (fysieke, organisatorische en logische) maatregelen.

Informatiesysteem
Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur, samen met de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Integrale beveiliging
Het gehele proces van vaststellen, treffen, onderhouden en controleren van een samenhangend pakket van maatregelen voor fysieke en informatiebeveiliging waarbij over alle relevante aandachtsgebieden (zoals economische, ecologische, maatschappelijke invloeden) de risico's in oogenschouw worden genomen en meegewogen.

70. TK, 1989-1990, 21551, nr. 3, p. 7.

Integriteit
Een kwaliteitskenmerk voor gegevens, een object of dienst in het kader van de (informatie)beveiliging. Het is een synoniem voor betrouwbaarheid. Een betrouwbaar gegeven is juist (rechtmatigheid), volledig (niet te veel en niet te weinig), tijdig (op tijd) en geautoriseerd (gemuteerd door een persoon die gerechtigd is de mutatie aan te brengen).

Internet Service Provider (ISP)
Leverancier van internetdiensten, vaak simpelweg aangeduid als 'provider'. De geleverde diensten kunnen zowel betrekking hebben op de internetverbinding zelf als op de diensten die men op het internet kan gebruiken.

Internet Relay Chat
IRC is een elektronische babbelbox van het internet. Door in te loggen op een IRC-server kan met meerdere mensen tegelijk, of met één netgebruiker apart, worden gecommuniceerd door getypte boodschappen uit te wisselen. IRC bestaat uit zogenoemde kanalen die ieder hun eigen onderwerp hebben, zodat gerichte discussies kunnen plaatsvinden.

IP-adres
Een adres waarmee een apparaat aangesloten op een computernetwerk eenduidig (logisch) kan worden geadresseerd binnen het TCP/IP-model. Het Internet Protocol-adres verbindt elke computer met een telecommunicatienetwerk of het internet via een uniek IP-adres, dat gebruikt wordt voor het bepalen van bestemming en herkomst van netwerkverkeer.

Item (asset)
Alles van waarde voor de organisatie. Items kunnen worden onderverdeeld naar data (gegevens), informatie en computersystemen, applicaties/software, fysieke componenten (apparatuur, gebouwen, andere faciliteiten) of personen.

Kwaliteitseisen (Betrouwbaarheidseisen)
De eisen voor beschikbaarheid, integriteit, vertrouwelijkheid, onweerlegbaarheid en controleerbaarheid die, vanuit belangen en afhankelijkheden, gesteld worden aan een (bedrijfs)proces of object. De kwaliteitseisen zijn meestal de randvoorwaarden voor de keuze van te treffen beveiligingsmaatregelen.

Kwetsbaarheid (vulnerability)
Een kwetsbaarheid is een zwakke plek in een proces, object, software of hardware dat kan worden misbruikt door één of meerdere dreigingen. Kwetsbaarheden kunnen worden gekwalificeerd als *enorm* (E), *groot* (G), *behoorlijk* (B), *minimum* (M) of *verwaarloosbaar* (V), afhankelijk van de vatbaarheid voor de betreffende zwakte en de gevolgen daarvan.

MAC-adres
Een MAC-adres staat voor Media Access Control en is een uniek identificatienummer dat aan een apparaat in een ethernet-netwerk is toegekend. Een MAC-adres wordt ook wel hardware-adres genoemd. Het zorgt ervoor dat apparaten in een ethernet-netwerk met elkaar kunnen communiceren. Vrijwel ieder netwerkapparaat heeft een vast, door de fabrikant bepaald MAC-adres.

Malware
Samentrekking van malicious (kwaadaardig) en software. Verzamelnaam voor software met kwaadaardige bedoelingen zoals virussen, wormen, Trojaanse paarden, keyloggers, spyware, adware en bots.

Man-in-the-middle-aanval
Een aanval waarbij de aanvaller zich tussen een klant (client) en een dienst (service) bevindt. Hierbij doet hij zich richting de klant voor als de dienst en andersom. Als tussenpersoon kan de aanvaller nu uitgewisselde gegevens afluisteren en/of manipuleren.

Moedwillig menselijk handelen
Moedwillig menselijk handelen omvat onbevoegde beïnvloeding, door kwaadwillenden veroorzaakte verstoringen en manipulatie gericht op het belemmeren, aanpassen of verstoren van een (bedrijfs)proces met gevolgen voor de directe omgeving, het (bedrijfs)proces zelf of de geleverde diensten.

Notice and Take Down (NTD)
Notice and Take Down is een gefaseerde procedure die gebruikt wordt om servers met illegale inhoud van het internet te verwijderen. Voorbeelden van NTD's zijn die voor kinderporno- en phishing-sites.

Openbaar telecommunicatienetwerk
De betekenis van het begrip 'openbaar telecommunicatienetwerk' komt uit artikel 1.1 sub g en sub h van de Telecommunicatiewet: '*een telecommunicatienetwerk dat onder meer voor de verrichting van openbare telecommunicatiediensten wordt gebruikt of een telecommunicatienetwerk waarmee aan het publiek de mogelijkheid tot overdracht van signalen tussen netwerkaansluitpunten ter beschikking gesteld wordt*'.

Obfuscation (versluiering)
Een techniek om de interne werking van malware te versluieren voor onderzoekers of onzichtbaar te maken voor virusscanners.

Object
Een fysiek voorwerp, een gegevens-set, een computerbestand, een systeem of een ander (virtueel) afgebakende geheel (entiteit) dat als onderwerp fungeert waarop het handelen van een persoon of subject is gericht.

Onweerlegbaarheid
Een kwaliteitskenmerk voor een object of dienst in het kader van de (informatie)beveiliging. Mate waarin onbetwistbaar bewezen kan worden dat een partij een valse ontkenning geeft van deelname in het geheel of deel van een communicatiestroom.

Overnemen
Het kopiëren van bestaande opgeslagen gegevens van een geautomatiseerd werk.

Patch
Een patch (letterlijk ‘pleister’) kan bestaan uit reparatiesoftware of kan wijzigingen bevatten die direct in een programma worden doorgevoerd om dat programma te repareren of te verbeteren.

Peer-to-peer-netwerk (P2P)
Een computernetwerk waarin de aangesloten computers gelijkwaardig zijn. Een peer-to-peer-netwerk kent geen vaste werkstations en servers, maar heeft een aantal gelijkwaardige aansluitingen die tegelijkertijd functioneren als server en als werkstation voor de andere aansluitingen in het netwerk. Bestanden die via P2P-netwerken worden uitgewisseld, worden in delen binnengehaald en tegelijkertijd weer gedeeld.

Phishing
Phishing is een verzamelnaam voor digitale activiteiten die ten doel hebben persoonlijke informatie aan mensen te ontfutselen. Een vorm van phishing is mensen lokken naar een valse website, die een kopie is van de echte website en ze daar - nietsvermoedend - zich laten aanmelden. De fraudeur krijgt hierdoor de beschikking over de inloggegevens van het slachtoffer met alle gevolgen van dien. De slachtoffers worden vaak via e-mail naar de valse website gelokt. De persoonlijke informatie kan direct worden misbruikt voor het doen van bijvoorbeeld grote uitgaven (in het geval van creditcardnummers) of voor wat in het Engels ‘identity theft’ wordt genoemd, het stelen van een identiteit. Dan zijn gegevens als burgerservicenummers (BSN), adressen en geboortedata nodig.

Polymorfe malware
Malware die verschillende vormen aanneemt, afhankelijk van de gebruikte software (webbrowser of besturingssysteem) van het slachtoffer.

Poort (port)
Een poort is een gedefinieerd communicatiekanaal op een computer. Op het moment dat communicatie tussen twee computers plaatsvindt, is op beide computers een programma actief waarvoor een bepaalde poort wordt gebruikt. Aan beide zijden van het communicatiekanaal ‘luistert’ de computer op deze poorten of er iets is voor het programma. Standaard luistert een computer naar alle poorten. Met een firewall kunnen poorten van een computer worden gesloten, zodat misbruik wordt voorkomen.

Port scan
Een scan van de poorten van een computer om snel een indruk te krijgen van welke diensten een computer allemaal gebruik maakt. Op basis daarvan kan een aanvaller bepalen welk soort kwetsbaarheden hij/zij kan gebruiken voor een aanval.

Proces
Met een proces wordt een primair (bedrijfs)proces bedoeld, de activiteiten die een organisatie uitvoert om het hoofddoel te bereiken. Voor het overzicht wordt, waar nodig, een proces opgedeeld in subprocessen. Met proces wordt hier niet het (geautomatiseerde) proces van informatieverwerking binnen een informatiesysteem bedoeld.

Proxy
Een proxyserver is een server die zich bevindt tussen de computer van de gebruiker en de computer die de gebruiker wil benaderen. De proxy is een ‘tussenpersoon’ die de opdrachten namens de gebruiker uitvoert. Proxyservers worden veel gebruikt om computers van een (lokaal) bedrijfsnetwerk gecontroleerd toegang te geven tot het internet. Een open proxy staat verbindingen van willekeurige gebruikers (IP-adressen) toe.

Rainbow table
Een tabel met mogelijke wachtwoorden en de hash-waarden van deze wachtwoorden. Ze worden gebruikt om wachtwoorden te testen op veiligheid of om deze te kraken. De techniek is vele malen sneller dan een brute force-techniek, waarbij de hash-waarden van de wachtwoorden nog moeten worden berekend.

Randapparatuur

Alle uitrusting die op computersystemen (geautomatiseerde werken) kan worden aangesloten. Het gaat om mobiele apparatuur of apparatuur die de functionaliteit uitbreiden, zoals PDA's, mobiele telefoontoestellen, printers, modems, netwerkapparatuur, beeldschermen, invoerapparaten, multimedia-apparatuur, externe harde schijven of usb-sticks. Artikel 1.1 sub jj van de Telecommunicatiewet omschrijft randapparatuur als volgt:

1. Uitrusting die bestemd is om op een openbaar telecommunicatienetwerk te worden aangesloten, zodanig dat zij: rechtstreeks op netwerkaansluitpunten kan worden aangesloten, of kan dienen voor interactie met een openbaar telecommunicatienetwerk via directe of indirecte aansluiting op netwerkaansluitpunten ten behoeve van overbrenging, verwerking of ontvangst van informatie.
2. Radiozendapparaten die geschikt zijn om op een openbaar telecommunicatienetwerk te worden aangesloten.
3. Uitrusting voor satellietgrondstations tenzij bij of krachtens hoofdstuk 10 anders is bepaald, doch met uitsluiting van speciaal geconstrueerde uitrusting die bedoeld is voor gebruik als onderdeel van een openbaar telecommunicatienetwerk.

Ransomware

Een vorm van malware waarbij computerbestanden worden versleuteld en pas na betaling weer vrijgegeven. Slachtoffers worden naar websites gelokt waarna er door een lek in de browser een programma geïnstalleerd wordt buiten medeweten van de gebruiker. Deze software versleutelt vervolgens bekende bestandstypes. Het slachtoffer krijgt een bericht met e-mailadres om de sleutel aan te vragen tegen betaling van een niet onaanzienlijk geldbedrag.

Reverse proxy

Een server die als een proxyserver van buiten naar binnen functioneert. Deze proxyserver wordt bijvoorbeeld gebruikt om de belasting vanuit het internet te controleren en vervolgens gelijkmatig te verdelen over verschillende webservers.

Risico

Een risico is de functie van de kans op en het gevolg van een ongewenste gebeurtenis. Dit maakt het mogelijk een waarde toe te kennen aan het gevolg van een ongewenste gebeurtenis. Die waarde is afhankelijk van de ernst van het gevolg. In deze definitie wordt ruimte gelaten voor het maken van bepaalde risicoafwegingen en rekening gehouden met niet te voorziene gebeurtenissen. Het risico kan worden geclassificeerd als *kritiek* (K), *substantieel* (S), *beperkt* (B) of *minimaal* (M) als resultante van de *kans (dreiging) x effect (kwetsbaarheid en impact)*.

Risicoanalyse

Een weging van de kansen en gevolgen van een ongewenste gebeurtenis. Het leidt tot inzicht in de ernst en waarschijnlijkheid van die gebeurtenis en in de weerbaarheid van een organisatie tegen bedreigingen van vastgestelde belangen en uitval en verstoringen van vitale processen. Die weerbaarheid wordt afgemeten aan de maatregelen die zijn genomen om de kans op verstoring te verminderen en de gevolgen beheersbaar te maken.

Scam

De term *scam* wordt vrij losjes gebruikt voor allerlei soorten frauduleuze handelingen die erop gericht zijn om geld van mensen afhandig te maken. Een bekende vorm zijn de 419-scams.

Security Information and Event Management (SIEM)

SIEM-systemen bieden real-time-analyse van security-waarschuwingen gegenereerd door bijvoorbeeld netwerksystemen, hardware of applicaties. SIEM-oplossingen verzamelen en correleren meldingen en worden gebruikt om beveiligingsgegevens te loggen en rapporten te genereren voor onder meer het afleggen van verantwoording.

Single serve

Dit houdt in dat een kwaadaardige server controleert of een client computer eerder contact heeft gelegd. Is dit niet het geval dan wordt malware aangeboden aan de client. Als de client wel eerder contact heeft gelegd dan wordt er geen malware meer aangeboden. Opsporing wordt zo gehinderd omdat het moeilijker is na te gaan wat de bron van besmetting is geweest.

Skimmen

Het onrechtmatig kopiëren van de gegevens van een elektronische betaalkaart, bijvoorbeeld een pinpas of creditcard. Skimmen gaat vaak gepaard met het bemachtigen van pincodes om betalingen te verrichten of geld op te nemen van de rekening van het slachtoffer.

Social Engineering

Het manipuleren van mensen om ze zover te krijgen dat ze informatie geven of een actie uitvoeren, zoals het klikken op een link of het installeren van malware.

Sociale netwerken

Online Sociale Netwerksites (OSN) zijn hulpmiddelen waarmee mensen hun (privé en/of zakelijke) sociale netwerk op internet kunnen onderhouden. Voorbeelden zijn Hyves, Facebook, Twitter en LinkedIn.

Spam
Spam is grootschalige ongewenste berichtgeving via e-mail, mobiele telefonie (sms of mms) of via een ander elektronisch kanaal zoals sociale netwerken, fax of bellen via een automatisch oproepsysteem, of via de telefoon. De inhoud van het bericht is verschillend en loopt uiteen van reclame tot het verzoek voor een financiële bijdrage. Spam betreft het grote volume van e-mailberichten dat verzonden wordt, niet de inhoud van het bericht.

Spear phishing
Vorm van phishing die specifiek gericht is op een bepaalde gebruiker of groepen van gebruikers, bijvoorbeeld medewerkers van een bepaalde organisatie.

Spyware
Een programma dat informatie over een gebruiker verzamelt en deze zonder dat de gebruiker daarvan op de hoogte is doorstuurt naar een derde partij.

Subject
Een persoon of (computer)proces dat handelingen kan verrichten en een relatie kan hebben met andere subjecten of objecten.

Technisch hulpmiddel
De wet geeft geen toegespitste definitie van wat onder een technisch hulpmiddel moet worden verstaan, bijvoorbeeld als het gaat om aftappen en/of opnemen van gegevens. Volgens de literatuur valt onder het begrip technisch hulpmiddel elk apparaat, waarmee het technisch mogelijk is door anderen gevoerde telecommunicatie op te nemen.[71]

Telecommunicatie
De betekenis van het begrip ‘telecommunicatie’ komt uit artikel 1.1 sub e van de Telecommunicatiewet: *‘iedere overdracht, uitzending of ontvangst van signalen van welke aard ook door middel van kabels, radiogolven, optische middelen of andere elektromagnetische middelen’*.

Telecommunicatiedienst
De betekenis van het begrip ‘telecommunicatiedienst’ komt uit artikel 1.1 sub f van de Telecommunicatiewet: *‘dienst die geheel of gedeeltelijk bestaat in de overdracht of routering van signalen over een telecommunicatienetwerk’*.
Het begrip ‘openbare telecommunicatiedienst’ staat in artikel 1.1 sub g van de Telecommunicatiewet: *‘telecommunicatiedienst die beschikbaar is voor het publiek’*.

TEMPEST
Telecommunications Electronics Materials Protected From Emanating Spurious Transmissions wordt gebruikt als verzamelterm voor technische beveiligingsmaatregelen, standaarden en instrumenten, die misbruik van elektronische straling zoals technische surveillance en afluisteren (spionage) van (niet-aangepaste) elektronische apparaten en systemen, voorkomt dan wel minimaliseert. Tegenwoordig gebruikt men vaker Emission Security (EMSEC) om naast TEMPEST ook andere disciplines van elektronische beveiliging aan te duiden.

Trojaans paard (Trojan horse)
Een trojan of trojan horse (Trojaans paard) is de naam voor software die geheime, kwaadaardige functies bevat. Het programma is vermomd als een legaal, onschuldig programma, maar voert daarnaast ongewenste functies uit. Die functies zijn bedoeld om bijvoorbeeld de maker of verspreider van het programma ongemerkt toegang te geven of om schade toe te brengen.

Two-factor authentication
Een manier van aanmelden (inloggen) op een computer, waarbij gebruik gemaakt wordt van twee van de drie volgende verschijningsvormen: iets dat de gebruiker weet (een wachtwoord of pincode), iets wat hij of zij heeft (een codegenerator of lijst met eenmalige codes) of iets wat hij of zij is (biometrische kenmerken, zoals een scan van de iris of een vingerafdruk).

Veerkracht (resilience)
De mate waarin een object, proces of systeem (de gevolgen van) dreigingen (dynamisch) kan opvangen zonder dat hierbij direct (significante) schade ontstaat waardoor de continuering of integriteit en betrouwbaarheid van de kritische functies in gevaar worden gebracht.

Verantwoordelijke
De (rechts)persoon of organisatie die in het kader van de Wbp formeel-juridisch gezien degene is die het doel en de middelen van de verwerking van persoonsgegevens vaststelt, dan wel aan wie de verwerking naar in het maatschappelijk verkeer geldende maatstaven wordt toegerekend.

Vertrouwelijkheid (exclusiviteit)
Een kwaliteitskenmerk van gegevens in het kader van de informatiebeveiliging. Met vertrouwelijkheid (exclusiviteit) wordt bedoeld dat een gegeven alleen te benaderen is door iemand die gerechtigd is het gegeven te benaderen. Wie gerechtigd is een gegeven te benaderen wordt vastgesteld door de eigenaar van het gegeven.

71. Noyon, Langemeijer en Remmelink, supplement 107, aant. 1a bij art. 139c.

Virus
Een klein programma bedoeld om dingen te doen met een systeem waar de eigenaar niet om gevraagd heeft of die men niet wil. Soms blijft het bij 'onschuldige' pop-up-venstertjes, maar vaak zijn virussen erg gevaarlijk. Virussen zijn er in vele soorten en maten.

Vitale Infrastructuur
Producten, diensten en de onderliggende processen die, als zij uitvallen of worden verstoord, maatschappelijke ontwrichting kunnen veroorzaken. Dat kan zijn omdat er sprake is van veel slachtoffers en/of grote economische schade, dan wel omdat de uitval van lange duur is en er geen reële alternatieven voorhanden zijn, terwijl de betreffende producten en diensten maatschappelijk niet kunnen worden gemist. De vitale infrastructuur is kritisch om de territoriale, fysieke, economische en ecologische veiligheid en de sociale en politieke stabiliteit van Nederland te garanderen.

Vitale Sector
Een publiek en/of private groep organisaties en bedrijven die producten, goederen of diensten leveren en/of beheren, die als kritisch zijn benoemd voor de handhaving van de vitale belangen of vitale infrastructuur van Nederland.
De vitale sectoren zijn: Energie, Drinkwatervoorziening, Telecommunicatie / ICT, Voedsel, Gezondheid, Keren en beheren oppervlaktewater, Financieel, Transport, Chemische en nucleaire industrie, Openbare Orde en Veiligheid, Rechtsorde en Openbaar Bestuur.

Warez
Warez is de verzamelnaam voor gekraakte software die via websites op het internet aangeboden wordt. Soms wordt er een serienummer meegegeven. Het gaat om software waarvan het copyright geschonden wordt, waardoor het illegaal is.

Weerstand (resistance)
De mate waarmee een object, proces of systeem bestand is tegen dreigingen via getroffen preventieve maatregelen.

WiFi
Wireless Fidelity, een populaire vorm van een draadloos netwerk. WiFi kent een groot bereik, namelijk tussen de 30 (binnen) en de 300 (buiten) meter. Een andere vorm van draadloos netwerk is Bluetooth.

Worm
Een programma speciaal gemaakt om zichzelf te verspreiden naar zoveel mogelijk computers. Een worm verschilt van een virus. Een virus heeft een bestand nodig om zichzelf te verspreiden, een worm niet. Een worm heeft niet altijd schadelijke gevolgen voor een computer, maar kan de verbinding wel langzaam maken.

Zero-day
Een zero-day-aanval misbruikt een nog onbekende of niet gemelde zwakke plek in een computerprogramma. Ze zijn nog niet bekend bij de softwareontwikkelaar of er is nog geen oplossing (patch) beschikbaar om het gat te dichten. Zero-day exploits worden gebruikt of gedeeld door hackers voordat de softwareontwikkelaar weet heeft van de kwetsbaarheid.

Zombiecomputer
Een computer geïnfecteerd met een bot. De geïnfecteerde computer vormt onderdeel van een botnet en staat als een 'zombie' ter beschikking van de internetcrimineel.

BIJLAGE E

Overzicht van organisaties

(ISC)2
(ISC)2 is een wereldwijde vereniging voor informatiebeveiligingsprofessionals met de nadruk op kennisuitwisseling, training en certificering voor onder andere Certified Information Systems Security Professional (CISSP).
> https://www.isc2.org

Agentschap Telecom (AT)
Aandachtsgebieden van AT zijn continuïteit, integriteit en beschikbaarheid van elektronische netwerken en diensten. Hieronder vallen crisismanagement in buitengewone omstandigheden, frequentieverwerving en -uitgifte, monitoring en toezicht om de continuïteit te waarborgen van draadloze communicatiediensten, zoals nooddiensten, C2000, alarmeringssystemen en radionavigatie. Daarnaast houdt het AT toezicht op het aanwezig zijn van tapvoorzieningen bij service providers. Het AT is onderdeel van het ministerie van Economische Zaken, Landbouw & Innovatie.
> http://www.agentschaptelecom.nl

Algemene Inlichtingen- en Veiligheidsdienst (AIVD)
De AIVD houdt zich bezig met dreigingen die een gevaar vormen voor de democratische rechtsorde, de veiligheid of andere gewichtige belangen van de staat. Daarnaast bevordert de AIVD de beveiliging van gegevens waarvan geheimhouding door de nationale veiligheid wordt geboden, en van die onderdelen van de overheid en het bedrijfsleven die van vitaal belang zijn voor de instandhouding van het maatschappelijke leven. De minister van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor de AIVD.
> https://www.aivd.nl

BREIN
BREIN onderneemt actie tegen piraterij in Nederland. Gezien het grensoverschrijdende karakter van piraterij werkt BREIN daarvoor nauw samen met internationale organisaties zoals MPA en IFPI en hun nationale anti-piraterij-units.
> http://www.anti-piracy.nl

CIO platform NL
Het CIO Platform Nederland is een vereniging van CIO's en IT-directeuren van private en publieke organisaties in Nederland.
> http://www.cio-platform.nl

College Bescherming Persoonsgegevens
Het CBP is de formele toezichthouder op zorgvuldig en (be)veilig(d) gebruik van persoonsgegevens. Het CBP richt zich onder meer op gebruik van de informatie in telecommunicatiesystemen en op publicaties op websites, met als invalshoek de privacy-problemen die burgers in de alledaagse praktijk op het internet ondervinden.
> http://www.cbpweb.nl/Pages/home.aspx

CPNI.NL
CPNI.NL is het Nederlandse platform voor cybersecurity. CPNI.NL betekent Centre for Protection of the National Infrastructure. Het is de opvolger van het NICC dat vanaf 1 januari 2011 is ondergebracht bij TNO. Voor een effectieve werkwijze brengt het CPNI.NL partijen bij elkaar in een nationale Infrastructuur voor de bestrijding van Cybercrime.
> http://www.cpni.nl

ECP-EPN
ECP-EPN is het platform in Nederland waar publiek-privaat wordt samen¬gewerkt aan belangrijke randvoorwaarden en doorbraken rond de digitale economie en samenleving. ECP-EPN is in 1998 opgericht door het ministerie van Economische Zaken en VNO-NCW.
> http://www.ecp.nl

European Network and Information Security Agency (ENISA)
Het Europees Agentschap voor netwerk- en informatiebeveiliging is een agentschap van de Europese Unie, opgericht in 2004 en gevestigd in Iraklion op Kreta. ENISA heeft tot taak informatienetwerken en daarmee verstuurde gegevens te helpen beveiligen voor de bescherming van burgers, consumenten, bedrijven en overheidsorganisaties in de Europese Unie. Het agentschap verzamelt onder meer gegevens, analyseert risico's en geeft voorlichting.
> http://www.enisa.europa.eu

European Programme for Critical Infrastructure Protection (EPCIP)
Het European Programme for Critical Infrastructure Protection is een initiatief van de Europese Commissie om de bescherming van de vitale infrastructuur in Europa te bevorderen. Op de site van EPCIP vindt u informatie over de voortgang van dit programma.
> http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm

FIOD
De FIOD is de opsporingsdienst van de Belastingdienst onder het gezag van het Functioneel Parket van het Openbaar Ministerie. De FIOD richt zich op fiscale fraude, financiële/financieel-economische fraude, fraude met vastgoed, witwassen en fraude met specifieke goederen.
> http://www.rijksoverheid.nl/onderwerpen/belasting-betalen/fraude-opsporen

FIRST
FIRST is een Forum voor Incident Response en Security Teams. Het is een platform waarbij aangesloten leden in vertrouwen kennis en ervaring kunnen uitwisselen. Daarnaast kan via het FIRST-netwerk snel en efficiënt internationaal worden gereageerd bij incidenten.
> http://www.first.org

GOVCERT.NL
GOVCERT.NL was tot 2012 het Computer Emergency Response Team van en voor de Nederlandse overheid. Zij ondersteunde overheidsorganisaties in het voorkomen en afhandelen van ICT-gerelateerde veiligheidsincidenten, 24 uur per dag, 7 dagen per week. Advies en preventie, waarschuwing, incidentafhandeling en kennisdeling waren hierbij sleutelwoorden. Vanaf 1 januari 2012 is GOVCERT.NL opgegaan in het Nationaal Cyber Security Centrum van Nederland. Het CERT-team van GOVCERT.NL gaat voor internationale partners verder onder de naam: NCSC-NL.
> http://www.govcert.nl
> http://www.ncsc.nl

IB-beraad
Het Informatiebeveiligingsberaad van de Rijksoverheid. In het IB-beraad zijn alle departementen vertegenwoordigd. In dit beraad vindt op ambtelijk niveau de afstemming plaats over de gemeenschappelijke aspecten van informatiebeveiliging.

Information Security Solutions Europe (ISSE)
ISSE is een Europese, onafhankelijke, multidisciplinaire security-conferentie en -beurs.

Internet Corporation for Assigned Names and Numbers (ICANN)
ICANN is een non-profitorganisatie die een aantal Internet-gerelateerde taken uitvoert, zoals het maken van top level domains, toewijzen van domeinnamen en de distributie van IP-nummers.
> http://www.icann.org

ISACA
ISACA is een wereldwijde vereniging voor informatiesysteem-auditors en informatiebeveiligingsmanagers met de nadruk op kennisuitwisseling, training en certificering voor onder andere CISA en CISM.
> http://www.isaca.nl

IWWN
Het International Watch and Warning Network, waarin het Nationaal Cyber Security Centrum (NCSC) participeert namens Nederland.

Joint Investigation Team (JIT)
Internationale gezamenlijke onderzoeksteams van politie en opsporingsinstanties. JIT's worden vanuit Nederland meestal vertegenwoordigd door het KLPD.
> http://www.eurojust.europa.eu/jit.htm

Jure
Jure.nl maakt rechterlijke uitspraken online toegankelijk door de publicatie ervan op haar website. Daarbij gaat het om een selectie van uitspraken die juridisch interessant zijn, of om uitspraken in zaken waar algemene maatschappelijke belangstelling voor is.
> http://www.jure.nl

Korps Landelijke Politiediensten (KLPD)
Het KLPD voert politietaken uit die een specialistisch karakter hebben of een bijzondere organisatie vergen, en taken die de grenzen van de politieregio's overschrijden dan wel een landelijk of internationaal belang hebben. Het KLPD richt zich op de aanpak van zware, georganiseerde criminaliteit, bestrijding van grof geweld en terrorisme. Kerntaken van het KLPD zijn het leveren van recherche-expertise en recherche-informatie en het bieden van ondersteuning aan de regionale korpsen met specifieke hulpmiddelen, informatietechnologie en logistieke diensten. Het KLPD heeft een landelijk Meldpunt Cybercrime, waar burgers melding kunnen maken van kinderporno en radicale en terroristische uitingen die zij op het internet tegenkomen. Het KLPD is een agentschap onder het ministerie van Veiligheid en Justitie.
> http://www.politie.nl/klpd

Logius
De gemeenschappelijke beheerorganisatie Logius staat ten dienste van alle ministeries en biedt publieke dienstverleners een samenhangende ICT-infrastructuur zodat burgers en bedrijven betrouwbaar, snel en gemakkelijk elektronisch zaken met hen kunnen doen. Logius biedt daartoe als essentiële bouwstenen generieke ICT-diensten voor toegang (PKIoverheid, DigiD), gegevensuitwisseling, informatiebeveiliging en standaardisatie. Organisatorisch valt Logius onder het ministerie van BZK.
> http://www.logius.nl

Mijn digitale wereld
Mijn digitale wereld is een nationale informatiewebsite over internet, e-mail en andere digitale toepassingen. De site is een gids voor de digitale wereld: wat zijn de vele mogelijkheden, hoe werken deze, waar moet u op letten, waar kunt u terecht bij problemen, welke organisaties in Nederland kunnen u verder helpen? De website is een initiatief van de Nederlandse overheid, het bedrijfsleven en diverse maatschappelijke organisaties. Mijndigitalewereld.nl is ontwikkeld als onderdeel van het nationale programma Digivaardig & Digibewust.
> http://www.mijndigitalewereld.nl

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor de ontwikkeling van elektronische dienstverlening van de Rijksoverheid. BZK is om die reden verantwoordelijk voor de veiligheid van deze elektronische diensten. Dit is onder andere terug te vinden in haar rol voor de organisaties ICTU en Logius. Daarnaast is BZK vanuit het belang van nationale veiligheid betrokken bij de beveiliging van ICT en vitale infrastructuren via organisaties als de AIVD en het NCC.[72]
> http://www.rijksoverheid.nl/ministeries/bzk

Ministerie van Economische Zaken, Landbouw en Innovatie

Het ministerie van Economische Zaken, Landbouw & Innovatie is verantwoordelijk voor het creëren van de juiste randvoorwaarden voor een goede werking van elektronische netwerken en -diensten. EL&I is verantwoordelijk voor een functionerende telecom- en ICT-markt met zelfregulering en preventie. Verder heeft EL&I een coördinerende verantwoordelijkheid voor het kabinetsbrede ICT-beleid en het beleid voor informatienetwerken en -diensten.
Het Agentschap Telecom (AT) de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) vallen onder de verantwoordelijkheid van de minister van EL&I.
> http://www.rijksoverheid.nl/onderwerpen/telecomwet-en-regelgeving

Ministerie van Veiligheid en Justitie

Het ministerie van Veiligheid en Justitie staat borg voor de strafrechtelijke handhaving van de wet- en regelgeving op het gebied van ICT-veiligheid door opsporing en vervolging. Het ministerie bepaalt het beleid. Het Openbaar Ministerie en de landelijke- en regionale politiediensten zijn verantwoordelijk voor de uitvoering ervan. Daarnaast werkt het ministerie volop mee aan de preventie van cybercrime via voorlichting. Het OM, het KLPD, de NCTV en het NCSC vallen onder de verantwoordelijkheid van de minister van Veiligheid en Justitie.
> http://www.rijksoverheid.nl/onderwerpen/cybercrime

Nationaal Crisis Centrum (NCC)

Plaats van afstemming van de bestuurlijke informatievoorziening en de noodzakelijke bijstand van onder andere politie en brandweer bij (dreigende) verstoringen van openbare orde en/of veiligheid. Het Nationaal Crisis Centrum is onderdeel van het NCTV (Nationaal Coördinator Terrorisme en Veiligheid) dat valt onder het ministerie van Veiligheid en Justitie.
> http://www.nationaalcrisiscentrum.nl

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

De NCTV is aangesteld om de samenwerking tussen alle instanties betrokken bij de bestrijding van terrorisme te verbeteren. De coördinator is verantwoordelijk voor analyse van informatie, beleidsontwikkeling en regie over te nemen beveiligingsmaatregelen bij de bestrijding van terrorisme. Doel is de slagvaardigheid van de overheid vergroten. Het gebruik van het internet voor radicale en terroristische doeleinden wordt bestreden onder regie van het NCTV. Organisatorisch en beheersmatig is de organisatie van de NCTV ondergebracht bij het ministerie van Veiligheid en Justitie.
> http://www.nctv.nl

Nationaal Cyber Security Centrum (NCSC)

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.
Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.
> http://www.ncsc.nl

Nationaal Platform Criminaliteitsbeheersing (NPC)

Het NPC is een publiek-privaat samenwerkingsverband waarbij overheid en bedrijfsleven zich richten op de aanpak van criminaliteitsvormen waarvan het bedrijfsleven slachtoffer is. Het NPC, onder voorzitterschap van de minister van Veiligheid en Justitie, komt twee keer per jaar bijeen om op strategisch niveau van gedachten te wisselen. Daarbij staat zowel de aanpak van huidige criminaliteitsproblemen als de koers voor de langere termijn centraal.
> http://www.rijksoverheid.nl/adres/n/nationaal-platform-criminaliteitsbeheersing-npc.html

72. Dit gaat mogelijk verschuiven naar aanleiding van de Nationale Cyber Security Strategie, zie http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/02/22/nationale-cyber-security-strategie-slagkracht-door-samenwerking.html

National High Tech Crime Unit (NHTCU)

Het Nationaal Team High Tech Crime is een onderdeel van de Dienst Nationale Recherche (DNR) van het Korps Landelijke politiediensten (KLPD). Dit gespecialiseerde team van digitaal rechercheurs onderzoekt vooral vormen van cybercrime waarbij zware en georganiseerde misdaad een rol speelt of als de vorm van cybercrime een (potentieel) ontwrichtend effect heeft op de nationale veiligheid of vitale belangen. Bovendien is dit team internationaal een eerste aanspreekpunt voor buitenlandse opsporingsdiensten en daar waar een landelijke aanpak noodzakelijk is om bedreigende situaties te voorkomen, of te doen stoppen.

Openbaar Ministerie

Het OM is verantwoordelijk voor de bestrijding en aanpak van cybercrime en de vervolging. Het OM heeft een Meldpunt Cybercrime (www.meldpuntcybercrime.nl/), waar burgers melding kunnen maken van kinderporno en radicale en terroristische uitingen die zij op het internet tegenkomen. Bij het Landelijk Parket is een landelijk kennis- en expertisecentrum cybercrime gevormd.
> http://www.om.nl/onderwerpen/cybercrime

Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA)

De Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) houdt toezicht op de naleving van de wet- en regelgeving voor post en elektronische communicatiediensten. Het gaat daarbij met name om de Postwet, de Telecommunicatiewet, de op deze wetten gebaseerde lagere regelgeving en Europese regelgeving. De OPTA handhaaft onder meer het spamverbod.
> http://www.rijksoverheid.nl/adres/o/onafhankelijke-post-en-telecommunicatie-autoriteit-opta.html

Platform voor Informatiebeveiliging (PvIB)

Het PvIB is het kenniscentrum op het gebied van Informatiebeveiliging in Nederland. Het PvIB is het platform waar informatie, kennis en ervaring over informatiebeveiliging wordt verzameld, verbeterd, verrijkt en weer wordt uitgedragen. Het PvIB verenigt alle betrokkenen en geïnteresseerden in het vakgebied Informatiebeveiliging.
> http://www.pvib.nl

Veilig Internetten

Deze website informeert u over veilig internetten en geeft voorlichting en adviezen over computerbeveiliging.
> http://www.veiliginternetten.nl

VNO-NCW

VNO-NCW is de grootste ondernemingsorganisatie van Nederland. VNO-NCW behartigt zowel op nationaal als op internationaal niveau de gemeenschappelijke belangen van het Nederlandse bedrijfsleven. De bij VNO-NCW aangesloten bedrijven en (bedrijfstak)organisaties vertegenwoordigen 90 procent van de werkgelegenheid in de Nederlandse marktsector. Het VNO-NCW heeft een eigen werkgroep rondom het thema informatiebeveiliging en cybercrime.
> http://www.vno-ncw.nl

Waarschuwingsdienst.nl

Waarschuwingsdienst.nl is een dienst van het Nationaal Cyber Security Centrum (NCSC) van de Nederlandse overheid. Deze site is een bron van informatie over veilig internetten en geeft voorlichting en adviezen over computerbeveiliging. Daarnaast waarschuwt de dienst tegen computervirussen, wormen en beveiligingslekken in software.
> http://www.waarschuwingsdienst.nl

Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC)

Het WODC is belast met het verrichten van onderzoek en het doen verrichten van onderzoek, het adviseren over voorgenomen beleidsprogramma's en te voeren beleid en te verrichten onderzoek evenals het verspreiden van binnen het WODC aanwezige kennis op het terrein van Justitie en met de documentatie van (sociaal-)wetenschappelijke publicaties.
> http://www.wodc.nl

BIJLAGE F

Checklist voor vaststellen en aangifte

Deze bijlage geeft een overzicht van technische gegevens voor het vaststellen of sprake is van een cyberincident en van benodigde of gewenste gegevens voor het doen van aangifte van een gepleegd feit.

1 Algemene gegevens

- Gegevens van de aangever:
  - naam;
  - adres en woonplaats;
  - contactgegevens;
  - beroep en functie;
  - identiteitsbewijs.
- Gegevens van de eigenaar/benadeelde: idem;
- Overzicht van gebeurtenissen en getroffen maatregelen;
- Schatting van de geleden schade en de herstelkosten;
- Informatie over mogelijke verdachten.

2 Algemene gegevens over het incident

- Tijdstip van herkenning en/of de (start en einde van de) aanval;
- Gegevens over de locatie, waar het feit is gepleegd (de plaats veiligheidsinbreuk waar het resultaat van de strafbare gedraging zichtbaar is);
- Gegevens van de Internet Service Provider of *Webhosting provider* (naam, adres, contactgegevens, soort contract/ dienst, inlogcodes);
- Gegevens van een daderindicatie (eventueel IP-adres van de verdachte);
- Gegevens van het vermiste, beschadigde, gekopieerde onderwerp (type, model, fabrikant, serienummers, IMEI-nummer, foto's, etc.);
- Specificatie over de aangerichte schade, zoals economische schade, verlies van (gevoelige of persoonsgegevens) gegevens, maatschappelijke impact of het totale verlies aan beschikbaarheid van de services (down time);
- Welke systemen zijn gecompromitteerd?
- Wat zijn dit voor systemen, wat is hun functie?
- Hoe en door wie werd geconstateerd dat het systeem is gecompromitteerd?
- Welke (herstel)acties zijn ondernomen?
- Zijn er reservekopieën (backups) aanwezig en van wanneer?
- Is de hacker nog actief op het systeem?

3 Algemene technische gegevens

Een beschrijving van de (technische) situatie:

- Soort omgeving;
- Gebruikte besturingssystemen en applicaties (inclusief versienummers);
- Netwerktopologie (schema, tekening, componenten, segmentering);
- Draadloze netwerk en fysieke locatie toegangspunten;
- Internet aansluiting (ISP, IP-adres, CallerID-gegevens, bandbreedte);
- Koppelingen met andere (externe) netwerken (inclusief router gegevens);
- Soorten (interne en externe) gebruikers en aantallen;
- Overzicht van alle gebruikersaccounts en hun toegangsrechten;
- Aanwezige beveiligingssystemen (firewalls, IDS, proxies, antivirus);
- Identity & Access management (wachtwoorden, tokens, RBAC);
- Netwerkbeveiliging (VPN, SSL, TLS, WiFi-beveiliging);
- Overige beveiligingsmaatregelen (encryptie, PKI, SIEM, USB-blokkering).

4 Technische gegevens van het incident

Van alle gecompromitteerde systemen (netwerkcomponenten, servers, werkstations, etc.):

- De begin- en eindtijd(en) van het incident;
- IP-adres(sen) betrokken bij de aanval (source en destination);
- Netwerkprotocollen betrokken bij de aanval (inclusief poortnummers);
- Gebruikersnamen (inclusief login-namen, e-mail en dergelijke) betrokken bij de aanval;
- Lijst van toegevoegde, besmette of gewijzigde computerbestanden;
- Welke handelingen zijn verricht aan de gecompromitteerde systemen?
- Zijn er digitale sporen veiliggesteld?

5 Volgen van de aanvaller

In sommige situaties kan het voorkomen dat de aanvaller nog actief is op het systeem.

- Kan de aanvaller worden gevolgd?
- Is het mogelijk om actief te monitoren op de acties die de aanvaller uitvoert?
- Zijn er onafhankelijke voorzieningen om de aanvaller te volgen (zoals een netwerk-tap)?

6 Logbestanden

Logbestanden van de systemen die betrokken kunnen zijn geweest bij het cyberincident (vastgelegd op het tijdstip van herkenning en de gehele periode gedurende het incident). In het bijzonder de begin- en eindtijd(en), source en destination-IP-adressen, (destination-) netwerkpoorten en de netwerkpakketten-headers zijn waardevol:

- Firewalls (complete logs met netwerkverkeer, poorten en IP-adressen);
- IDS en SIEM;
- Volledig netwerkdataverkeer dump (bijvoorbeeld vanuit IDS netwerk sensor);
- Antivirusprogramma's (update logs, meldingen, historie);
- Mailsysteem (log van de inkomende e-mail, inclusief de e-mail-headers die bijvoorbeeld de malware bevatten, en eventueel de relevante e-mailberichten zelf);
- Proxy of gateway server (netwerkverkeer en geautoriseerde connecties);
- Servers (log van besturingssysteem activiteit op de server, security log (aanmeldingen en mislukte aanmeldingen), gemaakte connecties, gebruik van bijzondere privileges, systeemlog (foutmeldingen) en dergelijke);
- Werkstations (log van besturingssysteemactiviteit op de server, security log (aanmeldingen en mislukte aanmeldingen), connecties, gebruik van bijzondere privileges, systeemlog en dergelijke).
- Webbrowser-logs (internethistorie, bookmarks, cookies en dergelijke);
- Logbestanden van de applicaties en applicatieservers die betrokken kunnen zijn geweest bij het cyberincident, zoals webservers, database servers, DNS-servers en FTP-servers.

7 Technische gegevens van betrokken systemen

Van alle betrokken systemen (netwerkcomponenten, servers, werkstations en dergelijke) de configuraties ten tijde van het tijdstip van herkenning en/of het zich voordoen van het incident:

- Systeemtijden en hun verschil met een onafhankelijke bekende tijdsbron.
  Voor een correlatie van logbestanden en het leggen van verbanden is tijdsynchronisatie van essentieel belang.
- Specificatie van platform (hardware) en besturingssysteem (soort, zoals Windows, Linux, Apple en versienummers/servicepacks);
- Overzicht van actieve services (webserver, fileserver, FTP, firewall, mail en degelijke).
- Overzicht van de actieve systeemconfiguratie;
- Lijst van geïnstalleerde programmatuur;
- Informatie over aanwezige firewall en antivirusmaatregelen;
- Netwerkconfiguraties (aansluitingen, IP-adressen);
- Lijst van actieve processen in geheugen;
- Lijst van actief aangemelde gebruikers;
- Lijst van open bestanden;
- Lijst van actieve netwerkverbindingen en netwerkstatus;
- Lijst van gebruikersgroepen en gebruikers;
- Lijst van netwerkshares en -koppelingen;
- Lijst van tijdsgebonden opdrachten;
- Lijst van automatisch geladen programma's.

8 Aanvullende technische gegevens en bestanden

Afhankelijk van de verschijningsvorm en aanvalstechnieken helpt het als de volgende aanvullende technische gegevens en computerbestanden beschikbaar zijn:

Malware

- Kopie van het computervirus of de geïsoleerde bestanden die bij het Trojaans paard horen, bijvoorbeeld door het isoleren van een besmet computerbestand;
- Image van het schone systeem (voordat dit werd geïnfecteerd) en een image van het gecompromitteerd systeem.

Computerinbraak

- Volledig netwerkverkeer (network dump);
- De geïsoleerde bestanden die bij de rootkit of het Trojaanse paard horen;
- Image van het schone systeem (voordat dit werd geïnfecteerd) en een image van het gecompromitteerd systeem.

Spoofing

- Bij ARP-spoofing: MAC-adressen.
- Bij e-mail-spoofing: e-mail (inclusief headers).
- Bij DNS-cache-vervuiling: loggegevens van aanpassing van een A-record.
- Bij DNS-spoofing: overzicht van eventuele geplaatste of aangepaste bestanden met tijdstip van plaatsing/aanpassing.

Sniffing

- Ping-methode of -variant:
  - Beschrijving van het gebruikte protocol met de verwachte resultaten;
  - Logbestand van het netwerkverkeer waaruit blijkt dat een bepaald systeem reageert op een Ping request.
- DNS-methode:
  - Logbestand van het netwerkverkeer waarin te zien is dat na netwerkverkeer te hebben verzonden naar een bepaald IP-adres, een DNS request werd uitgevoerd om de bijbehorende host name op te vragen.
- Uitlokking door honeypot:
  - Documentatie van het gecreëerde account, datum en tijd en locatie van aanmaak, en data en tijden waarop 'legitiem' ingelogd wordt of zal worden;
  - Logbestand van het systeem waaruit inlogpogingen op het gecreëerde account worden vastgelegd.

Open web proxy

- Logbestanden van de server die als open proxy werd gebruikt.

Defacing

- Overzicht van eventuele geplaatste of aangepaste bestanden met tijdstip van plaatsing/aanpassing;
- String (code) die de hacker naar de webserver verzendt;
- Informatie over DNS- en domeinregistratie;
- DNS-loggegevens (bijvoorbeeld van aanpassing van een A-record).

Cross site scripting

- Logbestanden van webserver of proxy;
- String (code) die de hacker naar de webserver verzendt met kenmerken zoals HTTP TRACE of HTTP GET/POST zonder referrer field in de communicatie;
- URL's met verwijzingen zoals IFRAME of <scrips>, <object> of <embed> tags.

SQL-injecties

- Logbestanden van webserver, proxy of database server;
- String (code) die de hacker naar de webserver verzendt met kenmerken zoals SQL-commando's CAST, DECLARE, SELECT, WHERE in de communicatie;
- Databasewaarden waaruit SQL-injectie kan blijken, zoals aanwezigheid van de keywords IFRAME of SCRIPT SRC.

Denial of Service

- De begin- en eindtijd(en), source IP-adressen, destination-IP-adres;
- Overzicht van omvang netwerkverkeer en (netwerk-) connecties in de tijd;
- Gebruikte netwerkpoorten en de netwerkdatapakketten.

Phishing

- naar welke informatie wordt 'ge-phished'?
- wat is het gevolg of mogelijk schade hiervan?
- de vervalste e-mailberichten;
- e-mailadres van de afzender;
- source-IP-adressen;
- een historie van bezochte websites of geopende links (URL's).

Open mail relay

- Logbestanden van de mailserver die als open relay werd gebruikt;
- de methode die werd gebruikt om mail door te sturen. Dit is op te maken uit de MAIL FROM en RCPT-TO-SMTP-instructies die werden gegeven;
- de complete oorspronkelijke e-mail in zijn originele staat (in platte tekst), inclusief de e-mail-headers. Hieruit valt de volgende informatie te halen:
  - Source-IP-adres;
  - Destination-IP-adres;
  - Tijdstip van verzending;
  - Tijdstip van ontvangst;
  - Mail-from-veld (zowel uit de header als de envelop);
  - Recipient-to-veld (zowel uit de header als de envelop);
  - Overzicht van mailservers die de mail hebben ontvangen en verstuurd.

Spam

- Het oorspronkelijke e-mailbericht in zijn originele staat (in platte tekst);
- Source-IP-adres;
- Destination-IP-adres;
- Tijdstip van verzending;
- Tijdstip van ontvangst;
- Mail-from-veld (zowel uit de header als de envelop);
- Recipient-to-veld (zowel uit de header als de envelop);
- Overzicht van mailservers die de mail hebben ontvangen en verstuurd.

BIJLAGE G

Checklist Besturingssystemen

De verschillende bestandslocaties en -instellingen zijn zo generiek mogelijk opgenomen in dit overzicht. Ze gelden voor de meeste versies van de genoemde platformen. De exacte locaties en instellingen kunnen echter afwijken. Bovendien zijn de opgenomen locaties en instellingen in dit overzicht niet limitatief.

G.1 Microsoft Windows

1 Opstartlocaties

Op Windows-platformen zijn technieken voor het automatisch opstarten van programma's [73]:

a. ***Opstartmappen***. Alle huidige Windows-versies bevatten zogenoemde opstartmappen, waarin gebruikers programma's kunnen plaatsen die automatisch opgestart worden zodra de computer opgestart is. De exacte locatie van de opstartmap verschilt per versie van Windows:
   - C:\Documents and Settings\All Users\Start Menu\Programs\Startup
   - C:\Documents and Settings\{Username}\Start Menu\Programs\Startup
   - C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

b. ***Registry***. De exacte locatie verschilt per versie van Windows. De meest voorkomende registry keys zijn[74]:
   - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
   - HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce
   - HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices
   - HKCU\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
   - HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
   - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
   - HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
   - HKLM\Software\Microsoft\Windows\CurrentVersion\Run
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
   - HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
   - HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
   - HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit

2 Netwerkshares en koppelingen

De Windows-platformen delen standaard de lokale harde schijf op het netwerk. Deze standaard-netwerkshares zijn verborgen voor de meeste gebruikers omdat ze zijn bestemd voor beheerders. De exacte locatie en netwerkshares kunnen per Windows-platform en versie verschillen. De voornaamste shares zijn:
- \\computernaam\C$ voor de lokale harde schijf C:\
- \\computernaam\admin$ voor Windows installatiefolder C:\Windows

3 Logbestanden

De logbestanden van het Windows-platform zijn te vinden onder de opties in het systeembeheer-gebeurtenissen-logboek of kunnen (offline) worden gelezen met speciale tools zoals Microsoft Logparser of Event Log Viewer. De logbestanden zijn op de meeste Windows-platformen te vinden onder:
- C:\windows\system32\config*.evt

73. De meeste opstartlocaties kunnen ook allemaal in één keer worden bekeken met de systeem-configuratie tool msconfig.exe of de tool autoruns uit de Microsoft Sysinternals Suite (http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx).
74. HKCU verwijst naar HKEY_CURRENT_USER, HKLM verwijst naar HKEY_LOCAL_MACHINE

4 Systeembestanden en instellingen

De essentiële systeembestanden en instellingen voor controle zijn[75]:

Onderdeel	Commando[76]
• Systeemtijd	date /t & time /t
• Aangemelde gebruikers	net sessions
• Open bestanden	openfiles
• Netwerkconfiguratie	ipconfig /all
• Netwerkverbindingen	netstat -A
• Netwerkstatus	nbtstat -an
• Netwerkroutering	route print
• Proces/netwerkpoort-koppelingen	netstat -anob
• Actieve processen in geheugen	tlist
• Services	net start
• Gebruikersgroepen	net localgroup
• Gebruikers	net user
• Gebruikersinstellingen	net accounts
• Netwerkshares	net share
• Netwerkkoppelingen	net use
• Audit-policy-instellingen	auditpol
• Group-policy-instellingen	gplist
• Tijdsgebonden opdrachten in de Scheduler	at
• Automatisch geladen programma's	autorunsc
• Aanmeld-scripts (logon scripts)	

Onderdeel

- Database Security Accounts Manager (SAM) (in C:\windows\system32\config of C:\Windows\SYSVOL\ntds)
- Windows-aanmeldscherm (normaal MSGINA.DLL en ingesteld onder HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL)
- Alle overige DLL-bestanden (bijvoorbeeld verificatie van integriteit vergelijken met bekende hash-waarden, datum en tijd)
- Gebruikers in alle groepen met bijzondere rechten, met name de beheerdersgroepen (Administrators, Enterprise Administrators, Domain Administrators);
- Toegangsrechten op de Windows Registry.

75. Uitgebreide toelichting kan worden gevonden in diverse literatuur, o.a. op het gebied van digitale forensische analyse van Windows-platformen (Carvey, 2007).

76. De commando's verwijzen naar instructies die op de meeste Windows-platformen direct vanaf een zogenoemde command line zijn uit te voeren. Open (met administrator-rechten) hiervoor de 'Command Prompt' via het menu of door het commando cmd vanaf het startmenu uit te voeren. De uitvoer van een instructie kan worden bewaard door deze direct op te slaan in een tekstbestand als: commando >>resultaat.txt

G.2 Linux

1 Opstartlocaties

Op Linux-platformen zijn technieken voor het automatisch opstarten van programma's onder meer:

- Opstartscripts in /etc/rc*.*
- Opstartscript /etc/rc.d/rc.local
- Opstartprogramma's via *Preferences* onder *Sessions*-menu via het GUI
- Opstartfolder .config/autostart
- Gnome of KDE-autostart-instellingen

2 Netwerkshares en koppelingen

De meeste Linux-platformen delen niet standaard de lokale harde schijf op het netwerk.

3 Logbestanden

De logbestanden zijn op de meeste Linux-platformen te vinden onder:

• /var/log	
• /var/log/message	Algemene (system)meldingen
• /var/log/auth.log	Authenication logs
• /var/log/kern.log	Kernel logs
• /var/log/cron.log	Crond logs (cron job)
• /var/log/maillog	Mailserver-logs
• /var/log/qmail/	Qmail log directory
• /var/log/httpd/	Apache access en error logs directory
• /var/log/lighttpd	Lighttpd access en error logs directory
• /var/log/boot.log	System boot log
• /var/log/mysqld.log	MySQL/Postgress database server log file
• /var/log/secure	Authentication log
• /var/log/utmp	Login-records-bestand

4 Systeembestanden en instellingen

De essentiële systeembestanden en -instellingen voor controle zijn:

Onderdeel	Commando
• Systeemtijd	date
• Netwerkconfiguratie	ifconfig
• Netwerkverbindingen	netstat
• Netwerkstatus	netstat
• Netwerkroutering	netstat
• Services	etc/inet.d
• Gebruikersgroepen	etc/group
• Gebruikers	etc/passwd
• Gebruikersinstellingen	etc/passwd

G.3 Apple Mac

1 Opstartlocaties

Op Apple-platformen zijn technieken voor het automatisch opstarten van programma's:

a. ***Opstartmappen***.
- Hard Drive/Library/ StartupItems
- Hard Drive/System/Library/ StartupItems

b. ***Login items.*** Deze zijn per gebruiker instelbaar onder de System Preferences.

2 Netwerkshares en koppelingen

De meeste Apple-platformen delen niet standaard de lokale harde schijf op het netwerk.

3 Logbestanden

De logbestanden zijn op de meeste Apple-platformen te vinden onder de Console-applicatie (te vinden via Spotlight of in de map Hulpprogramma's). Enkele nuttige logbestanden zijn:
- system.log voor het gehele system waaronder DNS en netwerk
- mail.log
- CrashReporter logs

BIJLAGE H

Stappenplan veiligstellen van digitale sporen

Deze bijlage geeft de systeembeheerder een beeld van de meest elementaire stappen voor het veiligstellen van digitale sporen. Het zelf verrichten van onderzoek wordt echter afgeraden! Belangrijke sporen kunnen onopzettelijk worden gewist en er kan er zelfs sprake zijn van wederrechtelijk handelen. Kom niet (fysiek noch digitaal) aan computers of andere voorwerpen als een strafrechtelijk onderzoek nodig is. Schakel in dat geval direct de autoriteiten (politie) in. Schakel bij twijfel deskundige hulp in, bijvoorbeeld van een particulier recherchebureau.

De te volgen procedures voor het veiligstellen van digitale sporen zijn voortdurend aan verandering onderhevig. Een digitaal rechercheur wordt geacht op de hoogte te zijn van de laatste ontwikkelingen.

Basisstappen voor het veiligstellen van digitale sporen zijn:

1 Veiligstellen van plaats veiligheidsinbreuk

Stel de fysieke omgeving van het gebied rondom de plaats veiligheidsinbreuk (PVI) veilig. Neem foto's van het systeem, inclusief de monitor, randapparatuur, toetsenbord, de voor- en achterkant, kabels en aansluitingen. Maak foto's van papieren, diskettes, usb-sticks en dergelijke in de onmiddellijke omgeving. Inventariseer en verzamel alle papieren, diskettes, usb-sticks en andere middelen die van belang kunnen zijn of bewijsmateriaal kunnen bevatten.

NB: Let op dat volatiele gegevens (tijdelijke vluchtige gegevens in het computergeheugen) eerst moeten worden onderzocht en veiliggesteld vóórdat verder kan worden gegaan met het uitschakelen van het systeem!

2 Shutdown van het systeem

Verwijder de stekker van het systeem uit het stopcontact. **Raak het toetsenbord, muis of aan/uit-schakelaars van het systeem niet aan** noch raak het systeem op andere wijze aan waardoor het een normale shutdown-procedure gaat doorlopen. Een normale shutdown (slaapstand, stand-by, volledig uit) kan logische bommen af doen gaan, bewijsmateriaal vernietigen en data in tijdelijke virtuele geheugens verwijderen.

3 Veiligstellen van het systeem

Het systeem moet verzegeld worden als het intact in beslag genomen moet worden en vervoerd naar een onderzoekslaboratorium. Plaats een lege en tegen schrijven beveiligde diskette of een stuk karton in de *floppy disk drive*. Label alle kabels en connectoren vóórdat deze worden losgekoppeld. Bevestig verzegeling voor bewijsmateriaal over aan/uit-schakelaars, floppy- en cd-romdrives en alle connectoren.

4 Voorbereiden van het systeem

Open de systeembehuizing als het systeem niet in beslag wordt genomen, of zodra het geplaatst is om onderzocht te worden in het laboratorium. Maak foto's van het interieur van het systeem voordat kabels worden losgekoppeld. Koppel alle power-aansluitingen los van hard disks, cd-rom- en floppydrives. Start het systeem en ga naar het startmenu (BIOS).

5 Onderzoek het systeem

Controleer het setup-menu op de actuele systeemdatum en -tijd. Noteer de datum en tijd en vergelijk dit met een bekende standaard. Dit is essentieel voor de verdere correlatie tussen bestandstijden en overig bewijsmateriaal.

6 Voorbereiden van het systeem voor acquisitie

Verander de opstartvolgorde in het systeem (BIOS) naar starten vanaf een cd-rom. Als dat mogelijk moet het systeem worden ingesteld om alleen vanaf een cd-rom op te starten.

NB: de acquisitie (verwerving) van de gegevens op de harde schijf kan ook plaatsvinden door de harde schijf te demonteren en via gespecialiseerde kopieerapparatuur forensisch te klonen (image). Stappen 6 en 7 kunnen dan worden overgeslagen.

7 Aansluiten van doelmedia

Plaats een forensisch schone harde schijf in het systeem als opslagdoel (aansluiten via USB is eventueel ook mogelijk). Sluit alleen deze doel-hard-disk aan. Deze doelschijf moet als disk1 worden geconfigureerd en de originele harde schijf als disk2.
Alle maatregelen om te voorkomen dat het originele systeem opstart moeten worden genomen. Plaats daarvoor de forensische boot-cd-rom met de acquisitie-software. Start het systeem van de forensische boot-cd-rom en controleer of de doelschijf wordt herkend.
Zet het systeem weer uit en sluit nu de power-aansluiting van de originele harde schijf weer aan.

8 Kopiëren van media

Start het systeem opnieuw van de forensische boot-cd-rom. Gebruik de software op deze cd-rom voor het kopiëren van de originele harde schijf naar de doelschijf. Wordt gebruik gemaakt van gespecialiseerde kopieerapparatuur, dan moet de originele harde schijf 'uitgebouwd' en aangesloten worden op deze apparatuur. Maak indien mogelijk een 2^{e} kopie.

9 Veiligstellen van bewijsmateriaal

Verwijder alle harde schijven uit het systeem. Plaats deze in een antistatische elektronicazak (gebruik hiervoor nooit standaard-plastic-seal-bags). Verzegel deze zak met een bewijsmateriaalzegel en noteer hierop data, tijdstip en initialen van de onderzoeker. Plaats al het bewijsmateriaal achter slot en grendel.

Vermeld bij het veiligstellen van sporen altijd door wie, hoe, waar, wanneer, wat en waarmee sporen zijn veiliggesteld.

Checklist Wet bescherming persoonsgegevens (Wbp)

1 Algemene checklist Wbp

In zijn algemeenheid kunnen de volgende stappen bij een onderzoek naar cyberincidenten worden onderscheiden om te voldoen aan de Wet bescherming persoonsgegevens.

Stap 1	Inventariseer de verwerkingen van persoonsgegevens binnen de organisatie.
Stap 2	Is er sprake van een verwerking van persoonsgegevens in de zin van de Wbp (artikel 2, 3 en 4 Wbp).
Stap 3	Stel per verwerking vast welke partijen een rol spelen bij de verwerking, te weten: • Wie is de verantwoordelijke; • Is er een bewerker; • Wie zijn de betrokkenen; • Aan wie worden de gegevens verstrekt (zie ook artikel 1 Wbp);
Stap 4	Stel een welbepaald en uitdrukkelijk omschreven doel (of de doeleinden) van de verwerking(en) van de persoonsgegevens vast (artikelen 7 en 9 Wbp).
Stap 5	Bepaal wat de rechtmatige grondslag is voor de verwerking(en) van de persoonsgegeven(s) (artikel 8 Wbp).
Stap 6	Bepaal welke gegevens noodzakelijk zijn voor het doel van de verwerking (artikel 11 Wbp).
Stap 7	Bepaal de bewaartermijn van de gegevens (artikel 10 Wbp).
Stap 8	Tref passende technische en organisatorische maatregelen voor de gegevensverwerkingen (artikel 13 en 14 Wbp).
Stap 9	(Indien aanwezig) Vraag instemming aan de OR voor de gegevensverwerkingen (artikel 27 WOR).
Stap 10	Melding van de gegevensverwerking aan het CBP (of indien aanwezig aan de functionaris van de gegevensbescherming), *tenzij het Vrijstellingsbesluit van toepassing is* (artikel 27, 28 en 62 t/m 64 Wbp).
Stap 11	Voldoe aan de informatieplicht en informeer de betrokkenen over: • Welke persoonsgegevens van hem worden verwerkt; • Met welk doel deze gegevens worden verwerkt; • Wie de ontvangers zijn van zijn persoonsgegevens, en welke rechten hij kan uitoefenen tegen het feit dat er persoonsgegevens van hem worden verwerkt (artikel 30 lid 3, 33, 34, 35, 35 en 40 Wbp).

2 Stappen controle eigen werknemers

Voor het *structureel steekproefsgewijs* volgen van werknemers vanwege hun gedrag op het bedrijfscomputernetwerk kunnen de volgende stappen worden onderscheiden.

Stap 1	Stel een welbepaald en uitdrukkelijk geformuleerd doel vast voor de gegevensverwerking. Het doel van de verwerking zou als volgt kunnen worden omschreven: “Interne controle en beveiliging van het bedrijfsnetwerk ter voorkoming van onrechtmatig gedrag en ongeautoriseerde toegang van personen die werkzaam zijn bij [naam organisatie].”
Stap 2	Bepaal wat de rechtmatige grondslag is voor de verwerking. *De verwerking van persoonsgegevens kan worden gerechtvaardigd op grond van artikel 8 sub f Wbp. De gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de werkgever. Het is hierbij wel van belang dat de maatregelen die de werkgever treft in verhouding staan tot het doel van de verwerking.*
Stap 3	Bepaal welke gegevens noodzakelijk zijn om dit doel te verwezenlijken. Houd hierbij rekening met het feit dat de gegevens toereikend en niet bovenmatig zijn in relatie tot het te verwezenlijken doel! Voor de te verzamelen gegevens kan worden gedacht aan: *Naam, functie, IP-nummer, username, wachtwoord, autorisatietabel, logs bezochte pagina’s, geadresseerden en opgevraagde bestanden (zie artikel 32 lid 4 Vrijstellingsbesluit).*
Stap 4	Bepaal de noodzakelijke bewaartermijn voor de verwerkelijking van het doel. *De gegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doel. In het Vrijstellingsbesluit wordt een bewaartermijn van 6 maanden gehanteerd (zie artikel 32 lid 6 Vrijstellingsbesluit).*
Stap 5	Stel een Gedragscode op waarin informatie wordt verstrekt over: • Het toegestane internet- en e-mailgebruik én dat dit internet- en e-mailgebruik van de (betreffende) medewerker(s) door de werkgever wordt gecontroleerd; • Het doel van de gegevensverwerking; • Wat de consequenties zijn van het niet naleven van de afspraken omtrent het toegestane internet en e-mailgebruik; • Welke rechten de betrokkene kan uitoefenen tegen de verwerking van zijn persoonsgegevens; • Wanneer en welke maatregelen worden getroffen in het geval afspraken over het internet en e-mailgebruik niet worden nageleefd.
Stap 6	Instemming van de ondernemingsraad.
Stap 7	Melding bij het CBP (of de benoemde functionaris), mits is voldaan aan alle eisen van artikel 32 Vrijstellingsbesluit. *Artikel 32 van het Vrijstellingsbesluit voorziet in een vrijstelling van melding in geval het doel van de verwerking de ‘interne controle en beveiliging’ is. Weliswaar moet voor de vrijstelling van melding ook worden voldaan aan alle overige eisen van artikel 32 Vrijstellingsbesluit.*
Stap 8	Publicatie Gedragscode op toegankelijke wijze. *‘Op toegankelijke wijze’ houdt in dat de Gedragscode voor een ieder op elk moment zonder drempels toegankelijk moet zijn. Hier kan bijvoorbeeld aan worden voldaan door de Gedragscode te publiceren op het Intranet.*

3 Wanneer de werkgever aangifte wil doen

Stap 9 Informeer de betrokkene op het moment dat daadwerkelijk tot aangifte wordt overgegaan (artikel 34, eerst lid onder b Wbp).
De verantwoordelijke voor de gegevensverwerking heeft de plicht om de betrokkene te informeren op het moment dat hij de gegevens aan een derde verstrekt. Aangezien de politie moet worden beschouwd als een derde, is de verantwoordelijke verplicht te laten weten dat er aangifte wordt gedaan.

4 Stappen in geval van opsporing strafbare gedraging externen

Voor het *structureel* volgen van externen vanwege hun gedrag op het bedrijfscomputernetwerk kunnen de volgende stappen worden onderscheiden.

Stap 1 Stel een welbepaald en uitdrukkelijk geformuleerd doel vast voor de gegevensverwerking. Het doel kan als volgt worden geformuleerd:
“Het controleren van de activiteiten van bezoekers van de website en of het netwerk ter voorkoming van onrechtmatig gedrag en ongeautoriseerde toegang tot de bestanden van [naam organisatie].”

Stap 2 Bepaal wat de rechtmatige grondslag is voor de verwerking.
Evenals bij de controle van het e-mailverkeer en het internetgebruik van eigen werknemers kan deze verwerking van persoonsgegevens worden gerechtvaardigd op grond van artikel 8 sub f Wbp.

Stap 3 Bepaal welke gegevens noodzakelijk zijn om dit doel te verwezenlijken.
Voor de te verzamelen gegevens kan worden gedacht aan:
Source- en Destination-IP-adres, tijdstip van aanval, webserver software, logging van de webserver en dergelijke (zie ook hoofdstuk 2).

Stap 4 Bepaal de noodzakelijke bewaartermijn voor de verwerkelijking van het doel.
Het is aan te bevelen verwerkingen van persoonsgegevens van externen met het oog op het achterhalen van strafbare gedragingen direct te vernietigen zodra deze niet meer nodig zijn voor het lopend onderzoek. Als de persoonsgegevens worden verwijderd is ook niet langer sprake van een verwerking van persoonsgegevens in de zin van de Wbp en hoeft de verwerking ook niet gemeld te worden bij het CBP (of bij de daarvoor aangestelde functionaris).

Stap 5 Melding bij het CBP (of de benoemde functionaris)
Let op! Slechts in het geval dat de verwerkingen van persoonsgegevens ***structureel*** *worden verwerkt, moeten deze ook worden gemeld.*

Stap 6 Publicatie Privacy-statement op de website waarin in ieder geval de volgende informatie is opgenomen:
- contactgegevens van de verantwoordelijke;
- het doel van de gegevensverwerking;
- eventuele ontvangers van de gegevens (waaronder de politie in geval verdenking strafbaar feit), en
- de rechten van de betrokkene.

Het plaatsen van een zogenoemde *login banner* waarin staat dat alléén geautoriseerde gebruikers toegang tot het systeem hebben en als het systeem wordt gebruikt zonder autorisatie, handelingen gevolgd en opgeslagen worden en kunnen worden gebruikt voor aangifte bij de politie.

Colofon

Uitgave
Nationaal Cyber Security Centrum, Den Haag | Januari 2012

Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast voorziet het in informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

Nationaal Cyber Security Centrum
Wilhelmina van Pruisenweg 104 | 2595 AN Den Haag
Postbus 117 | 2501 CC Den Haag

T 070-888 75 55
F 070-888 75 50

E info@ncsc.nl
I www.ncsc.nl

Januari 2012