Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

ICT-Beveiligingsrichtlijnen voor Webapplicaties

VERDIEPING

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. Het NCSC is een onderdeel van de Directie Cyber Security van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

Samenwerking en bronnen
Deze beveiligingsrichtlijnen zijn opgesteld door het NCSC, in een nauwe samenwerking met het Centrum voor Informatiebeveiliging en Privacybescherming (CIP) en met meerdere deskundigen uit publieke en private organisaties. Hun bijdrage, de inhoudelijke reviews evenals openbaar toegankelijke bronnen hebben in sterke mate bijgedragen aan de inhoud van deze beveiligingsrichtlijnen. In bijlage C worden de individuele deskundigen die een bijdrage geleverd hebben met naam genoemd.

ICT-Beveiligingsrichtlijnen voor Webapplicaties

VERDIEPING

INHOUDSOPGAVE

Inleiding

Aanleiding voor de Beveiligingsrichtlijnen

Digitale informatie-uitwisseling is een essentieel onderdeel geworden voor het functioneren van de Nederlandse samenleving. Betrouwbare digitale communicatie is van wezenlijk belang en vraagt om voortdurende zorg. Dat dit geen makkelijke opgave is blijkt wel uit het veelvoud van incidenten. De Beveiligingsrichtlijnen bieden een leidraad naar een veiliger dienstverlening.

Deze ICT-Beveiligingsrichtlijnen voor Webapplicaties (hierna Richtlijnen genoemd) bestaan uit twee documenten die na implementatie bijdragen aan een betere beveiliging van webapplicaties bij organisaties en de (rijks)overheid. Het document Richtlijnen beschrijft de beveiligingsrichtlijnen voor webapplicaties op hoofdniveau, bijbehorend beleid, uitvoering en beheersing. Dit document (Verdieping) vormt een ondersteunend document en beschrijft de beveiligingsrichtlijnen op detailniveau en geeft richting (handelingsperspectief) met betrekking tot de implementatie en controleerbaarheid van de beveiligingsrichtlijnen. Waar mogelijk worden concrete adviezen geven. Met de adviezen in dit deel kan worden voldaan aan de beveiligingsrichtlijnen uit het document Richtlijnen.

Webapplicaties

Wanneer dit document spreekt over een webapplicatie, dan gaat het om een applicatie die bereikbaar is met een webbrowser of een andere client, die ondersteuning biedt voor het Hypertext Transfer Protocol (http). Kern van deze definitie is dat een webapplicatie altijd bereikbaar is op basis van http of de met versleuteling beveiligde vorm hiervan: https (http secure). De functionaliteit die een webapplicatie kan bieden is onbeperkt. De techniek is echter altijd gebaseerd op de http-standaard zoals gedefinieerd in 'Request for Comments' (RFC) 1945[1], 2616[2], 2617[3], 2817[4], 6265[5], 6585[6] en 7540[7].

Ook bijbehorende infrastructuur, het koppelvlak met internet, de opslag van de gegevens en de netwerkservices worden in dit document beschouwd als aandachtsgebied. Voorbeelden van applicaties, die volgens deze definitie onder de noemer 'webapplicatie' vallen, zijn internetsites, extranetten, intranetten, software-as-a-service (SaaS)-applicaties, webservices en web-api's.

Doelgroep

Dit document heeft drie primaire doelgroepen:

- De eerste doelgroep bestaat uit partijen die verantwoordelijk zijn voor het stellen van beveiligingskaders en de controle op naleving hiervan. Hierbij kan worden gedacht aan securitymanagers en systeemeigenaren van de te leveren ICT-diensten.
- De tweede doelgroep bestaat uit diegenen die betrokken zijn bij het ontwerp- en ontwikkelproces, de implementatie en het beheer van webapplicaties. Deze doelgroep moet de beveiligingsrichtlijnen implementeren. Bij deze doelgroep zijn drie partijen te onderscheiden:
  - interne afdelingen.
  - externe leveranciers van software.
  - externe webhostingpartijen.
- De derde doelgroep bestaat uit de controlerende instanties (IT-auditors) die op basis van deze richtlijnen een objectieve ICT-beveiligingsassessment uitvoeren.

Doelstelling

Deze Richtlijnen geven een overzicht van beveiligingsmaatregelen die aanbieders van webapplicaties kunnen nemen om een bepaalde mate van veiligheid te bereiken. De beveiligingsmaatregelen hebben niet alleen betrekking op de webapplicatie, maar ook op de beheeromgeving en de omringende hard- en softwareomgeving die noodzakelijk is om de webapplicatie te laten functioneren.

Toepassing van de Richtlijnen

Organisaties kunnen (een deel van) deze Richtlijnen voor bepaalde toepassingsgebieden verheffen tot een normenkader. In tegenstelling tot de beveiligingsrichtlijnen, die adviserend van aard zijn, is een normenkader dwingend voor het toepassingsgebied. Ook kunnen de Richtlijnen worden gebruikt in aanbestedingen, het uitbesteden van dienstverlening en in onderlinge afspraken bij ketenprocessen. Afhankelijk van de aard en de specifieke kenmerken van de betreffende dienst kunnen beveiligingsrichtlijnen worden geselecteerd en kunnen de wegingsfactoren van de individuele beveiligingsrichtlijnen worden aangepast om de gewenste situatie te weerspiegelen.

Prioriteit

De prioriteit van elke beveiligingsrichtlijn wordt in algemene zin gewaardeerd volgens de classificatie Hoog, Midden of Laag. Deze

1 RFC 1945: Hypertext Transfer Protocol -- HTTP/1.0: http://www.ietf.org/rfc/rfc1945.txt
2 RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1: http://www.ietf.org/rfc/rfc2616.txt
3 RFC 2617: HTTP Authentication (Basic and Digest): http://www.ietf.org/rfc/rfc2617.txt
4 RFC 2817: Upgrading to TLS Within HTTP/1.1: http://www.ietf.org/rfc/rfc2817.txt
5 RFC 6265: HTTP State Management Mechanism: http://www.ietf.org/rfc/rfc6265.txt
6 RFC 6585: Additional HTTP Status Codes: http://www.ietf.org/rfc/rfc6585.txt
7 RFC 7540: Hypertext Transfer Protocol Version 2 (HTTP/2): https://tools.ietf.org/html/rfc7540

drie classificaties vormen drie punten op een continuüm van mogelijke waarden waarbij Hoog de sterkste mate van gewenstheid is (must have), Midden een redelijk sterke mate van gewenstheid is (should have) en Laag een gewenste, maar niet noodzakelijke voorwaarde vormt (nice to have). De drie waarden zijn moeilijk exact te definiëren, maar vormen een functie van kans op optreden van een bedreiging en de mogelijke schade als gevolg hiervan.

De uiteindelijke afweging voor een specifieke webapplicatie voor een specifieke organisatie is afhankelijk van de weging van risico's die uit een risicoanalyse naar voren komen. Daarbij wordt gekeken naar de kans op optreden van een bedreiging, het te verdedigen belang[8] en de mogelijke impact hiervan op de bedrijfsvoering. De beveiligingsrichtlijnen bieden de maatregelen die genomen kunnen worden om het optreden van bedreigingen terug te dringen en/of de impact in geval van optreden van een bedreiging te beperken.

Als voorbeeld van een aanpassing van de algemene classificaties in specifieke situaties kan worden gekeken naar beschikbaarheidsmaatregelen. De noodzaak van beschikbaarheidsmaatregelen kan bijvoorbeeld laag zijn in situaties waar het niet beschikbaar zijn van een webdienst weinig impact heeft op de bedrijfsvoering. De noodzaak kan juist hoog zijn in situaties waar de impact en de kans op optreden van een bedreiging groot zijn.

Uitgangspunten

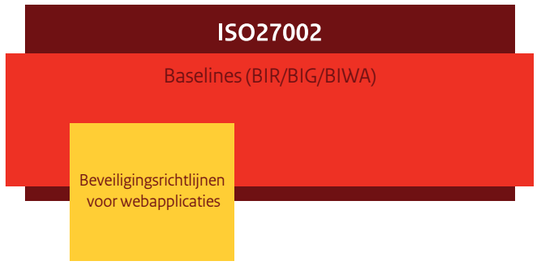
Deze Richtlijnen:

- zijn generiek van opzet en voor een breed spectrum van dienstverlening toepasbaar;
- richten zich op de vier kernaspecten van informatiebeveiliging: beschikbaarheid, integriteit, vertrouwelijkheid en controleerbaarheid;
- hebben betrekking op webapplicaties en de omgeving die hiervoor benodigd is. Dit omvat de hardware waarop de software draait, het netwerk, de koppelingen tussen componenten, het beheer en alle software die noodzakelijk is om de webdienst op een veilige manier aan te bieden;
- kunnen als norm worden gebruikt bij aan- en uitbestedingen van diensten en onderlinge afspraken;
- beschrijven in Richtlijnen vooral beveiligingsmaatregelen op hoog niveau die organisaties kunnen nemen om webapplicaties veiliger te maken;
- beschrijven in Verdieping op detailniveau de (deel)beveiligingsmaatregelen en hoe deze geïmplementeerd kunnen worden.

Context/scope

Deze Richtlijnen richten zich op de beveiliging van webapplicaties vanuit het oogpunt van de aanbiedende partij (de serverzijde). De Richtlijnen richten zich niet op de clientinrichting van gebruikers van de webapplicatie.[9] Er zijn daarom in deze Richtlijnen geen directe beveiligingsmaatregelen opgenomen voor de manier waarop afnemende partijen (de werkstations) veilig gebruik kunnen maken van webapplicaties.

Deze Richtlijnen zijn niet alomvattend en kunnen naast beveiligingsvoorschriften en baselines met een bredere scope (zoals BIR[10] en BIG[11]) worden gebruikt. Waar dergelijke baselines uit een deelverzameling van de maatregelen uit ISO-standaard 27002 bestaan, kennen deze Richtlijnen wel een gedeeltelijke overlap met ISO27002 en baselines, maar zijn ze op bepaalde onderdelen gedetailleerder uitgewerkt.



Figuur 1. Positionering Richtlijnen ten opzichte van ISO27000x en overheidsbaselines

De Richtlijnen bieden specifieke verdieping voor de beveiliging van webapplicaties. De beveiliging van webapplicaties moet passen binnen de beveiligingsopzet die organisaties voor hun overige processen en omgeving al ingericht zouden moeten hebben, bijvoorbeeld op basis van de ISO 27002.

Deze Richtlijnen zijn primair technisch van aard. Dit betekent dat een aantal aspecten van informatiebeveiliging geen onderdeel uitmaakt van het raamwerk dat in deze Richtlijnen wordt gehanteerd. Het raamwerk besteedt bijvoorbeeld nauwelijks tot geen aandacht aan zaken als beveiligingsorganisatie, fysieke beveiliging en personeel. Niet-technische maatregelen worden uitsluitend opgenomen wanneer deze noodzakelijk worden geacht voor de technische context of wanneer andere normenkaders of standaarden hier onvoldoende op ingaan. Indien een risicoanalyse aanleiding geeft voor het invullen van deze aanvullende beveiligingsmaatregelen dan wordt verwezen naar andere beveiligingsstandaarden zoals ISO 27001 en ISO 27002.

Deze Richtlijnen zijn het uitgangspunt voor de beveiliging van webapplicaties en een organisatie kan de beveiliging van zijn webapplicaties (laten) toetsen op basis van deze Richtlijnen. De toetsende organisaties kunnen deze Richtlijnen gebruiken om een objectief beveiligingsassessment uit te voeren. Bij het beoordelen van een specifieke situatie en bij het implementeren van de Richtlijnen (het oplossen van tekortkomingen) kan naar deze Richtlijnen verwezen worden.

Verschil tussen versie 2012 en versie 2015

De opbouw van de Richtlijnen versie 2012 was gebaseerd op het raamwerk beveiliging webapplicaties (RBW)[12] van het NCSC en onderverdeeld naar de volgende lagen:

- Algemene maatregelen
- Netwerkbeveiliging
- Beveiliging van het platform/besturingssysteem
- Beveiligen van een webapplicatie op applicatieniveau
- Afscherming van webapplicaties via authenticatie- en autorisatiemechanismen
- Implementatie van vertrouwelijkheid en onweerlegbaarheid in webapplicaties
- Integratie van de webapplicatie met de verschillende beveiligingscomponenten
- Inrichting van monitoring, auditing en alerting

De opbouw en formulering van deze Richtlijnen, versie 2015, is gebaseerd op het SIVA-raamwerk.[13] Dit raamwerk helpt bij het systematisch in kaart brengen van auditobjecten en de beschrijving van richtlijnen voor de in kaart gebrachte auditobjecten. Daarnaast zorgt het voor een betere verbinding van beleid, uitvoering en beheersing van de te nemen maatregelen.

Het SIVA-raamwerk bestaat uit vier componenten: Structuur, Inhoud, Vorm en Analysevolgorde. In de volgende paragraaf worden Structuur, Inhoud en Vorm besproken. Analysevolgorde gaat over de wijze waarop deze structuur gebruikt wordt bij het ontwikkelen van referentiekaders. Omdat we hier te maken hebben met bestaande richtlijnen voor een specifiek auditobject (webapplicatie-omgeving) is de component Analysevolgorde niet van toepassing. De opbouw van deze Richtlijnen wordt verder toegelicht in de volgende paragraaf.

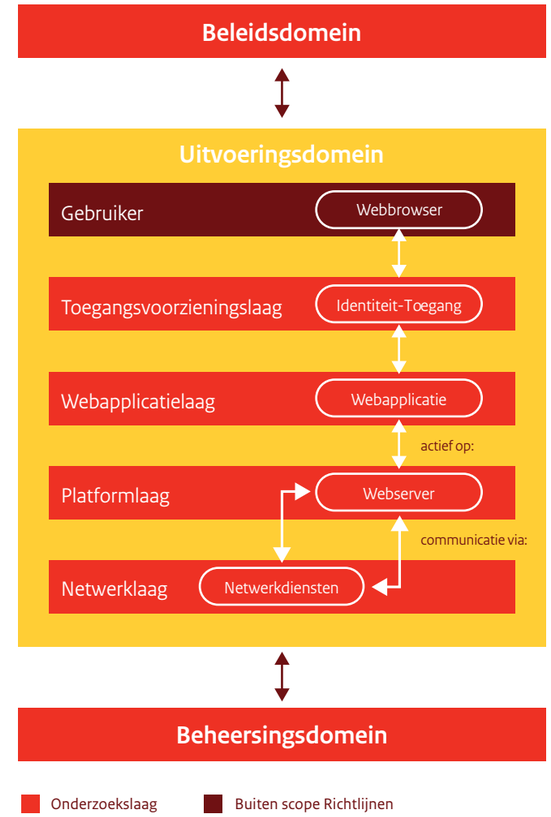
In bijlage F is een verwijzingstabel opgenomen waarin is aangegeven in welke richtlijn(en) iedere richtlijn uit 2012 is opgenomen.

Organisatie van de Richtlijnen

In deze paragraaf wordt de indeling van deze Richtlijnen toegelicht.

Indeling van de webapplicatie-omgeving op basis van domeinen (Structuur)

De beveiligingsrichtlijnen zijn, naar de gelijknamige domeinen, georganiseerd in drie hoofdstukken: beleidsdomein, uitvoeringsdomein en control- of beheersingsdomein. Deze indeling komt voort uit het SIVA-raamwerk. Figuur 2 geeft de indeling van de richtlijnen.



Figuur 2. Indeling van de beveiligingsrichtlijnen

8 Of mate van bereidheid risico's te accepteren.
9 Clientbeveiliging ligt gezien de diversiteit buiten de scope en worden qua risico geclassificeerd als een niet te beïnvloeden en niet te vertrouwen factor.
10 BIR = Baseline Informatiebeveiliging Rijksdienst
11 BIG = Baseline Informatiebeveiliging Nederlandse Gemeenten
12 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/raamwerk-beveiliging-webapplicaties.html
13 Voor achtergronden en de wetenschappelijke basis van het SIVA-raamwerk wordt verwezen naar het proefschrift van W. Tewarie. 'SIVA – Methodiek voor de ontwikkeling van auditreferentiekaders', 2014.

Beleidsdomein
Hier bevinden zich elementen die aangeven wat in organisatiebrede zin bereikt kan worden en bevat daarom conditionele en randvoorwaardelijke elementen die van toepassing zijn op de overige lagen, zoals doelstellingen, informatiebeveiligingsbeleid, strategie en vernieuwing, organisatiestructuur en architectuur.

Uitvoeringsdomein
In dit domein wordt de implementatie van de ICT-diensten uiteengezet, zoals toegangsvoorzieningen, webapplicaties, platformen, webservers en netwerken.

Beheersingsdomein
Evaluatieaspecten en meetaspecten zijn in dit domein opgenomen. Daarnaast treffen we hier ook de beheerprocessen aan, die noodzakelijk zijn voor de instandhouding van ICT-diensten. De informatie uit de evaluaties en de beheerprocessen is niet alleen gericht op het bijsturen van de geïmplementeerde webapplicaties, maar ook om het bijsturen en/of aanpassen van de eerder geformuleerde conditionele elementen die gebaseerd zijn op “onzekere” informatie en aannames, visie en uitgestippeld beleid.

Een voorbeeld van een dergelijke aanname is een inschatting van de capaciteitsbehoefte. In de praktijk kan (en zal) het gebruik anders zijn dan oorspronkelijk verondersteld. Dan is een mechanisme nodig dat de daadwerkelijke belasting meet en een proces waarin eventueel noodzakelijke veranderingen worden vastgesteld en doorgevoerd.

Maatregelen per domein (Inhoud)
Binnen de domeinen zijn de verschillende onderwerpen benoemd. Binnen het uitvoeringsdomein is bovendien een verdere structuur aangebracht, om uitdrukking te geven aan de verschillende (technische) disciplines die hier een rol spelen. Ieder onderwerp heeft hier een eigen specifiek beleid en een eigen specifieke beheersing. Daar waar specifiek beleid meerdere onderwerpen raakt, is dit – om dubbelingen tegen te gaan – alsnog als algemeen beleid opgenomen, ook al is de inhoud vrij specifiek van aard. Op dezelfde manier zijn ook vrij specifieke beheersingsmaatregelen in de algemene beheersing terecht gekomen.

Beschrijving van de richtlijnen (Vorm)
De Richtlijnen kennen een doelstelling en een risico. Hiermee is vastgelegd wat de richtlijn inhoudt en waarom deze gesteld wordt. Vervolgens wordt per conformiteitsindicator uit de richtlijn (de onderstreepte trefwoorden) een aantal maatregelen gegeven, waarmee kan worden bereikt (of vastgesteld) dat invulling is gegeven aan de richtlijn. De conformiteitsindicatoren worden nader gedefinieerd in bijlage A.

Waar noodzakelijk zijn maatregelen voorzien van een nadere toelichting (*cursief gedrukt*). Bij sommige richtlijnen is een verdiepende tekst bijgevoegd die dieper ingaat op de mogelijke invulling van bepaalde maatregelen.

Met nadruk wordt gesteld dat de beschreven doelstellingen mogelijk ook met een (deels) andere invulling bereikt kunnen worden dan door de uitwerking die in deze richtlijnen bij de maatregelen wordt aangegeven. De beschreven maatregelen zijn een handreiking aan opdrachtgevers, technici en auditors. Zij zullen zelf de eindafweging moeten maken en deze verantwoorden. Voor het verantwoorden kunnen zij dan verwijzen naar de criteria en doelstellingen, met een beschrijving hoe hieraan op andere wijze invulling is gegeven.

Over de bijlagen
Bijlage A bevat een opsomming plus definitie van alle in deze richtlijn gebruikte conformiteitsindicatoren.

Een overzicht van alle gebruikte afkortingen staat in bijlage B.

Bij het samenstellen van deze beveiligingsrichtlijnen is een aantal literatuurbronnen geraadpleegd. Op plaatsen waar informatie uit literatuurbronnen verwerkt is, wordt naar die bron verwezen in de vorm van ‘[x]’. ‘[x]’ verwijst naar een document opgenomen in bijlage C.

In bijlage D wordt een overzicht gegeven van de in deze beveiligingsrichtlijnen beschreven aanvalsmethoden.

Bijlage E bevat een beschrijving van mogelijke kwetsbaarheden die zich kunnen voordoen in de verschillende domeinen.

Bijlage F is een tabel waarin de maatregelen uit de beveiligingsrichtlijnen uit 2012 worden gerelateerd aan de overeenkomstige maatregelen uit deze richtlijn.

Tot slot gebruiken de beveiligingsrichtlijnen ook voetnoten om bepaalde termen of begrippen te verduidelijken. Deze voetnoten herkent u aan een cijfer in superscript (bijvoorbeeld: [3]).

NOOT Als dit document de naam van een product, dienst, fabrikant of leverancier noemt, betekent dit niet dat het NCSC deze op enige wijze goedkeurt, afkeurt, aanraadt, afraadt of op een andere manier hiermee verbonden is.

Onderhoud van de Richtlijnen
Het NCSC is verantwoordelijk voor het opstellen en onderhouden van deze Richtlijnen en zal ze periodiek actualiseren. Indien noodzakelijk zal het NCSC tussentijds door middel van een addendum of erratum de Richtlijnen aanpassen.
Hebt u aanvullingen op, opmerkingen over of eigen ervaringen met deze Richtlijnen? Het NCSC ontvangt ze graag via richtlijnen@ncsc.nl.

Relatie met andere documenten
Deze Richtlijnen zijn afgeleid van het ‘Raamwerk beveiliging webapplicaties (RBW)’ [1] van het NCSC. De beveiligingsadviezen uit het RBW zijn in dit document op een andere wijze gerangschikt en in sommige gevallen opgedeeld indien dit de opbouw ten goede kwam (zie bijlage F voor de verwijzingstabel).

Daarnaast wordt in beveiligingsrichtlijnen verwezen naar de volgende relevante normen, standaarden, best practices, zoals:
- Open Web Application Security Project (OWASP)[14] Top 10 2013 [2]
- OWASP Testing Guide v3 [3]
- OWASP Code Review Guide [4]
- OWASP Application Security Verification Standard (ASVS) [5]
- NEN-ISO/IEC 27001 ‘Managementsystemen voor informatiebeveiliging’ [6][15]
- NEN-ISO/IEC 27002 ‘Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging’ [7][16]
- NEN-ISO/IEC 27005 ‘Information security risk management’ [8][17]
- Basisnormen Beveiliging en Beheer ICT-infrastructuur [9]
- Nederlandse Overheid Referentie Architectuur (NORA)[18] Dossier Informatiebeveiliging [10]

---

14 Het Open Web Application Security Project (OWASP) is een wereldwijde charitatieve not-profitorganisatie met als doel de beveiliging van applicatiesoftware te verbeteren. Hun missie is om applicatiebeveiliging zichtbaar te maken, zodat mensen en organisaties een weloverwogen beslissingen kunnen nemen over de veiligheidsrisico’s met betrekking tot applicaties. OWASP heeft ook een Nederlandse Chapter <https://www.owasp.org/index.php/Netherlands>.

15 NEN-ISO/IEC 27001:2013 specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bij-houden en verbeteren van een gedocumenteerd ISMS in het kader van de algemene bedrijfsrisico’s voor de organisatie. De eisen in deze internationale norm zijn algemeen en bedoeld om van toepassing te zijn voor alle organisaties, ongeacht type, omvang of aard.

16 NEN-ISO/IEC 27002:2013 geeft richtlijnen en principes voor het initiëren, het implementeren, het onderhouden en het verbe-teren van informatiebeveiliging binnen een organisatie.

17 NEN-ISO/IEC 27005 geeft richtlijnen voor risicobeheer en ondersteunt de uitvoering van informatiebeveiliging op basis van een risicomanagementaanpak.

18 De Nederlandse Overheid Referentie Architectuur (NORA) bevat principes, beschrijvingen, modellen en standaarden voor het ontwerp en de inrichting van de elektronische overheid. Het is een instrument dat door overheidsorganisaties kan wor-den benut in de verbetering van de dienstverlening aan burgers en bedrijven <http://www.e-overheid.nl/onderwerpen/e-overheid/architectuur/nora-familie/nora>.

Beleidsdomein

Doelstelling

De doelstelling van het beleidsdomein is om vast te stellen of er voldoende randvoorwaarden op het strategisch niveau zijn geschapen om webapplicaties veilig te doen functioneren, zodat de juiste ondersteuning wordt geleverd voor het bereiken van de afgesproken doelstellingen.

Inleiding

In dit domein zijn richtlijnen opgenomen voor algemeen beleid rondom webapplicaties: beleid dat individuele technische domeinen overstijgt. Met dit beleid geven organisaties de kaders waarbinnen de realisatie en operatie van webapplicaties moet plaatsvinden. Ook dient in dit beleid te zijn beschreven onder welke voorwaarden processen en systemen ondergebracht mogen worden in een cloudomgeving.[11][19] Tevens dient beschreven te worden hoe dit beleid op naleving wordt gecontroleerd.

Risico's

Door het ontbreken van een door het management uitgevaardigd beleid bestaat het risico dat onvoldoende sturing wordt gegeven aan de veilige inrichting van de ICT-omgeving waar de webapplicatie een onderdeel van uitmaakt. Dit zal een negatieve impact hebben op de realisatie van organisatiedoelstellingen.

Kwetsbaarheden en bedreigingen

In bijlage E wordt een overzicht gegeven van de mogelijke kwetsbaarheden en bedreigingen die van belang zijn voor webapplicaties. De volgende kwetsbaarheden en bedreigingen spelen een rol op deze laag: lekken van informatie en weerlegbaarheid, misbruik van een vals subcertificaat voor een specifiek domein en misbruik van een vals rootcertificaat.

Beveiligingsrichtlijnen

Binnen de laag Beleid worden onderstaande richtlijnen beschreven en per richtlijn worden conformiteitsindicatoren en de betreffende maatregelen uitgewerkt.

- Informatiebeveiligingsbeleid (B.01)
- Toegangsvoorzieningsbeleid (B.02)
- Risicomanagement (B.03)
- Cryptografiebeleid (B.04)
- Contractmanagement (B.05)
- ICT-landschap (B.06)

B.01 Informatiebeveiligingsbeleid

Omschrijving

Informatiebeveiliging start bij een door het management ondersteund informatiebeveiligingsbeleid, waarover helder wordt gecommuniceerd met medewerkers en, indien relevant, externe partners.

Organisaties die niet voldoen aan de ISO-standaard 27002 of een daarop gebaseerde baseline, worden geadviseerd de ISO-27002 hanteren om tot een deugdelijk algemeen informatiebeveiligingsbeleid, zowel qua proces als inhoud, te komen. Het informatiebeveiligingsbeleid legt onder meer vast hoe de organisatie ten aanzien van informatiebeveiliging is ingericht en wie welke taken en verantwoordelijkheden heeft.

Voor de beveiliging van webapplicaties zijn er enkele specifieke aandachtspunten ten aanzien van de inhoud van het informatiebeveiligingsbeleid.

Beveiligingsrichtlijn B.01

Informatiebeveiligingsbeleid formuleren

Richtlijn (wie en wat)
De organisatie formuleert een informatiebeveiligingsbeleid en besteedt hierin specifiek aandacht aan webapplicatiegerelateerde onderwerpen zoals dataclassificatie, toegangsvoorziening en kwetsbaarhedenbeheer.

Doelstelling (waarom)
Hiermee wordt ervoor gezorgd dat in het beveiligingsproces specifiek aandacht is voor de webapplicaties van de organisatie.

Risico
Onvoldoende sturing van inspanningen op het gebied van informatiebeveiliging ten aanzien van webapplicaties, waardoor deze niet of onvoldoende bijdragen aan de doelstellingen van de organisatie.

Classificatie
Hoog

Richtlijn 2012
Bo-1

19 Dit geldt zowel voor infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS) als software-as-a-service (SaaS) cloud-oplossingen.

Maatregelen

informatiebeveiligingsbeleid

01 Het informatiebeveiligingsbeleid voldoet aan de eisen die in ISO-standaard 27002[20] of een voor de organisatie geldende baseline worden gesteld.
Denk hierbij voor gemeentes aan de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG).
Voor de Rijksoverheid gelden het Voorschrift Informatiebeveiliging Rijksdienst (VIR) en de Baseline Informatiebeveiliging Rijksdienst (BIR).

02 Laat het informatiebeveiligingsbeleid vaststellen door verantwoordelijk hoger management (CxO–niveau).

dataclassificatie

03 Stel een dataclassificatieschema op.
Met behulp van het schema kan bepaald worden welke mate van beveiliging vereist is.

toegangsvoorziening

04 Formuleer specifiek beleid voor het verlenen van toegang tot functies en gegevens aan personen en systemen.

kwetsbaarhedenbeheer

05 Formuleer voorschriften om de risico's van kwetsbaarheden in ICT-componenten te verminderen.
Denk hierbij bijvoorbeeld aan voorschriften voor hardening van platform- en netwerkcomponenten en voorschriften voor het tijdig doorvoeren van patches en security-updates van softwarecomponenten.

06 Voer een responsible-disclosurebeleid[21] in.
Beveiligingsonderzoekers kunnen zo gevonden kwetsbaarheden in uw website op een vertrouwelijke manier melden. U kunt deze dan herstellen voordat anderen er misbruik van kunnen maken.

B.02 Toegangsvoorzieningsbeleid

Omschrijving

Het toegangsvoorzieningsbeleid maakt deel uit van het informatiebeveiligingsbeleid en geeft regels en voorschriften voor de organisatorische en technische inrichting van de toegang tot ICT-voorzieningen, bijvoorbeeld applicatie (gebruikers) en ICT-componenten (beheerders). Het toegangsvoorzieningsbeleid beschrijft onder andere de manier waarop de organisatie omgaat met identiteits- en toegangsbeheer.

Beveiligingsrichtlijn B.02

Toegangsvoorzieningsbeleid formuleren

Richtlijn (wie en wat)
Het toegangsvoorzieningsbeleid formuleert, op basis van eisen en wensen van de organisatie, richtlijnen voor de organisatorische en technische inrichting (ontwerp) van de processen en middelen, waarmee de toegang en het gebruik van ICT-diensten gereguleerd wordt.

Doelstelling (waarom)
De effectieve toegang tot informatiesystemen voor bevoegde gebruikers bewerkstelligen en de integriteit, vertrouwelijkheid en controleerbaarheid van de gegevens binnen informatiesystemen garanderen.

Risico
Door het ontbreken van toegangsvoorzieningsbeleid kan er onduidelijkheid ontstaan bij het toekennen van rechten aan gebruikers. Hierdoor kunnen niet-geautoriseerde gebruikers mogelijk toegang krijgen tot informatie waarop zij geen recht horen te hebben.

Classificatie
Hoog

Richtlijn 2012
Bo-12

Maatregelen

eisen en wensen

01 Documenteer zakelijke behoeften en beveiligingseisen voor de toegangsvoorzieningen en stel deze vast.
Eisen en wensen bepalen functionele (zakelijke) en niet-functionele (beveiligings)eisen met betrekking tot toegangsvoorziening. De functionele eisen zijn gerelateerd aan de faciliteiten voor de medewerkers om op een efficiënte en effectieve manier zijn/haar taken te kunnen uitvoeren en de juiste resources (data) te kunnen benaderen. De niet-functionele eisen zijn gerelateerd aan de faciliteiten om beveiliging te kunnen realiseren.

organisatorische inrichting

02 Identificeer gebruikersgroepen, -profielen en/of –rollen.
De organisatie legt gebruikersgroepen, -profielen en/of -rollen vast.
Hiermee wordt beschreven welke soorten gebruikers zijn onderscheiden.
Er moet specifiek aandacht zijn voor de anonieme (internet)gebruiker: wat krijgt hij te zien, wat mag hij doen.

03 Leg alleen de hoogst noodzakelijke gegevens van gebruikers vast.
Digitale identiteiten zijn gevoelige persoonsgegevens, waarvan de beveiliging de hoogste aandacht moet hebben.
Publiceer het privacybeleid waarin is vastgelegd hoe de organisatie met digitale identiteiten en persoonsgegevens omgaat.

04 Leg de relatie vast tussen gebruikersgroepen, -profielen en/of -rollen en het dataclassificatieschema.
Hier wordt het dataclassificatieschema van B.01/03 bedoeld.

05 Leg vast welke combinaties van functies, taken en/of rollen ongewenst zijn (functiescheiding).
Het proces van aanvraag, toekenning, schorsing en intrekking kent een zodanige functiescheiding, dat het niet mogelijk is voor één enkele functionaris om – direct of indirect – volledige controle over alle middelen toe te wijzen aan één gebruiker.
Het beheerproces van de technische middelen voor identificatie, authenticatie en autorisatie kent een zodanige functiescheiding, dat het niet mogelijk is voor één enkele beheerder om – direct of indirect – volledige controle over alle middelen te verwerven.

06 Stel eisen aan de toegestane authenticators.
Denk hierbij aan regels voor wachtwoorden (lengte, complexiteit, hergebruik), maar ook aan de toepassing van biometrie, crypto-keys, en dergelijke.
Ook indien er geen expliciete eisen aan een authenticator worden gesteld, dient dit als zodanig gedocumenteerd te zijn.

technische inrichting

07 Stel eisen aan de inzet van technische middelen voor identificatie, authenticatie en autorisatie.

08 Stel richtlijnen en procedures op voor de technische inrichting van toegangsvoorzieningen (identificatie, authenticatie en autorisatie) in informatiesystemen, besturingssystemen en netwerken.
Deze richtlijnen zullen in ieder geval in lijn moeten liggen met de richtlijnen voor platformen en webservers (zie U/PW.01), met eventueel specifieke aanvullingen.

09 Stel eisen aan:
- de uniformiteit en flexibiliteit van authenticatiemechanismen;
- de rechten voor platformaccounts;
- het automatisch verbreken van de sessie (zie ook richtlijn U/WA.08);
- de identificatie/authenticatie(mechanismen) om voldoende sterke wachtwoorden af te dwingen.
  - *Bij de regelgeving in het beleid over platforminrichting zou er onder andere aandacht moeten zijn voor het inperken van rechten van platformaccounts om:*
- *schade als gevolg van aanvallen via bijvoorbeeld buffer-overflows en code-injecties te beperken;*
- *nieuwe bestanden aan te kunnen maken of bestaande bestanden te kunnen wijzigen of verwijderen.*

10 Baseer de inrichting van het identiteit- en toegangsbeheer op een vastgesteld ontwerp.
In dit document is vastgelegd welke functies (identiteit-, authenticator-, profiel- en toegangsbeheer) waar (centraal/decentraal) worden uitgevoerd.

20 ISO/IEC 27002:2013: Chapter 5. Information Security Policies.
21 Voor meer informatie, zie: https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsiblediscl osure.html.

B.03 Risicomanagement

Omschrijving

De impact van een kwetsbaarheid is zeer afhankelijk van de (web) applicatie en de ondersteunende infrastructuur waarin deze kwetsbaarheid zich bevindt. De impact wordt ook mede bepaald door de functionaliteit, de aard van de verwerkte gegevens en het gebruik van de applicatie. Het is dan ook belangrijk dat de beveiligingsbehoeften aan de hand van een risicoanalyse worden bepaald. Een risicoanalyse is het systematisch beoordelen van:
- de schade die waarschijnlijk zal ontstaan door een beveiligingsincident als de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie en andere bedrijfsmiddelen worden geschonden;
- de waarschijnlijkheid dat een beveiligingsincident optreedt rekening houdend met de aanwezige bedreigingen, kwetsbaarheden en de getroffen maatregelen.

De resultaten van deze risicoanalyse worden gebruikt om te bepalen welke prioriteiten moeten worden gesteld ten aanzien van het beheer van beveiligingsrisico's en het implementeren van maatregelen ter bescherming tegen deze risico's. Deze resultaten worden vastgelegd in een informatiebeveiligingsplan. Dit informatiebeveiligingsplan maakt de noodzakelijke stappen voor het implementeren van maatregelen concreet en beschrijft wie wanneer en waarvoor verantwoordelijk is. Hierin wordt ook beschreven dat de maatregelen regelmatig, door middel van onderzoek, worden gecontroleerd op werking en naleving van deze Richtlijnen. Het is belangrijk om de beveiligingsrisico's en geïmplementeerde maatregelen periodiek te evalueren, om:
- in te kunnen spelen op wijzigingen in bedrijfsbehoeften en prioriteiten;
- nieuwe bedreigingen en kwetsbaarheden te bepalen;
- te bevestigen dat maatregelen nog steeds effectief en geschikt zijn.

Beveiligingsrichtlijn B.03

Risicomanagement uitvoeren

Richtlijn (wie en wat)
Voor de webapplicatieomgeving wordt risicomanagement uitgevoerd waarbij (web)applicaties en hun ondersteunende infrastructuur zowel tijdens ontwikkeling als tijdens operationeel gebruik periodiek worden onderworpen aan een (informatie) risicoanalyse.

Doelstelling (waarom)
Bepalen of de risico's (nog) binnen de voor de organisatie acceptabele grenzen liggen en verantwoordelijken informatie verschaffen voor het treffen van eventuele (aanvullende) maatregelen.

Risico
Tekortkomingen in de (web)applicaties en hun ondersteunende infrastructuur worden niet of niet tijdig gesignaleerd. Hierdoor kan de uitvoering van de bedrijfsprocessen die door de (web) applicatie worden ondersteund, worden verstoord.

Classificatie
Hoog

Richtlijn 2012
B0-2

Maatregelen

risicoanalyse

01 Maak gebruik van een breed toegepaste risicoanalyse-methode.
Voorbeelden van bestaande risicoanalyse-methodes:
» **ISF**: Information Risk Analysis Methodology (IRAM)[22]
» National Institute of Standards and Technology (NIST): SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments[23]
» **ISO**: NEN-ISO/IEC 27005:2011 'Information security risk management'
» **Software Engineering Institute (SEI)**: Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)[24]
» **Microsoft:** The Security Risk Management Guide[25]
» **BIG-OP:**
› Baselinetoets v1.0[26]
› Diepgaande Risicoanalysemethode Gemeenten v1.0[27]

02 Voer voor (nieuwe) webapplicaties een risicoanalyse uit en herhaal deze risicoanalyses periodiek.
Dit kan ook door voor clusters van webapplicaties een generieke risicoanalyse uit te voeren en bij geconstateerde kwetsbare functionaliteiten of hogere risico's voor een specifieke webapplicatie een diepgaande analyse uit te voeren.

03 Houd van elke uitgevoerde risicoanalyse de rapportage beschikbaar en stel er een informatiebeveiligingsplan bij op.
Registreer van elke applicatie waarop een risicoanalyse wordt uitgevoerd wanneer dit gebeurd is en wanneer deze hernieuwd moet worden.

04 Volg aantoonbaar de aanbevelingen/verbetervoorstellen uit de risicoanalyses op.
Bij elk rapport is een besluitenlijst, in alle aanbevelingen/verbetervoorstellen uit het rapport van een besluit worden voorzien.
Bij elk besluit tot actie is een registratie van de afwikkeling. Hiervoor kan ook een issue-tracker-systeem[28] gebruikt worden, met verwijzing naar de risicoanalyse.

B.04 Cryptografiebeleid

Omschrijving

Het cryptografiebeleid beschrijft de manier waarop de organisatie omgaat met cryptografisch materiaal en procedures. Cryptografie ligt aan de basis van een reeks belangrijke maatregelen voor informatiebeveiliging. Een solide cryptografiebeleid is daarom een randvoorwaarde om aan deze maatregelen het gewenste vertrouwen te ontlenen.

Beveiligingsrichtlijn B.04

Cryptografiebeleid formuleren

Richtlijn (wie en wat)
Het cryptografiebeleid formuleert eisen die worden gesteld aan processen en procedures rond het beheer van cryptografisch materiaal en de opslag en distributie van dit materiaal.

Doelstelling (waarom)
Beschermen van cryptografische sleutels op een manier die past bij de aard van de cryptografisch beschermde gegevens (data-classificatie B.01/03).

Risico
Het beheer van de cryptografische sleutels sluit niet aan bij het beschermingsbelang van de beschermde gegevens, waardoor het beheer van de cryptografische sleutels niet doelmatig is.

22 https://www.securityforum.org/iram/
23 http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
24 http://www.sei.cmu.edu/solutions/risk/octave-allegro.cfm
25 http://www.microsoft.com/en-us/download/details.aspx?id=6232
26 https://www.ibdgemeenten.nl/wp-content/uploads/2014/06/14-0609-BIG-Baselinetoets-v1.0.pdf
27 https://www.ibdgemeenten.nl/wp-content/uploads/2014/08/14-0806-Diepgaande-risicoanalyse-methode-gemeenten-v1.0-2.pdf
28 http://nl.wikipedia.org/wiki/Issue_tracker of http://en.wikipedia.org/wiki/Issue_tracking_system

Classificatie
Hoog

Richtlijn 2012
B5-1, B5-7

Maatregelen

processen en procedures

01 Stel eisen aan processen en procedures voor aanvraag, creatie, hernieuwing, intrekken en beheer van sleutelmateriaal en certificaten.
Zie NIST SP 800-57 (deel 2)[29] en NIST SP 800-133[30] voor standaarden voor cryptografische processen en procedures.
Certificaten hebben een maximale geldigheid. Borg dat certificaten tijdig worden vernieuwd. Door het certificaat tijdig te vernieuwen blijft de organisatie in staat aan te sluiten bij het vertrouwelijkheidsniveau binnen het public key infrastructure (PKI)-stelsel.

02 Stel eisen aan procedures voor beheer om te zorgen voor een 'soepele' migratie wanneer een patch een certificaat van de lijst met vertrouwde certificaten verwijdert.
Dit geldt ook als leveranciers een deel van de eerder door hen uitgegeven certificaten intrekken.[31]
De maatregelen dienen (langdurige) verstoring van de dienstverlening te voorkomen. Dit kan betekenen dat deze patches worden uitgesteld als nog niet alle certificaten van de systemen vervangen zijn (zie ook C.09).

opslag en distributie

03 Stel eisen aan opslag van sleutelmateriaal.
Besteed expliciet ook aandacht aan back-ups met sleutelmateriaal erin.
Zie NIST SP 800-57 (deel 1[32] en 3[33]) voor standaards voor het werken met cryptografische technieken en sleutels.
Overweeg bij bedrijfskritische systemen met een groot beschermingsbelang van de beschermde gegevens een voorschrift voor het gebruik van een hardware security module (HSM).

04 Stel eisen aan distributie van sleutelmateriaal.
Het distribueren van sleutelmateriaal zal minstens zo goed beveiligd moeten zijn als de bescherming die de sleutels moeten leveren.

B.05 Contractmanagement

Omschrijving

Wanneer de ontwikkeling en/of het beheer over de gehele of een deel van de ICT-dienstverlening met betrekking tot webapplicaties wordt uitbesteed, moeten de beveiligingseisen in een overeenkomst (bijvoorbeeld contract en/of Service Level Agreement (SLA)) tussen beide partijen worden vastgelegd. Dit geldt ook als standaard software wordt ingekocht, zoals bij software-as-a-service (SaaS). Deze overeenkomst moet garanderen dat er geen misverstanden bestaan tussen beide partijen.
Aandachtspunten die in de overeenkomst geadresseerd moeten worden, zijn onder andere:
» Beschrijving van de dienst
Verwijzing per geleverde dienst naar de betreffende service-level-specificaties. Denk hierbij aan concrete beschrijving van diensten, servicetijden (normale servicetijden, weekends, feestdagen en vakantiedagen), servicebeschikbaarheid, responsetijden, oplostijden et cetera.
» Overlegstructuren, contactpersonen en correspondentie
Vastleggen wanneer gestructureerd overleg plaatsvindt, wie aan dit overleg deelnemen. Ook zal een overzicht opgenomen moeten worden van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten (escalatiematrix).
» Geschillen
Beschrijving wat de procedure is bij het optreden van onderlinge conflicten of geschillen tussen gebruikersorganisatie en dienstverlener.
» Prestatie-indicatoren, meten en rapportages
Beschrijving van de prestatie-indicatoren (Key Performance Indicators (KPI's)), hoe deze worden gemeten en hoe hierover wordt gerapporteerd.
» Rapportages
Om zicht te hebben, te krijgen en te houden op alles wat te maken heeft met de dienstverlening. Denk hierbij aan afspraken over de inhoud, de frequentie en de verspreiding (distributie) van de rapportage.
» Beveiliging
Denk hierbij aan afspraken over procedures voor de beveiliging van systemen, services en data, maatregelen bij het schenden van beveiligingsprocedures en hoe met beveiligingsincidenten wordt omgegaan.
» De noodzakelijke beveiligingseisen, zodat aan de beveiligingseisen en -wensen wordt voldaan afspraken over het uitvoeren van audits bij de externe partij;
› afspraken over de toegang tot de ICT-omgeving door derden;

29 http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf
30 http://csrc.nist.gov/publications/nistpubs/800-133/sp800_133.pdf
31 Zie bijvoorbeeld de volgende factsheet 'Certificaten met 1024-bit RSA worden uitgefaseerd' van het NCSC.
https://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-certificaten-met-1024-bit-rsa-worden-uitgefaseerd.html
32 http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf
33 http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf

- afspraken over externe certificering van de (extern) ontwikkelde software. Denk hierbij aan standaardsoftware, software-as-a-service (SaaS) of de ontwikkeling van (maatwerk) software is uitbesteed;
- afspraken om de (extern) ontwikkelde software te mogen auditen, bijvoorbeeld het uitvoeren van codereviews;
- afspraken over het uitvoeren van andere tests, bijvoorbeeld penetratietest (zie maatregel C.04) om mogelijke kwetsbaarheden op te sporen.

Beveiligingsrichtlijn B.05

Contractmanagement vastleggen

Richtlijn (wie en wat)
In een contract met een derde partij voor de uitbestede levering of beheer van een web-applicatie (als dienst) zijn de beveiligings-eisen en -wensen vastgelegd en op het juiste (organisatorische) niveau vastgesteld.

Doelstelling (waarom)
Het handhaven van het beveiligingsniveau, wanneer de verantwoordelijkheid voor de ontwikkeling en/of het beheer van de webapplicatie is uitbesteed aan een andere organisatie.

Risico
Een (web)dienst waarvan de eigenschappen onduidelijk of onberekenbaar zijn, waardoor het gewenste beveiligingsniveau niet gehaald wordt en/of gebruikers onvoldoende vertrouwen in de dienstverlening hebben.

Classificatie
Hoog

Richtlijn 2012
Bo-14

Maatregelen

beveiligingseisen en -wensen

01 Laat het (beveiligings)beleid onderdeel zijn van het pakket beveiligingseisen en -wensen dat is opgesteld bij de verwerving van webdiensten en middelen.
Documenteer van de eisen die voortkomen uit het beveiligingsbeleid of deze door de leverancier ingevuld zijn in de offerte, in het contract en in de uitvoering/levering.

02 Laat de requirements en specificaties voor de webdienst onderdeel zijn van het eisenpakket dat is opgesteld bij de verwerving van diensten en middelen.
Let er op dat hierbij niet alleen de primaire functionele aspecten als requirement worden opgenomen, maar ook beheeraspecten, (management)rapportages en dergelijke.
Deze eisen kunnen ontstaan als uitkomst van onderhandelingen, maar dienen zeker onderdeel van het contract te zijn.

B.06 ICT-landschap

Omschrijving

In het ICT-landschap legt de organisatie vast welke ICT-componenten er zijn en hoe deze aan elkaar gerelateerd zijn. Het verschaft inzicht en overzicht over de ICT-componenten en hun onderlinge samenhang. Bovendien wordt uit het ICT-landschap duidelijk hoe de componenten de bedrijfsprocessen van de organisatie ondersteunen. Dit is een belangrijk hulpmiddel bij het uitvoeren van de risicoanalyse.

Belangrijke onderdelen van het ICT-landschap zijn:
» beveiligingsintegratie-aspecten;
» documentatie.

Beveiligingsrichtlijn B.06

ICT-landschap vastleggen

Richtlijn (wie en wat)
De organisatie heeft de actuele documentatie van het ICT-landschap vastgelegd, met daarin de bedrijfsprocessen, de technische componenten, hun onderlinge samenhang en de ICT-beveiligingsarchitectuur.

Doelstelling (waarom)
Het geven van inzicht geven in de relatie tussen techniek en bedrijfsprocessen en de manier waarop en mate waarin deze op elkaar aansluiten. Hiernaast geeft het ICT-landschap inzicht in de interactie en relaties tussen webapplicaties en andere componenten in de ICT-infrastructuur.

Risico
Dagelijkse operatie is niet in lijn met het geformuleerde beleid en de impact van toekomstige innovaties kan niet in volle omvang en geïntegreerd in beeld worden gebracht.

Classificatie
Midden

Richtlijn 2012
Bo-3, B6-1

Maatregelen

bedrijfsprocessen

01 Inventariseer en karakteriseer de bedrijfsprocessen, functies, rollen, et cetera die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
Het gaat hier om zowel primaire processen, functies, rollen et cetera als secundaire. Dus ook technisch beheer van de infrastructuur, identiteitenbeheer.

technische componenten

02 Benoem en beschrijf de technische componenten (waaronder infrastructuur en software) die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
Dit is inclusief de technische componenten die voor de beveiliging gebruikt worden.

03 Benoem en beschrijf de koppelingen met externe netwerken die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
Naast de functionele eigenschappen dient ook de beveiliging van de externe koppelingen opgenomen te worden.[34]

04 Benoem en beschrijf de beveiligingsmaatregelen die hun weerslag hebben (in componenten) in het ICT-landschap.
Deze beschrijving bevat alle (configuratie)elementen die bepalend zijn voor het correct functioneren van de getroffen beveiligingsmaatregel.

onderlinge samenhang

05 Benoem en beschrijf de onderlinge samenhang tussen technische componenten (waaronder infrastructuur en software) die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
Hieronder valt nadrukkelijk ook de relatie tussen de diverse technische componenten en de aanwezige beveiligingsservices, waaronder:
» *de toegangsvoorzieningen (zie U/TV.01);*
» *de (applicatie-)firewall, loadbalancers, et cetera ;*
» *back-up- en restorefaciliteiten.*
Merk op dat technische componenten elkaar onderling ook beveiligingsservices kunnen en zullen leveren. Gezamenlijk vormen zij een (geïntegreerde) dienst.
In het geval van virtualisatie verdienen de regels die op de hypervisor zijn ingesteld extra aandacht. Deze zijn belangrijk om de scheiding van virtuele omgevingen te waarborgen.

06 Benoem en beschrijf de functionele relaties tussen de applicaties die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.
Bij de beschrijving van de functionele relaties hoort ook onder welke voorwaarden welke gegevens worden uitgewisseld.

07 Benoem en beschrijf de onderlinge samenhang tussen bedrijfsprocessen die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.

08 Benoem en beschrijf de samenhang tussen bedrijfsprocessen en technische componenten die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn.

ICT-beveiligingsarchitectuur

09 Geef met behulp van de ICT-beveiligingsarchitectuur inzicht in de relatie tussen de toegangsvoorzieningen en het gehele ICT-landschap (inclusief beveiligingsservices).
De inrichting van het identiteit- en toegangsbeheer is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke functies (identiteit-, authenticator-, profiel- en toegangsbeheer) waar (centraal/decentraal) worden uitgevoerd.
Het architectuurdocument geeft aan op welke wijze de toegangsvoorzieningen onderdeel uit maken van de beveiligingsarchitectuur.

Verdieping

Beveiligingsintegratie

Beveiligingsintegratie houdt in dat een webapplicatie de beschikking krijgt over informatie die aanwezig is binnen de beveiligingscomponenten. Hierdoor kan een beveiligingsoplossing binnen een webapplicatie worden hergebruikt en hoeven ontwikkelaars de betreffende functionaliteit niet in elke webapplicatie afzonderlijk in te bouwen.

Hieronder een overzicht van de verschillende manieren waarop een beveiligingscomponent informatie beschikbaar kan stellen aan de achterliggende webservers:

» Opslaan van gegevens in een tussenliggende datastore
Hierbij plaatst de beveiligingscomponent beveiligingsgegevens in een database. Achterliggende applicaties die deze gegevens willen gebruiken, kunnen de gegevens vervolgens weer uit de database halen. In feite is deze manier van beveiligingsintegratie een combinatie van passieve integratie (beveiligingscomponent plaatst de gegevens altijd in de database) en actieve integratie (de achterliggende applicatie moet de gegevens zelf weer actief uit de database halen).
» Doorgeven van waarden via een querystring
Bij deze oplossing plakt de beveiligingscomponent belangrijke gegevens achter de gebruikte URL in de vorm van een querystring. De achterliggende applicatie kan vervolgens de gegevens uit de querystring gebruiken.
» Doorgeven van waarden via http-headers
De informatie die de beveiligingscomponent wil aanbieden, kan de component ook meesturen via http-headers. De achterliggende applicatie kan besluiten om de gegevens uit deze headers te gebruiken (zie ook U/WA.03).

Met de invoer van elk nieuw beveiligingscomponent dient men zich

34 Zie voor een voorbeeld hiervan de Operationele Handreiking BIR: http://www.earonline.nl/index.php/BIR_-_Operationele_Handreiking_vs._1.0

af te vragen: hoe wordt deze component binnen de omgeving geïntegreerd?

Belangrijk is vast te stellen:
» welke services de omgeving van de beveiligingscomponent zal afnemen;
» op welke manier de omgeving deze services zal afnemen (actief of passief, welke protocollen).

De vereisten die uit deze overwegingen naar voren komen, dienen vervolgens als input voor een productselectie. Door bij elk nieuw of te vervangen beveiligingscomponent deze vereisten in ogenschouw te nemen, ontstaat een omgeving van nauw verwante componenten die moeiteloos met elkaar kunnen communiceren.

Documentatie

De essentie van het documenteren is dat gemaakte ontwerp en inrichtingskeuzen verantwoord en onderbouwd zijn. Dus niet alleen vastleggen wat de huidige situatie (as-is) is, maar ook waarom deze zo is, dus wat de noodzaak van toepassing is. Om dit gefundeerd te onderbouwen zullen er verwijzingen naar functionele eisen, risicoanalyses, best practices en (mogelijke) alternatieven opgenomen moeten worden. Alle gedocumenteerde ontwerpen inrichtingskeuzen moeten te herleiden zijn naar functionele eisen. Documentatie speelt ook een (belangrijke) rol bij het bepalen van de impact van wijzigingen en het voorkomen van ontwerpbeslissingen (fouten). Documentatie moet dan ook na elke wijziging worden bijgewerkt en oude documentatie moet worden gearchiveerd. Dit geldt zowel voor systeem- als gebruikersdocumentatie.

Voor elke maatregel wordt documentatie onderhouden. Daarnaast wordt afhankelijk van de gevoeligheid van de webapplicatie regelmatig het bestaan van maatregelen gecontroleerd en gedocumenteerd. De mate van compliance wordt aan de verantwoordelijke voor de webapplicatie en de beveiligingsfunctionaris gerapporteerd.

Documentatie moet goed leesbaar zijn, voorzien zijn van een datum (evenals de revisiedata), een eigenaar hebben, op een ordelijke manier worden onderhouden en gedurende een bepaalde periode worden bewaard. Er moeten procedures en verantwoordelijkheden worden vastgesteld en bijgehouden voor het opstellen en aanpassen van documentatie. Documentatie kan gevoelige informatie bevatten en er moeten dan ook maatregelen zijn getroffen om de documentatie te beveiligen tegen ongeautoriseerde toegang (inzien en wijzigen).

De set aan documentatie beschrijft onder andere:
» Hoe wordt omgegaan met risicomanagement, de benodigde bedrijfsmiddelen, de geïmplementeerde maatregelen en noodzakelijke mate van zekerheid; kortom de vastgelegde en vastgestelde procedures en processen.
» De plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken zijn duidelijk en schematisch gedocumenteerd, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald.
» De beveiligingsinstellingen van de ICT-componenten zijn zodanig gedocumenteerd dat duidelijk is waarom voor bepaalde instellingen gekozen is (verantwoording en onderbouwing). Hierbij wordt speciale aandacht besteed aan de defaultwaarden voor systeeminstellingen.

Uitvoeringsdomein

Doelstelling

Vanuit de klant- en organisatie-invalshoek is het doel van de diensten op de ICT-lagen betrouwbare diensten te leveren. Vanuit de assessmentinvalshoek is het doel om vast te stellen of de geleverde diensten adequaat en veilig zijn ingericht.

Inleiding

In dit domein zijn richtlijnen opgenomen voor de specifieke ICT-lagen die gerelateerd zijn aan specifieke ICT-diensten. Alle beleidstypen, bijvoorbeeld informatiebeveiligingsbeleid, cryptografiebeleid, etc., die op de beleidslaag vanuit het hoger managementniveau zijn ontwikkeld zijn leidend voor de invulling van deze ICT-lagen. De totale ICT-dienst als geheel en de specifieke ICT-dienst per laag hebben als het ware een part-whole relatie. Dit betekent dat de ICT-lagen als geheel (veilige) diensten bieden aan de organisatie en haar klanten. De specifieke diensten vormen schakels in de keten. Onder het motto “de keten is net zo sterk als de zwakste schakel” wordt er aandacht besteed aan de specifieke ICT-diensten. Deze specifieke diensten worden in onderlinge samenhang bezien, bijvoorbeeld de relatie tussen webapplicatie, platformen en het netwerk. Per specifieke ICT-dienst, bijvoorbeeld een netwerklaag, wordt verder bezien vanuit een bepaalde invalshoek. Deze invalshoeken zijn gerelateerd aan de volgende onderwerpen:

- operationeel beleid per specifieke dienst;
- processen, taken en verantwoordelijkheden;
- relaties en afhankelijkheden (tussen diverse typen medewerkers, systemen onderling en communicatie over en weer tussen medewerkers en systemen);
- organisatiestructuur en architectuur.

Domeinen

Binnen het uitvoeringsdomein worden richtlijnen voor de ICT-lagen geformuleerd. De lagen die uitgewerkt worden zijn:

- toegangsvoorzieningsmiddelen;
- webapplicaties;
- platformen en webservers;
- netwerken.

De betrokken maatregelen zullen binnen de specifieke lagen worden uitgewerkt.

UITVOERINGSDOMEIN
» TOEGANGSVOORZIENINGSMIDDELEN

Doelstelling

De doelstelling van de laag "Toegangsvoorzieningsmiddelen" is om te waarborgen dat de toegang tot objecten als data, webapplicaties, computerapparatuur en netwerken ingericht is volgens specifieke beleidsuitgangspunten van de organisatie. De werking voldoet aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid van deze objecten.[35]

Inleiding

Toegangsvoorziening bestaat uit twee hoofdcomponenten: identiteitbeheer en toegangsbeheer. Identiteitbeheer en toegangsbeheer zijn onlosmakelijk met elkaar verbonden. Toegangsbeheer is vrijwel betekenisloos wanneer geen correcte invulling is gegeven aan identiteitbeheer. In deze richtlijnen worden deze twee lagen daarom gezamenlijk behandeld.

Binnen het authenticatieproces wordt ervoor gezorgd dat alleen onder vooraf vastgestelde voorwaarden de identiteit van een gebruiker of systeem wordt geregistreerd, een authenticatiemiddel wordt verstrekt en autorisaties worden verleend.

Binnen de technische realisatie van de toegangsvoorzieningen worden identiteiten gecontroleerd, gerealiseerd en beschikbaar gesteld aan de ICT-omgeving.

Onder identiteitbeheer vallen alle activiteiten die nodig zijn in het kader van identiteiten. Het gaat hierbij om het beheer van identiteiten: het toevoegen, verwijderen en wijzigen van identiteiten, maar zeker ook het authenticeren van identiteiten op basis van hun authenticator. Een identiteit bestaat uit een identifier (zoals een gebruikersnaam), een authenticator (zoals een wachtwoord) en een gebruikersprofiel.

Toegangsbeheer heeft als doel om gebruikers op een efficiënte manier te voorzien van de juiste autorisaties, op basis van 'least privilege', 'need-to-know' of 'need-to-access'. Toegangsbeheer betreft alle activiteiten die webapplicaties moeten uitvoeren om de autorisaties voor webapplicaties in te regelen en af te dwingen, zoals het in runtime verifiëren van autorisaties op basis van een autorisatietabel: mag een gebruiker wel of geen gebruik maken van (delen van) de webapplicatie.

De identifier en/of het gebruikersprofiel bepaalt vervolgens welke autorisaties een gebruiker krijgt binnen de webapplicatie.

Risico's

Door het ontbreken van adequate toegangsbeveiliging tot (web) applicaties, systemen en netwerken bestaat het risico dat onbevoegden zich toegang kunnen verschaffen tot deze objecten, waardoor ongewenste acties op de services kunnen plaatsvinden en/of informatie kan worden ontvreemd of verminkt.
Identiteiten zijn gevoelige persoonsgegevens. Wanneer een systeem onvoldoende bescherming biedt tegen misbruik of diefstal kan dit leiden tot identiteitsfraude (binnen het systeem of elders met misbruik van identiteiten uit het systeem).

U/TV.01
Toegangsvoorzieningsmiddelen

Omschrijving

Als het ontwerp met betrekking tot identiteit- en toegangsbeheer is vastgesteld, kan worden bepaald waar het toegangsvoorzieningsmiddel, zogeheten identiteit- en toegangsmanagement (IAM)-tooling, wordt ingezet.

De keuze voor dergelijke tooling wordt mede bepaald door de keuze om delen van identiteit- en toegangsbeheer buiten webapplicatie(s) te plaatsen (te centraliseren). Het inzetten van tooling 'vermindert' de complexiteit van webapplicaties omdat het authenticeren en autoriseren van gebruikers los wordt gekoppeld van de webapplicatie. Door de authenticatie los te koppelen van de webapplicatie, is het eenvoudiger om in de toekomst andere authenticatoren in te zetten voor het beveiligen van de webapplicatie. Hiervoor worden wijzigingen doorgevoerd in de tooling en hoeft de achterliggende webapplicatie hier 'in principe' niets van te merken.

Beveiligingsrichtlijn U/TV.01

Toegangsvoorzieningsmiddelen inzetten

Richtlijn (wie en wat)
De inzet van identiteit- en toegangsmiddelen levert betrouwbare en effectieve mechanismen voor het vastleggen en vaststellen van de identiteit van gebruikers, het toekennen van de rechten aan gebruikers, het controleerbaar maken van het gebruik van deze middelen en het automatiseren van arbeidsintensieve taken.

Doelstelling (waarom)
Het efficiënter maken van het identiteit- en toegangsbeheer en zorgen dat functies en gegevens uitsluitend beschikbaar worden gesteld aan diegenen waarvoor deze bedoeld zijn als waarborg voor vertrouwelijkheid en integriteit.

Risico
Gegevens worden ingezien, gewijzigd of verwijderd door individuen die hiervoor vanuit organisatie geen toestemming, recht of opdracht hebben.

Classificatie
Hoog

Richtlijn 2012
Bo-12, B4-1

Maatregelen

vastleggen van de identiteit

01 Ondersteun de initiële vaststelling en vastlegging van de identiteit van personen met het toegangsvoorzieningsmiddel.
In het toegangsvoorzieningsbeleid is vastgelegd met welke mate van zekerheid de identiteit van een persoon moet worden vastgesteld om deze als gebruiker te mogen registreren.

02 Bied adequate bescherming van de vastgelegde gebruikers- en toegangsgegevens met het toegangsvoorzieningsmiddel.
Wachtwoorden moeten altijd eenwegsvercijferd worden opgeslagen door gebruik van hashing in combinatie met salts.

vaststellen van de identiteit (authenticatie)

03 Ondersteun in voldoende mate het vaststellen van de identiteit van natuurlijke personen met het authenticatiemiddel.
In het beleid is vastgelegd met welke mate van zekerheid de identiteit moet worden vastgesteld om van een geslaagde authenticatie te mogen spreken. Dit zal in de regel tot uiting komen in de keuze van (een combinatie van) authenticatiemiddelen.[36]
Het is mogelijk verschillende authenticatiemiddelen te accepteren, die ieder een eigen mate van zekerheid kennen. In dat geval zal bij de autorisatie naar het gebruikte authenticatiemiddel gekeken moeten worden, om te bepalen of de authenticatie voldoende zekerheid geeft om toegang te mogen verschaffen.

04 Ondersteun het wachtwoordbeleid met het authenticatiemiddel.
Voor zover binnen de webapplicatie van wachtwoorden gebruik gemaakt wordt, worden de regels uit het beleid afgedwongen door geprogrammeerde controles.

toekennen van de rechten (autorisatie)

05 Wijs rechten toe op basis van het toegangsvoorzieningsbeleid.

06 Houd een actueel overzicht bij van accounts en de personen die daar gebruik van maken:
- » service-accounts;
- » beheeraccounts;
- » gebruikersaccount;
- » (web)applicatie-accounts.

07 Trek de rechten direct in en blokkeer direct het account wanneer een gebruiker geen recht op toegang meer heeft.
Dit gebeurt bijvoorbeeld door uitdiensttreding.

08 Voer periodiek een audit uit op de uitgedeelde autorisaties.

controleerbaar maken van het gebruik

09 Registreer het beheren en onderhouden van identiteiten en autorisatie onweerlegbaar.
Het toegangssysteem en ondersteunde systemen maken gebruik van mechanismen om activiteiten vast te leggen (loggen).

10 Registreer het verkrijgen van autorisatie en het gebruik van functionaliteit onweerlegbaar.

automatiseren van arbeidsintensieve taken

11 Ondersteun met het ingezette identiteits- en toegangsmanagementtool conform het toegangsvoorzieningsbeleid de complete levenscyclus van identiteiten en autorisaties:
- »
- » aanvragen;
- » toekennen;
- » wijzigen;
- » intrekken/schorsen/verwijderen;
- » conform voorgeschreven procedures.

35 Vaak ook aangeduid als CIAA (Confidentiality, Integrity, Availability en Auditability).

36 Zie voor afwegingen ten aanzien van de keuze van het authenticatiemiddel: https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_WEB.pdf

UITVOERINGSDOMEIN
» WEBAPPLICATIES

Doelstelling
De doelstelling van de laag “Webapplicaties” is om te waarborgen dat webapplicaties functioneren zoals is beoogd, ingericht zijn volgens specifieke beleidsuitgangspunten van de organisatie en voldoen aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid.

Inleiding
De beveiliging van een webapplicatie hoeft geen geïntegreerd onderdeel van de webapplicatie zelf te zijn, maar kan ook als losstaande component functioneren in de infrastructuur van de webapplicatie. Een firewall op applicatieniveau (Web Application Firewall (WAF)) is bijvoorbeeld een typisch losstaande component die geen geïntegreerd onderdeel van de webapplicatie is, maar wel beveiligingsservices biedt aan deze webapplicatie.

Veel van de bekendste kwetsbaarheden in webapplicaties, zoals cross-site scripting (XSS) en SQL-injectie, vinden hun oorsprong in fouten tijdens het ontwikkelen van software. Dit hoofdstuk besteedt aandacht aan de belangrijkste maatregelen op het gebied van softwareontwikkeling die de aanwezigheid van deze kwetsbaarheden grotendeels voorkomen en de kans op schade door de aanwezigheid van ernstige kwetsbaarheden in webapplicaties reduceren.

Risico’s
De ervaren of veronderstelde betrouwbaarheid van de webapplicatie wordt ondermijnd door derden, doordat zij in staat zijn de (inhoud van de) webapplicatie te manipuleren of verstoren. Oorzaken kunnen gelegen zijn in het niet (correct) of onvolledig toepassen van bekende richtlijnen en beveiligingstechnieken in zowel de ontwikkel- als de productiefase.

Beveiligingsrichtlijnen
Binnen de laag Webapplicaties worden onderstaande richtlijnen beschreven en per richtlijn worden conformiteitsindicatoren en de betreffende maatregelen uitgewerkt.
- Operationeel beleid voor webapplicatie (U/WA.01)
- Webapplicatiebeheer (U/WA.02)
- Webapplicatie-invoer U/WA.03)
- Webapplicatie-uitvoer (U/WA.04)
- Betrouwbaarheid van gegevens (U/WA.05)
- Webapplicatie-informatie (U/WA.06)
- Webapplicatie-integratie (U/WA.07)
- Webapplicatiesessie (U/WA.08)
- Webapplicatiearchitectuur (U/WA.09)

U/WA.01 Operationeel beleid voor webapplicaties

Omschrijving
Het operationeel beleid voor webapplicaties beschrijft de manier waarop de organisatie omgaat met het inrichten en beschikbaar stellen van webapplicaties. Het operationeel beleid is een concretere uitwerking van het bovenliggende beleid. Een solide operationeel beleid is daarom een randvoorwaarde voor een veilige inrichting van een webapplicatie-omgeving.

Beveiligingsrichtlijn U/WA.01

Operationeel beleid voor webapplicaties formuleren

Richtlijn (wie en wat)
Het operationeel beleid voor webapplicaties bevat richtlijnen en instructies en procedures met betrekking tot ontwikkeling, onderhoud en uitfasering van webapplicaties.

Doelstelling (waarom)
De ontwikkeling van de webapplicatie optimaal ondersteunen en de klant betrouwbare diensten bieden.

Risico
Geen eenduidige richting voor webapplicaties, waardoor de beveiliging van de webapplicatie los staat van zijn omgeving. Dit verhoogt de kans op beveiligingsincidenten.

Classificatie
Hoog

Richtlijn 2012
-

Maatregelen

richtlijnen
01 Stel richtlijnen op voor:
- ontwikkeling, onderhoud en uitfasering van webapplicaties;
- beveiliging van webapplicaties;
- verwerking van gegevens;
- koppelingen met onderliggende systemen;
- koppelingen met achterliggende systemen.

Gebruik bij de ontwikkeling van webapplicaties methodes voor Secure Software Development. [37]
Onderliggende systemen zijn alle elementen uit de hardware/software stack waarop de webapplicatie draait.
Achterliggende systemen zijn systemen die direct of indirect door de webapplicatie ontsloten of bereikt worden.

instructies en procedures
02 Stel instructies en procedures op voor:
- het werken met gescheiden ontwikkel-, test-, acceptatie- en productie-omgevingen (OTAP);
- contentmanagement.

Besteed aandacht aan het regelmatig evalueren en bijstellen van de richtlijnen. Indien deze instructies en procedures ruimte bieden om af te wijken van de richtlijn, dient hieraan de vereiste van ‘pas toe of leg uit’ gekoppeld te zijn.

Risico
Ongecontroleerde wijzigingen waarvan niet bekend is wie daarvoor verantwoordelijk is.

Classificatie
Midden

Richtlijn 2012
-

Maatregelen

procesmatig en procedureel
01 Voer beheerwerkzaamheden uit volgens afgesproken richtlijnen en procedures.
Hier gaat het er vooral om dat er zicht is op de vooraf bekende werkzaamheden en hoe deze worden uitgevoerd. Het reageren of en afhandelen van incidenten valt hier nadrukkelijk ook onder, hoewel voor het oplossen van beveiligingsincidenten natuurlijk geen standaardrecept te geven is.
02 Laat leidinggevenden en systeemeigenaren vooraf criteria vastleggen waaraan de operationele webapplicatie moet voldoen.
Bewaking van de criteria zal deels het werk van de webapplicatiebeheerders zijn, deels onder monitoring (C.07) vallen. De exacte verdeling verschilt per webapplicatie.

geautoriseerd
03 Voorkom dat hiertoe niet geautoriseerde gebruikers toegang krijgen tot beheerfuncties binnen de applicatie.

functieprofielen
04 Op basis van taken, verantwoordelijkheden en bevoegdheden zijn de verschillende beheerrollen geïdentificeerd.
Naast de diverse inhoudelijke taakgebieden is hierin expliciet aandacht voor ongewenste combinaties van bevoegdheden. Deze zijn in verschillende rollen ondergebracht (functiescheiding, zie ook U/TV.01/05 en U/TV.01/06).
05 Vul in de autorisatiematrix in:
- aan welke rollen welke bevoegdheden worden toegekend;
- hoe functiescheiding tot uitdrukking komt.

De functiescheiding geeft bijvoorbeeld aan dat één enkele beheerder niet in staat is – direct of indirect – volledige controle over alle functies te verwerven.
06 Richt een proces in voor het definiëren en onderhouden van de rollen.
Dit proces is afgestemd met de primaire bedrijfsprocessen.

U/WA.02 Webapplicatiebeheer

Omschrijving
Het (dagelijks) beheer van een webapplicatie draagt zorg voor het handhaven van de getroffen maatregelen. Daarmee levert het een belangrijke bijdrage aan de continue beleidscompliance van de webapplicatie en is dus een stabiliserende factor.

Beveiligingsrichtlijn U/WA.02

Webapplicatiebeheer inrichten

Richtlijn (wie en wat)
Het webapplicatiebeheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.

Doelstelling (waarom)
Effectief en veilig realiseren van de dienstverlening.

37 Vanuit opdrachtgeversoogpunt bijvoorbeeld: http://www.cip-overheid.nl/wp-content/uploads/2014/05/Grip-op-SSD-SIVA-Beveiligingseisen-v1-0.pdf
Vanuit ontwikkelaarsoogpunt bijvoorbeeld: https://www.securesoftwarefoundation.org/FrameworkSecureSoftware-Downloads.html

U/WA.03 Webapplicatie-invoer

Omschrijving

Ongecontroleerde (ongevalideerde) invoer van gebruikers is een belangrijke dreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookiewaarden, SQL-queries, et cetera, bestaat er een (grote) kans dat een kwaadwillende de webapplicatie compromitteert. Een gebrek aan invoervalidatie kan tot kwetsbaarheden zoals XSS, commando- en SQL-injectie leiden.

Als een webapplicatie wel invoervalidatie en filtering uitvoert, blijkt deze filtering vaak niet voldoende effectief om alle mogelijke aanvallen op de webapplicatie te blokkeren. Dit is voornamelijk het geval op het moment dat de webapplicatie gebruik maakt van blacklisting[38] om mogelijk gevaarlijke strings uit de invoer te verwijderen.

De belangrijkste vuistregel voor invoer in een webapplicatie is dat de applicatie geen enkele invoer mag vertrouwen en daarom moet valideren. Alle invoer moet daarom voor verwerking door de webapplicatie worden gevalideerd op juistheid, volledigheid en geldigheid. Daarbij dient de invoer minimaal gevalideerd te worden op waarden die buiten het geldige bereik vallen (grenswaarden), ongeldige tekens, ontbrekende of onvolledige gegevens, gegevens die niet aan het juiste formaat voldoen en inconsistentie van gegevens ten opzichte van andere gegevens binnen de invoer dan wel in andere gegevensbestanden. Invoervalidatie is de doorslaggevende voorwaarde voor betrouwbare gegevensverwerking en ongeldige invoer wordt door de webapplicatie geweigerd.

De richtlijnen voor invoerbehandeling zijn van toepassing voor *alle* invoer die van buiten de webapplicatie komt. Dus niet alleen (eind) gebruikers, maar ook externe systemen en applicaties.
Er geldt een aantal uitgangspunten met betrekking tot invoer bij het ontwikkelen van webapplicaties, deze zijn:
» De client (applicatie)[39] is niet te vertrouwen en dus de invoer die hier vandaan komt ook niet.
» De invoer wordt voor valideren eerst genormaliseerd.
» De invoer die niet aan één of meerdere controles voldoet wordt verwijderd of geweigerd.

In het ontwikkelproces van de webapplicatie zal de software expliciet op een correcte invulling van deze uitgangspunten onderzocht moeten worden. Dit vraagt om uitgebreide testen of gerichte codereviews.

38 http://en.wikipedia.org/wiki/Blacklist
39 http://nl.wikipedia.org/wiki/Client_%28applicatie%29

Beveiligingsrichtlijn U/WA.03

Webapplicatie-invoer beperken

Richtlijn (wie en wat)
De webapplicatie beperkt de mogelijkheid tot manipulatie door de invoer te normaliseren en te valideren, voordat deze invoer wordt verwerkt.

Doelstelling (waarom)
Voorkom (on)opzettelijke manipulatie van de webapplicatie, waardoor de vertrouwelijkheid, integriteit en/of beschikbaarheid van de webapplicatie aangetast worden.

Risico
Inzage, wijziging, verlies, of misbruik van gegevens door bijvoorbeeld manipulatie van de webapplicatielogica.

Classificatie
Hoog

Richtlijn 2012
B3-1, B3-3, B3-6, B3-7

Maatregelen

manipulatie

01 Valideer de invoer op de server.
Uitgebreide testen kunnen aannemelijk maken dat invoercontroles niet te omzeilen zijn. Gerichte codereviews leveren in de regel meer zekerheid op.
02 Verbied of beperk het gebruik van dynamische file includes.
Wanneer kwaadwillenden via malafide invoer willekeurige bestanden kunnen verwerken in de webapplicatie, bestaat de mogelijkheid dat willekeurige webapplicatiecode wordt uitgevoerd op de server. Hiermee is het bijvoorbeeld mogelijk om ongeautoriseerd de database op een server te benaderen.

normaliseren

03 Converteer alle invoer naar een veilig formaat, waarbij risicovolle tekens uit de invoer 'onschadelijk' worden gemaakt.

valideren

04 Weiger foute, ongeldige of verboden invoer.

Verdieping

Invoerconversie

Invoer moet eerst worden genormaliseerd voordat deze door de webapplicatie wordt gevalideerd. Hierdoor wordt voorkomen dat malafide verzoeken niet door de filtermechanismen van de webapplicatie worden herkend. Normalisatie staat ook wel bekend als anti-evasion[40] of canonicalization[41].
Voorbeelden van normalisatie zijn:
» Zet NULL tekens om naar spaties.
» Zet backslash '\' om naar forward slashes '/'.
» Zet mixed-case strings om naar lowercase strings.
» Codeer bijzondere tekens in uniforme codering (bijvoorbeeld 8-bit Unicode Transformation Format (UTF-8[42])).
» Normaliseer padverwijzingen als '/./' en '/../'.
» Verwijder overbodige spaties en regeleinden.
» Verwijder onnodige witruimtes.
» et cetera.
Converteer alle risicovolle tekens naar een veilig formaat.

De escape (\) voorafgaand aan een teken geeft aan dat het teken letterlijk moet worden geïnterpreteerd, \" wordt ". Een andere vorm van escaping is door gebruik te maken van de hexadecimale waarde van een teken, \x22 wordt ".[43] Dit levert echter niet de gewenste tekst op indien deze wordt gecompileerd met een ASCII[44]-incompatibele tekenset.[45]

Tekens uit de invoer die verwerkbaar en niet ongewenst zijn kunnen nog steeds risicovol zijn bij het gebruik hiervan binnen de programmalogica. Om problemen hiermee te voorkomen moeten deze tekens 'onschadelijk' worden gemaakt.

Risicovolle tekens kunnen onderdeel uitmaken van legitieme invoer. Neem onderstaand voorbeeld waarbij de plaatsnaam ('s-Gravenhage) tot een syntactische incorrecte query leidt

```
SELECT * FROM nieuws WHERE titel LIKE
'%'s-gravenhage%';
```

Door een escape voor de apostrof te plaatsen, beschouwt de database de apostrof als onderdeel van de invoer en niet als onderdeel van de query. Veel programmeertalen ondersteunen standaardfuncties voor het escapen van gevaarlijke tekens.

Soortgelijke conversies gelden voor bijvoorbeeld HTML, XML, et cetera.

Voer escaping uit op de invoer na het toepassen van whitelists en eventueel blacklists. Escaping is toegespitst op de programmaonderdelen waar invoer wordt verwerkt.

Invoervalidatie

De inhoud van een http-request wordt gevalideerd. De verdeling van validaties tussen de webserver en de webapplicatie is afhankelijk van de webserver waarmee de webapplicatie samenwerkt (zie ook U/PW.02).
De volgende onderdelen van een http-request worden minimaal gevalideerd voordat het request wordt verwerkt:
» URL's;
» Cookies;
» Http-headers;
» Query parameters (variabelen die de client via GET requests doorgeeft);
» Form parameters (variabelen die de client via POST requests doorgeeft);
» XML (hieronder vallen ook protocollen als Simple Object Access Protocol (SOAP), JavaScript Object Notation (JSON) en Representational State Transfer (REST));
» Bestanden.

De inhoud van alle onderdelen van een http-request wordt gevalideerd op basis van verwerkbare invoer.
De validatie wordt uitgevoerd op:
» Type (bijvoorbeeld string of integer).
» Lengte
» Formaat (bijvoorbeeld een reguliere expressie)
» Tekens (bijvoorbeeld alleen 'A-Z' en 'a-z')

De inhoud van http-requests kan ook op basis van expliciet bekende verwerkbare invoer (whitelist) gevalideerd worden, om te voorkomen dat malafide inhoud het mogelijk maakt om de applicatielogica te beïnvloeden.
Voldoet de invoer niet aan één of meerdere van bovenstaande controles, dan wordt de invoer geweigerd.

De inhoud van alle onderdelen van een http-request wordt gevalideerd op basis van ongewenste invoer.
Als het moeilijk is om op basis van de whitelisting alle mogelijke malafide invoer uit te filteren, dan kan de invoer aanvullend worden gevalideerd op malafide sleutelwoorden, tekens en patronen (blacklisting). Denk aan invoervelden waar de gebruiker vrije tekst kan invoeren.
De webapplicatie filtert de invoer op basis van:
» Malafide sleutelwoorden (bijvoorbeeld 'DROP' of ' rm ')

40 https://www.owasp.org/index.php/Virtual_Patching_Best_Practices#Anti-Evasion_Capabilitiesl
41 https://www.owasp.org/index.php/Canonicalization,_locale_and_Unicode of http://en.wikipedia.org/wiki/Canonicalization
42 http://tools.ietf.org/html/rfc3629
43 22 is de hexadecimale ASCII waarde van een dubbel aanhalingsteken.
44 http://en.wikipedia.org/wiki/ASCII
45 ASCII was tot december 2007 de meest gebruikte tekenset op het internet, daarna werd dit UTF-8.

» Malafide tekens (bijvoorbeeld ‘’’ of ‘”’)
» Malafide patronen (bijvoorbeeld ‘/**/’ of ‘..\..\’)

De filtering is toegespitst op de programmaonderdelen waarin de invoer wordt verwerkt. Bij het gebruik van invoer voor het samenstellen van een databasequery zijn andere filters vereist dan voor het samenstellen van een LDAP-query.

In het geval de invoer één of meerdere sleutelwoorden, tekens of patronen van de blacklist bevat, worden deze uit de invoer verwijderd alvorens deze invoer verder gebruikt wordt binnen de applicatielogica.
Voor andere protocollen dan http gelden soortgelijke controles. Denk ook aan interne consistentie, zoals geldige scheiders voor attachments in email (Simple Mail Transfer Protocol (SMTP)).

U/WA.04 Webapplicatie-uitvoer

Omschrijving

Naast het ontbreken van validatie van invoer ontbreekt het bij sommige webapplicaties ook aan de validatie van uitvoer. Als een webapplicatie onvoldoende controles uitvoert op de uitvoer die het terugstuurt naar de gebruiker, kan het gebeuren dat er zich onbedoelde of ongewenste inhoud in de uitvoer bevindt. Uitvoervalidatie voorkomt dat de webapplicatie ongewenste opdrachten geeft aan de client, bijvoorbeeld in het geval van XSS. Uitvoervalidatie kan worden geïmplementeerd door het coderen van alle dynamische inhoud van een webpagina. Veel webpagina’s bevatten naast statische ook dynamische informatie. Deze dynamische informatie kan bijvoorbeeld afkomstig zijn uit databases of externe bronnen maar kan ook gebaseerd zijn op invoer van de gebruiker. Zeker in het laatste geval bestaat de kans dat aanvallers misbruik maken van onvoldoende filtering of codering.

Beveiligingsrichtlijn U/WA.04

Webapplicatie-uitvoer beperken

Richtlijn (wie en wat)
De webapplicatie beperkt de uitvoer tot waarden die (veilig) verwerkt kunnen worden door deze te normaliseren.

Doelstelling (waarom)
Voorkom manipulatie van het systeem van andere gebruikers.

Risico
Via uitvoer van de webapplicatie de werking van of informatie op het systeem van anderen manipuleren.

Classificatie
Hoog

Richtlijn 2012
B3-4

Maatregelen

normaliseren

01 Converteer alle uitvoer naar een veilig formaat.
Uitgebreide testen kunnen aannemelijk maken dat uitvoer altijd genormaliseerd wordt. Gerichte codereviews leveren in de regel meer zekerheid op.
Het coderen van dynamische pagina-inhoud houdt in dat de webapplicatie mogelijk ‘gevaarlijke’ tekens codeert. Hoe de webapplicatie deze informatie moet coderen is afhankelijk van de plek in de pagina waar deze dynamische inhoud verschijnt. Zo moet men speciale tekens in HTML, JavaScript, HTML-attributen en URL’s allemaal op een andere wijze coderen. Neem bijvoorbeeld het ’groter dan’-teken (>). Afhankelijk van de plek waar dit teken wordt gebruikt, ziet de gecodeerde versie van dit teken er als volgt uit:
» *HTML-gecodeerd: <*
» *HTML-attribuut-gecodeerd: >*
» *JavaScript-gecodeerd: \x3E*
» *CSS-gecodeerd: \3E*
» *URL-gecodeerd: %3E*
Veel scripting- en programmeertalen hebben standaardbibliotheken waarmee deze codering kan worden uitgevoerd.

U/WA.05 Betrouwbaarheid van gegevens

Omschrijving

Gevoelige (vertrouwelijke) gegevens worden beschermd door gebruik te maken van cryptografische technieken in de database, bestanden en/of communicatie. Welke gegevens gevoelig of vertrouwelijk zijn, moet door de organisatie op basis van een risicoanalyse (B.03) en classificatieschema (B.01/03) worden vastgesteld.
Beschikbare cryptografische technieken zijn versleuteling en hashing en de daarvan afgeleide digitale handtekening.

Beveiligingsrichtlijn U/WA.05

Betrouwbaarheid van gegevens garanderen

Richtlijn (wie en wat)
De webapplicatie garandeert de betrouwbaarheid van informatie door toepassing van privacybevorderende en cryptografische technieken.

Doelstelling (waarom)
Gegevens in opslag en transport beschermen tegen ongeautoriseerde kennisname en manipulatie.

Risico
Onbevoegden nemen kennis van gegevens die zijn opgeslagen of worden gecommuniceerd en zijn mogelijk in staat deze te verminken.

Classificatie
Hoog

Richtlijn 2012
B5-2, B5-3, B5-4, B5-5

Maatregelen

privacybevorderende technieken

01 Pas, wanneer de webapplicatie persoonsgegevens verwerkt, de privacy-by-designprincipes toe.
Privacy by Design[46] kent 7 uitgangspunten:
1. *Proactief ipv reactief; Preventief ipv herstellend;*
2. *Privacy als standaard;*
3. *Privacy geïntegreerd in het ontwerp;*
4. *Volledige functionaliteit – Positive-Sum ipv zero-sum;*
5. *Veiligheid van begin tot eind – Bescherming tijdens de volledige levenscyclus;*
6. *Zichtbaarheid en transparantie – Houd het open;*
7. *Respect voor de privacy – laat de gebruiker centraal staan.*

02 Maak waar mogelijk gebruik van privacybevorderende technieken.
Denk hierbij bijvoorbeeld aan anonimisering of pseudonimisering (het gebruik van een pseudo-identiteit die niet rechtstreeks te koppelen is aan een natuurlijke persoon) van gegevens.

cryptografische technieken

03 Versleutel of hash gevoelige gegevens in databases en bestanden.
Het is niet altijd nodig een complete database te versleutelen. Soms kan volstaan worden met het versleutelen van enkele tabellen en zelfs kolommen uit tabellen.
Versleuteld opgeslagen gegevens kunnen tijdens communicatie versleuteld blijven, ook wanneer het communicatiekanaal zelf versleuteld is. Dit levert een extra beveiligingslaag.
Versleutel de gegevens altijd op applicatieniveau. Het versleutelen van een volledige harde schijf (full disk encryption) biedt geen bescherming tegen sommige dreigingen.

04 Gebruik cryptografisch sterke sessie-identificerende cookies.
Cookies zijn bijzondere gegevensbestanden. Ze worden onder meer gebruikt voor het onderhouden van sessies. Deze sessie-identificerende cookies dienen te zijn gegenereerd door een cryptografische nummergenerator. Sessie-cookies worden niet gegenereerd op basis van persoonlijke of gevoelige informatie zoals een gebruikersnummer of wachtwoord.

05 Versleutel communicatie.
Dit zal in de regel gebeuren met TLS (vroeger SSL).
Richtlijnen voor het veilig inzetten van TLS worden besproken in de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).[47] Deze algemene richtlijnen zijn onverkort van toepassing voor het beveiligen van verbindingen met webapplicaties.
Als de webapplicatie een (contact)formulier bevat of vertrouwelijke/gevoelige gegevens worden uitgewisseld, wordt de hele webapplicatie via https aangeboden. Bezoeken de meeste gebruikers de webapplicatie via een entreepagina in een andere webapplicatie (bijvoorbeeld via www.example.com naar secure.example.com), dan wordt ook deze webapplicatie via https aangeboden. Een bezoeker wordt bij elk bezoek doorverwezen van de http- naar de https-versie.
Naast deze algemene richtlijnen zijn de volgende specifieke aanwijzingen van toepassing bij het gebruiken van TLS voor http-verkeer, oftewel https:
» *Schakel, indien mogelijk, http-compressie uit. Http-compressie maakt een website vatbaar voor de BREACH-aanval.*
» *Ondersteun Http Strict Transport Security (HSTS). Als u HSTS ondersteunt, zal de browser voor elke terugkerende bezoeker vereisen dat de website opnieuw via https wordt aangeboden. Dit helpt man-in-the-middle-aanvallen te voorkomen.*
» *Heeft uw website meerdere domeinnamen (bijvoorbeeld met en zonder ‘www.’), ondersteun dan https op elk van deze domeinnamen. Verwijs een bezoeker van de site onder een domeinnaam direct door naar de https-versie van de site onder die domeinnaam. Verwijst u domeinnamen onderling ook door (bijvoorbeeld de versie zonder ‘www.’ naar de versie met ‘www.’), doe die doorverwijzing dan tussen de https-versies van de site onder die domeinnamen. Verwijs geen domeinnamen naar elkaar door via http. Zorg dat elk van de domeinnamen voorkomt als SubjectAlternativeName in het TLS-certificaat. Schakel HSTS in op elk van de domeinnamen.*
» *Vermijd het vermengen van inhoud van de webapplicatie die via http en via https wordt aangeboden (mixed content). Dat voorkomt dat een aanvaller de vertrouwelijke delen van uw webapplicatie alsnog weet te achterhalen of te manipuleren.*
» *Schakel, indien mogelijk, renegotiation uit. Renegotiation is slechts nodig in twee gevallen. Ten eerste is het van waarde voor webapplicaties die grote hoeveelheden data versturen van of naar de gebruiker (in de orde van gigabytes). Ten tweede wordt het gebruikt bij webapplicaties die verbindingen beveiligen met clientcertificaten.*

06 Onderteken transacties met een digitale handtekening.
Digitale handtekeningen beschermen de onweerlegbaarheid van (de herkomst van) gegevens.

46 Zie: https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-dutch.pdf

U/WA.06 Webapplicatie-informatie

Omschrijving

Webapplicaties maken soms gebruik van client-side scripts zoals JavaScript. Commentaarregels in scripts gedurende de ontwikkel- en testfase zijn normaal, maar in een productieomgeving ongewenst omdat de commentaarregels onnodig informatie vrijgeven waarvan een kwaadwillende misbruik kan maken.
Tijdens deployment van een webapplicatie kan alle code die naar clients wordt gestuurd, ontdaan worden van commentaar. Als alternatief zijn application-level firewalls in staat om commentaarregels uit HTML- en scriptcode te verwijderen en zodoende 'gefilterde' antwoorden terug te geven aan de client.

Beveiligingsrichtlijn U/WA.06

Webapplicatie-informatie beperken

Richtlijn (wie en wat)
De webapplicatie beperkt de informatie in de uitvoer tot de informatie die voor het functioneren van belang is.

Doelstelling (waarom)
Beperk het (onnodig) vrijgeven van informatie tot een minimum.

Risico
Kennis nemen van de technologieën van de webapplicatie, om deze vervolgens te gebruiken om de webapplicatie aan te vallen.

Classificatie
Hoog

Richtlijn 2012
B3-11

Maatregelen

Uitvoer

01 Verwijder commentaarregels uit de scripts (code).
02 Verwijder of pseudonimiseer verwijzingen naar interne bestands- of systeemnamen.
De webapplicatie geeft geen informatie over de interne werking of configuratie van de webapplicatie zelf of een van de systemen waarmee de webapplicatie samenwerkt. Eenvoudige testen volstaan om aannemelijk te maken dat uitvoer geen informatie over interne werking of configuratie prijsgeeft.

U/WA.07 Webapplicatie-integratie

Omschrijving

Een webapplicatie integreert met onder- en achterliggende systemen (bijvoorbeeld het onderliggende besturingssysteem en een achterliggende database) door gebruik te maken van commando's en queries.

Grofweg bestaan er twee methoden om vanuit een webapplicatie een query of commando te genereren, die gebruik maakt van invoer van gebruikers: via dynamische strings of via parameters.
Bij dynamische strings plakt de webapplicatie een vaste string (bijvoorbeeld de start van een SELECT-statement) aan een variabele (bijvoorbeeld de inhoud van de WHERE-clause). Via deze methode bestaat de mogelijkheid dat de door een gebruiker geleverde invoer de query op ongecontroleerde wijze verandert. Hierdoor kunnen gegevens bijvoorbeeld vernietigd worden of ongefilterd bij de gebruiker komen, waardoor de vertrouwelijkheid geschonden wordt.

Bij het gebruik van geparametriseerde queries is de syntax van de query statisch en wordt invoer alleen gebruikt om vooraf gedefinieerde variabelen te vullen. Door te voorkomen dat de syntax van de query wijzigt, voorkomt de webapplicatie SQL-injectieaanvallen.
Geparametriseerde queries zijn ook efficiënter: doordat ze voorgedefinieerd zijn, gebruiken ze bekende tabelstructuren optimaal. Toch geven ze de gebruiker geen volledige vrijheid. Op dezelfde manier voorkomen statisch geprogrammeerde commando's ervoor dat de gebruiker geen mogelijkheid heeft de aard van de commando's te beïnvloeden.

Beveiligingsrichtlijn U/WA.07

Webapplicatie-integratie communiceren

Richtlijn (wie en wat)
De webapplicatie communiceert alleen met onder- en achterliggende systemen op basis van statisch geconfigureerde (geparametriseerde) queries en commando's en uitsluitend ten behoeve van de noodzakelijke functionaliteit.

Doelstelling (waarom)
Kwetsbaarheid van de onder- en achterliggende systemen voorkomen en de integriteit en vertrouwelijkheid garanderen.

47 Zie https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

Risico
Via manipulatie (bijvoorbeeld commando- of SQL-injectie) kennis nemen van de inhoud van de onder- en achterliggende systemen of deze kunnen manipuleren.

Classificatie
Hoog

Richtlijn 2012
B3-5

Maatregelen

commando's en queries

01 Bouw commando- en queryteksten op met uitsluitend in de code reeds aanwezige vaste tekstfragmenten.
De leverancier van de software geeft hierover een verklaring van een onafhankelijke derde af of stelt de broncode beschikbaar voor review.
02 Geef gebruikersinvoer die gebruikt moet worden in commando's en queries op een zodanige manier door, dat de beoogde werking niet wordt gewijzigd.
Voor zover er sprake is van gebruikersinvoer in commando's en queries wordt deze als parameters doorgegeven. Het doel hiervan is te voorkomen dat de gebruiker zelf kan bepalen welke commando's of queries worden uitgevoerd.

noodzakelijke functionaliteit

03 Houd van elke webapplicatie bij welke functionaliteit van backendsystemen nodig is.
De koppeling met backend systemen is gedocumenteerd, inclusief de aard van de koppeling en de daarvoor noodzakelijke (gebruikers) rechten. Functies die niet nodig zijn voor de functionaliteit van een (web)applicatie vormen een onnodig risico en dienen daarom achterwege te blijven.
Denk hierbij aan File Transfer Protocol (FTP), Telnet, Post Office Protocol (POP)/SMTP (postbusfunctie), et cetera.
04 Verbied directe data-toegang tot backendsystemen, tenzij andere opties niet voorhanden zijn.

U/WA.08 Webapplicatiesessie

Omschrijving

De webapplicatie biedt expliciete functionaliteit om de sessie te verbreken:
» Daar waar de gebruiker en/of beheerder kan inloggen op de webapplicatie is expliciete functionaliteit aanwezig om uit te loggen (het verbreken van de sessie). Tijdens het uitloggen van een gebruiker wordt de sessie onklaar gemaakt en kan een kwaadwillende met eventuele onderschepte sessiegegevens geen verbinding meer opzetten.
» Bij het aanmelden (effectief een wijziging van autorisatieniveau van de gebruiker) wordt de bestaande sessie ongeldig en een nieuwe sessie gestart. Zo kan een vooraf ingestelde sessie niet misbruikt worden na wijziging van autorisatieniveau.
» Verder is het van belang aandacht te besteden aan de idle time-out en de verbindingstijd per sessie, zodat gebruikers automatisch worden uitgelogd op het moment dat zij geen gebruik meer (lijken te) maken van de webapplicatie. Hoe lang mag een gebruiker verbonden (geauthenticeerd) blijven zonder zichtbare activiteit? Er dient een limiet gesteld te worden aan de maximale tijd dat een gebruiker inactief is.
» Ook de beperking van de sessieduur (verbindingstijd) biedt aanvullende beveiliging voor webapplicaties. Door de sessieduur te beperken, neemt de kans op ongeautoriseerde toegang af.
» Op deze manier wordt het risico verminderd dat een kwaadwillende een webapplicatie ongeautoriseerd kan benaderen, doordat een vorige gebruiker vergeten is uit te loggen.

De beleidsmatige keuzes over maximale sessieduur et cetera komen uit B.02/09. Zie ook U/WA.05/04 en U/PW.03/03 voor maatregelen om sessie-identifiers in cookies tegen diefstal te beschermen.

Beveiligingsrichtlijn U/WA.08

Webapplicatiesessie beëindigen

Richtlijn (wie en wat)
De (gebruikers)sessie die ontstaat na het succesvol aanmelden van een gebruiker, kent een beperkte levensduur en de gebruiker kan deze sessie zelf beëindigen.

Doelstelling (waarom)
Voorkomen dat derden de controle over een sessie kunnen krijgen.

Risico
Kennisname of wijziging van gegevens door onbevoegde derden.

Classificatie
Hoog

Richtlijn 2012
B4-2

Maatregelen

aanmelden

01 Maak bij het aanmelden een nieuwe sessie aan en verbreek een eventueel al bestaande sessie van die gebruiker. Maak de oude sessie-identifier ongeldig.

levensduur

02 Beëindig de sessie na een vooraf vastgestelde en geconfigu-

reerde tijdspanne van inactiviteit van de gebruiker (idle-time).
Voer een configuratie van de webapplicatie uit waaruit blijkt dat beperking van de idle-time-out en sessieduur is toegepast.
De webapplicatierserver bewaakt zelf de levensduur van een sessie en mag zich hiervoor niet verlaten op de webbrowser.

03 Beëindig de sessie na een vooraf vastgestelde en geconfigureerde sessietijd (session-time).

zelf beëindigen

04 Bied de gebruiker de mogelijkheid de sessie op eigen initiatief te beëindigen (uitloggen).
Dit geldt zowel voor de gebruiker als voor beheerders van de webapplicatie.

05 De sessie is na beëindiging niet langer geautoriseerd binnen de webapplicatie.
Alle op de webserver geregistreerde informatie over de actieve sessie wordt verwijderd, cookies en dergelijke komen te vervallen.
Na beëindiging van een sessie zijn verdere handelingen binnen die sessie niet mogelijk.

U/WA.09 Webapplicatiearchitectuur

Omschrijving

De architectuur van webapplicaties beschrijft de functionele en beveiligingssamenhang en legt de relatie met (de architectuur van) het algemene ICT-landschap. Vanuit een eenduidig gemeenschappelijk beeld worden webapplicaties conform deze architectuur gerealiseerd. Hiervoor worden de richtlijnen, instructies en procedures van U/WA.01/02 toegepast. Op deze manier wordt zeker gesteld dat iedere webapplicatie aan de vereiste functionele en beveiligingsdoelen bijdraagt.

Beveiligingsrichtlijn U/WA.09

Webapplicatiearchitectuur beschikken

Richtlijn (wie en wat)
Voor het implementeren, integreren en onderhouden van webapplicaties zijn architectuur- en beveiligingsvoorschriften beschikbaar.

Doelstelling (waarom)
Een webapplicatie-infrastructuur bieden die een betrouwbare verwerking garandeert.

Risico
Onvoldoende beheersing van de webapplicatie-omgeving, waardoor gebruikers het vertrouwen in de dienstverlening verliezen en mogelijkheden voor misbruik ontstaan.

Classificatie
Hoog

Richtlijn 2012
-

Maatregelen

architectuurvoorschriften

01 Stel architectuurvoorschriften op die actief worden onderhouden.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08).
Het document:
- *heeft een eigenaar;*
- *is voorzien van een datum en versienummer;*
- *bevat een documenthistorie (wat is wanneer en door wie aangepast);*
- *is actueel, juist en volledig;*
- *is door het juiste (organisatorische) niveau vastgesteld/geaccordeerd.*

De ICT-afdeling en de ICT-securitymanager zijn in ieder geval deel van 'het juiste (organisatorische) niveau'.

beveiligingsvoorschriften

02 Scheid vertrouwde en niet-vertrouwde domeinen: toepassen van scheidingen in netwerken (DMZ).
Zie U/NW.03.

03 Pas het principe van 'least privilege' toe op hoe de webapplicatie van onderliggende servers gebruikmaakt.
Hiervoor moet expliciet bekend zijn welke rechten een webapplicatie minimaal moet hebben om volledig functioneel te zijn. Alleen deze rechten zijn toegewezen aan het account waaronder de webapplicatie draait. Wanneer een webapplicatie tijdens het opstarten tijdelijk hogere rechten nodig heeft (bijvoorbeeld om een TCP-poort aan te maken), dan dient het zo snel mogelijk daarna afstand te doen van deze hogere rechten.

04 Configureer webapplicaties en onderliggende servers zodanig dat ook security-gerelateerde events worden vastgelegd.
Hieronder vallen in ieder geval alle activiteiten die geblokkeerd werden omdat de rechten van de gebruiker of applicatie ontoereikend waren om de activiteiten uit te voeren.

UITVOERINGSDOMEIN
» PLATFORMEN EN WEBSERVERS

Doelstelling

De doelstelling van de laag “Platformen en webservers” is te waarborgen dat de platformen (besturingssystemen) en webservers ingericht zijn volgens specifieke beleidsuitgangspunten van de organisatie en voldoen aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid.

Inleiding

Deze paragraaf gaat in op het ontwerpen, inrichten/configureren, beschikbaar stellen en handhaven van de beveiliging voor platformen en webservers zodat deze systemen beter bestand zijn tegen aanvallen van kwaadwillenden.

Het platform waarop een webapplicatie draait, is in de regel een besturingssysteem als Windows of Linux-/UNIX-varianten. Ditzelfde geldt voor applicaties waarvan een webapplicatie gebruikmaakt zoals applicatieservers en databaseservers.

Het uitgangspunt bij de beveiliging van platformen en webservers is het hardenen van de ICT-omgeving (zie ook richtlijn B.01/05). Hardening houdt in dat je het systeem zo inricht, dat dit systeem beter bestand is tegen aanvallen van kwaadwillenden. De technische stappen die nodig zijn om een systeem te hardenen verschillen per type systeem. De logische stappen verschillen echter veel minder. De richtlijnen in dit hoofdstuk zijn dan ook generiek van aard. Specifieke maatregelen voor de verschillende besturingssystemen en webservers worden aangeboden door de Security Benchmarks division[48] (voorheen het Center for Internet Security).

De Security Benchmarks division helpt organisaties hun informatiebeveiliging te verbeteren door het verminderen van het risico als gevolg van ontoereikende technische beveiligingsmaatregelen. Om dit te bereiken faciliteert de Security Benchmarks division de op consensus gebaseerde ontwikkeling van (1) best practices (maatregelen) voor beveiligingsconfiguratie, (2) tools voor het meten van de status van informatiebeveiliging, en (3) hulpmiddelen om weloverwogen investeringsbeslissingen op het gebied van informatiebeveiliging te kunnen nemen. De hulpmiddelen (benchmarks) die worden aangeboden door de Security Benchmarks division worden (vaak) gezien als de de facto standaard voor beveiligingsconfiguratie maatregelen en worden gebruikt bij het uitvoeren van audits. De door de CIS ontwikkelde benchmarks worden toegepast door zowel de overheid, het bedrijfsleven, de industrie als de academische wereld.[49]

Risico’s

Door gebruik te maken van kwetsbaarheden in platformen en webservers, zijn onbevoegden in staat kennis te nemen van bedrijfs- of privacygevoelige gegevens, de gegevens te manipuleren of de beschikbaarheid van de webapplicatie negatief te beïnvloeden. Bovendien bestaat het risico dat zij in staat zijn de sporen van dit gebruik te wissen of verhullen, of dit uit andermans naam doen.

Beveiligingsrichtlijnen

Binnen de laag Platformen en webservers worden onderstaande richtlijnen beschreven en per richtlijn worden conformiteitsindicatoren en maatregelen uitgewerkt.

- Operationeel beleid voor platformen en webservers (U/PW.01)
- Webprotocollen (U/PW.02)
- Webserver (U/PW.03)
- Isolatie van processen/bestanden (U/PW.04)
- Toegang tot beheermechanismen (U/PW.05)
- Platform-netwerkkoppeling (U/PW.06)
- Hardening van platformen (U/PW.07)
- Platform- en webserverarchitectuur (U/PW.08)

48 https://benchmarks.cisecurity.org/index.cfm
49 De benchmarks zijn te downloaden via https://benchmarks.cisecurity.org/downloads/multiform/

U/PW.01 Operationeel beleid voor platformen en webservers

Omschrijving

Het operationeel beleid voor platformen en webservers beschrijft de manier waarop de organisatie omgaat met het inrichten en beschikbaar stellen van platformen en webservers. Configuratie van deze objecten vormt de basis voor informatiebeveiliging. Het operationeel beleid is een concretere uitwerking van het bovenliggende beleid, bijvoorbeeld zoals in B.01. Een solide operationeel beleid is daarom een randvoorwaarde voor een veilige inrichting van een webapplicatieomgeving.

Platformen en webservers sluiten bij voorkeur aan op centrale toegangsvoorzieningen (zie U/TV) voor identificatie, authenticatie en autorisatie. Dit is echter in lang niet alle gevallen mogelijk. In die situaties zal op platform- en webserverniveau invulling gegeven moeten worden aan de vereisten voor toegangsvoorzieningen.

Het is cruciaal dat de authenticatie tot platformen en webservers zeer strikt wordt ingeregeld. Afhankelijk van het type besturingssysteem kunnen hier verschillende maatregelen voor worden getroffen.

De volgende aanbevelingen zijn van toepassing op vrijwel alle besturingssystemen:

- Zorg dat het systeem niet toegankelijk is op basis van anonieme generieke accounts zoals een gastaccount.
- Beperk de toegang op afstand tot accounts met gelimiteerde rechten. Zorg dat de toegang op basis van root- of beheerderaccounts niet mogelijk is. Beheerders moeten op afstand inloggen met een gelimiteerd beheeraccount en vervolgens lokaal, daar waar nodig, gebruik maken van verhoogde rechten via mechanismen als sudo (Linux) en RunAs (Windows).
- Overweeg de invoering van sterke authenticatiemechanismen voor de toegang tot systemen. Deze mechanismen kenmerken zich door het gebruik van ten minste twee factoren voor authenticatie.
- Beperk het aantal groepen waartoe een gebruiker behoort (groepslidmaatschappen). Machtigingen en rechten die aan een groep worden toegekend, gelden ook voor de leden van die groep.
- Implementeer een strikt wachtwoordbeleid. In een wachtwoordbeleid worden de minimale wachtwoordlengte, lengte van de wachtwoordhistorie, complexiteit van het wachtwoord en account lock-outs vastgelegd.
- Voorkom dat wachtwoorden in leesbare vorm worden opgeslagen door middel van het gebruik van hashing (in combinatie met salts).
- Verwijder of blokkeer ongebruikte accounts en standaard aanwezige accounts.
- Hernoem ‘bekende’ accounts die niet verwijderd kunnen worden (zoals ‘administrator’) of maak gebruik van sterke wachtwoorden.
- Wijzig het standaardwachtwoord van een systeem alvorens het in gebruik te nemen.

Voor webservers gelden soortgelijke aanbevelingen.

Beveiligingsrichtlijn U/PW.01

Operationeel beleid voor platformen en webservers formuleren

Richtlijn (wie en wat)
Het operationeel beleid voor platformen en webservers formuleert richtlijnen, instructies en procedures voor inrichting en beheer van platformen en webservers.

Doelstelling (waarom)
Betrouwbare ondersteuning van de programmatuur die op het platform draait.

Risico
De beoogde werking van het platform wordt aangetast, bijvoorbeeld doordat de beveiliging wordt doorbroken.

Classificatie
Hoog

Richtlijn 2012
B2-2

Maatregelen

richtlijnen

01 Stel voorschriften (baselines) op voor de veilige configuratie van platformen en webservers.
De baseline dient aandacht te geven aan de compartimentering van applicatiedata, software en configuratiebestanden. Deze dienen van elkaar gescheiden te zijn.
Maak gebruik van bestaande richtlijnen van leveranciers en erkende kennisinstituten als NIST, SANS, et cetera.
02 Besteed in de voorschriften expliciet aandacht aan hardening van platformen en webservers.
Dit is een inhoudelijke eis aan de richtlijn, gericht op het (on) beschikbaar maken van functionaliteiten.
03 Besteed in de voorschriften expliciet aandacht aan de configuratie en het gebruik van accounts.

instructies en procedures

04 Stel instructies en procedures op voor:
- het creëren en onderhouden van voorschriften voor de veilige configuratie van platformen en webservers;
- het toepassen van voorschriften voor de veilige configuratie van platformen en webservers.

Besteed aandacht aan het regelmatig evalueren en bijstellen van de richtlijnen. Zie de inleiding voor een aantal concrete aanbevelingen.
Indien deze instructies en procedures ruimte bieden om af te wijken van de richtlijn, dient hieraan de vereiste van ‘comply or explain’ gekoppeld te zijn.

U/PW.02 Webprotocollen

Omschrijving

De webserver dient de communicatie met de client zodanig af te schermen en beschermen, dat het voor derden niet mogelijk is:
» kennis te nemen van hetgeen gecommuniceerd wordt;
» zich voor te doen als de betreffende client.
Voorbeelden van mogelijk misbruik zijn:
» diefstal - van cookies, bijvoorbeeld via XSS;
» fraude - transactie onder een valse identiteit aanbieden.
Hiervoor moet een kwaadwillende derde in staat zijn tot:
» afluisteren van de communicatie;
» misbruiken van http-methoden die niet noodzakelijk zijn voor de webapplicatie;
manipuleren van cookies, bijvoorbeeld via JavaScript.

Http ondersteunt verschillende methoden (zie RFC 7540 voor http/2). In de praktijk gebruikt een webapplicatie vaak alleen de methoden GET en POST. Voor veel scripts en objecten op een webserver geldt zelfs dat alleen de GET-methode nodig is.

Het lekken van informatie moet zoveel mogelijk worden voorkomen. Via http-headers kan onnodig informatie worden vrijgegeven. Het gebruik dient dus waar mogelijk te worden beperkt.

Door het stelen van cookies (diefstal) of via Cross-Site Request Forgery (CSRF) kunnen kwaadwillenden ongewild transacties uitvoeren uit naam van een gevalideerde gebruiker (fraude). Voor CSRF kan dit via links op malafide websites of in e-mails. De kans op misbruik van gestolen cookies kan de webapplicatie minimaliseren door de inhoud van een cookie te koppelen aan het ip-adres waaraan deze inhoud is toegekend. De kans op CSRF kan de webapplicatie verder minimaliseren door gebruik te maken van dynamische tokens en het uitvoeren van een controle op de Origin-[50] of Referer[51]-header.

Op het moment dat zich een probleem voordoet binnen een webapplicatie zal de webserver veelal de http-statuscode[52] 500 Internal Server Error terugsturen. Dit wijst de client op een exceptie (foutsituatie). De mogelijkheid bestaat dat de webserver bij deze exceptie gevoelige informatie over de webapplicatie openbaart (databasenamen, gebruikersnamen, bestandsnamen, interne ip-adressen, et cetera). Hiertegen moeten maatregelen worden getroffen.

Beveiligingsrichtlijn U/PW.02

Webprotocollen garanderen

Richtlijn (wie en wat)
De webserver garandeert specifieke kenmerken van de inhoud van de protocollen.

Doelstelling (waarom)
Voorkom inzage, wijziging of verlies van gegevens door manipulatie van de logica van de webserver of webapplicatie.

Risico
De werking van de webserver of webapplicatie wordt gemanipuleerd, waardoor deze onder controle komt van een aanvaller.

Classificatie
Hoog

Richtlijn 2012
B3-2, B3-8, B3-9, B3-10, B3-12

Maatregelen

specifieke kenmerken

01 Behandel alleen http-requests waarvan de gegevens een correct type, lengte, formaat, tekens en patronen hebben.
Dit zal in de regel een producteigenschap van de betreffende webserver zijn. De leverancier van de software geeft hierover een verklaring van een onafhankelijke derde af of stelt de broncode beschikbaar voor review. Op de veelgebruikte Apache HTTP Server kan modSecurity handvatten bieden.
De verdeling van controles op de specifieke kenmerken is afhankelijk van de webserver en de webapplicatie(s) waarmee de deze samenwerkt. Zie ook U/WA.03.

02 Behandel alleen http-requests van initiators met een correcte authenticatie en autorisatie.
Valideer de volgende scenario's:
» *Het is niet mogelijk om een cookie te gebruiken vanaf een ip-adres anders dan het ip-adres aan wie het cookie verstrekt is.*
» *Het is niet mogelijk om transacties voor gevalideerde gebruikers uit te voeren vanaf een andere website dan de website waarop de gebruiker is gevalideerd.*
De leverancier van de software geeft hierover een verklaring van een onafhankelijke derde af of stelt de broncode beschikbaar voor review.

50 https://wiki.mozilla.org/Security/Origin
51 http://en.wikipedia.org/wiki/HTTP_referer
52 http://nl.wikipedia.org/wiki/Lijst_van_HTTP-statuscodes

protocollen

03 Sta alleen de voor de ondersteunde webapplicaties benodigde http-requestmethoden (GET, POST, etc.) toe en blokkeer de overige niet noodzakelijke http-requestmethoden.
In de ontwerp- of configuratiedocumentatie is vastgelegd:
» *welke http-methoden voor het functioneren van http van belang zijn;*
» *welke http-headers voor het functioneren van http van belang zijn;*
» *welke http-requestmethoden (GET, POST, etc.) voor de ondersteunde webapplicaties benodigd zijn;*
» *welke informatie in de http-headers voor het functioneren van belang zijn;*
» *welke standaard foutmelding(en) worden getoond/verstuurd;*
» *op welke wijze bovenstaande is gerealiseerd, denk hierbij aan de configuratie van de webserver en, indien van toepassing, de application-level firewall;*
» *eventuele noodzakelijke afwijkingen van bovenstaande, omdat de webapplicatie anders niet kan functioneren zijn onderbouwd.*
Methoden anders dan GET en POST zijn vrijwel nooit nodig binnen traditionele webapplicaties en vormen alleen een extra beveiligingsrisico (misbruik). Voor Web 2.0 zijn soms wel aanvullende methoden nodig. Het is in alle gevallen aan te raden om niet-benodigde http-methoden via configuratie van de webserver of via de application-level firewall te blokkeren.

04 Verstuur alleen http-headers die voor het functioneren van http van belang zijn.
Alleen headers die voor het functioneren van http en de webapplicatie van belang zijn, worden opgenomen in de http-responses aan gebruikers. Alle overige http-headers kan de applicatie in de regel zonder gevolgen uit een http-response verwijderen.

05 Toon in http-headers alleen de hoogst noodzakelijke informatie die voor het functioneren van belang is.
Informatie in standaard http-headers (bijvoorbeeld type webserver of versienummer) kan misbruikt worden door een kwaadwillende. Voorbeeld: het is voor een client niet van belang om te weten welk type webserver antwoord heeft gegeven op het http-request. De Server-header kan dan ook uit het antwoord worden verwijderd of worden voorzien van een nietszeggende inhoud.

06 Bij het optreden van een fout wordt de informatie in een http-response tot een minimum beperkt. Een eventuele foutmelding zegt wel dat er iets is fout gegaan, maar niet hoe het is fout gegaan.
Webservers bieden functionaliteit om standaardmeldingen te laten genereren aan de hand van specifieke statuscodes. Een applicatiefirewall zou een dergelijke statuscode kunnen detecteren en een standaardfoutmelding (bijvoorbeeld 'Er heeft zich een onbekende fout voorgedaan.') terugsturen naar de gebruiker en het gedetailleerde antwoord van de webserver negeren. Foutmeldingen geven geen informatie over de werking van de applicatie.

U/PW.03 Webserver

Omschrijving

Via een zogenaamde 'directory listing' kan een gebruiker via internet de inhoud van een directory bekijken. Het opvragen van een 'directory listing' via internet komt overeen met het lokaal uitvoeren van een dir-commando onder Windows of een ls-commando onder UNIX/Linux. Zodra een webserver de mogelijkheid biedt om 'directory listings' uit te voeren, bestaat de mogelijkheid dat een kwaadwillende de inhoud van 'vertrouwelijke' directories raadpleegt (zoals de '/etc/'-directory onder UNIX/Linux-systemen). De toegang tot bestanden in directories moet altijd verlopen via de webapplicatie: de webapplicatie bepaalt absolute paden voor bestanden die de gebruiker rechtstreeks mag benaderen (bijvoorbeeld afbeeldingen) en fungeert als medium voor bestanden die de gebruiker niet rechtstreeks mag benaderen (bijvoorbeeld gegevensbestanden).

Vaak vertrouwen webapplicaties op client cookies om sessiegegevens, inclusief gebruikersauthenticatie- en –autorisatiegegevens, te bewaren. Het is mogelijk om XSS-aanvallen uit te voeren als kwaadwillenden toegang hebben tot deze gevoelige gegevens die in client-side cookies zijn opgeslagen. Via de attributen HttpOnly en Secure wordt de beveiliging van client cookies verhoogd. HttpOnly zorgt dat de cookie uitsluitend via http-verbindingen gebruikt kan worden en niet via bijvoorbeeld JavaScript (manipulatie). Secure limiteert de communicatie van cookies tot beveiligde verbindingen (afluisteren) en voorkomt dat de cookie-inhoud voor onbevoegden zichtbaar wordt.

Bij een clickjacking-aanval wordt een webpagina in een frame op een andere website geopend waar gebruikers andere inhoud zien en daar interactie mee aangaan. De aanvaller kan deze interactie ongemerkt laten uitvoeren op de webpagina van het doelwit, misbruik makend van de sessie van de gebruiker. De webserver kan met behulp van de http-headers X-Frame-Options en Content-Security-Policy: frame-ancestors het laden van de webpagina's in frames beperken.

Beveiligingsrichtlijn U/PW.03

Webserver inrichten

Richtlijn (wie en wat)
De webserver is ingericht volgens een configuratie-baseline.

Doelstelling (waarom)
Ongewenste vrijgave van informatie tot een minimum beperken, met name waar het gaat om informatie die inzicht geeft in de opbouw van de beveiliging.

Risico
De werking van de webserver of webapplicatie wordt gemanipu-

leerd, waardoor deze onder controle komt van een aanvaller.

Classificatie
Hoog

Richtlijn 2012
B3-13, B3-16

Maatregelen

configuratie-baseline

01 Beschrijf de parametrisering van de webserver in een configuratiedocument.
Maak gebruik van bestaande richtlijnen van leveranciers en erkende kennisinstituten als NIST, SANS, et cetera.

02 Verbied het opvragen van de inhoud van het filesysteem van de server. Ondersteun geen directory-listings.
Staat directory listing aan, dan kan de websitebezoeker de inhoud van bepaalde mappen zien. In de regel zal dit via instructies in de configuratie van de webserver gerealiseerd worden. Deze worden bij implementatie ingevuld, bij een audit gecontroleerd.

03 Stel voor alle cookies de flags 'secure' en 'HttpOnly' in.
In de regel zal dit via instructies in de configuratie van de webserver gerealiseerd worden. Deze worden bij implementatie ingevuld, bij een audit gecontroleerd.

04 Verstuur bij alle http-responses de http-headers 'Content-Security-Policy: frame-ancestors' en (tijdelijk) 'X-Frame-Options'.
'Content-Security-Policy' wordt op het moment van schrijven nog niet door alle browsers ondersteund. Zolang dit nog het geval is kan gelijktijdig 'X-Frame-Options' gebruikt worden. Deze header kan worden ingesteld op 'DENY' (niet in frame laden), 'ALLOW-FROM' (toestaan vanaf een bepaalde andere website) of 'SAMEORIGIN' (alleen binnen een pagina van dezelfde herkomst).

U/PW.04
Isolatie van processen/bestanden

Omschrijving

Isolatie is een manier om een proces (draaiende applicatie) af te scheiden van de rest van een besturingssysteem en andere processen. Hiermee wordt wederzijdse beïnvloeding voorkomen.

Een bekende implementatie van isolatie is chroot. Het commando chroot (change root) wijzigt de rootdirectory voor een proces. Door een proces via chroot te laten werken, heeft het proces geen toegang meer tot bestanden die zich buiten deze root-directory bevinden. Dit mechanisme kan bijvoorbeeld worden ingezet om een Apache-server geïsoleerd te laten draaien.

Naast het afschermen van directories via chroot bestaan er ook mechanismen om andere delen van het besturingssysteem af te schermen; voorbeelden zijn het beperken van I/O-rates, het beperken van het toegestane hoeveelheid geheugen en het beperken van de toegestane hoeveelheid CPU-cycles.

Virtualisatie is een vorm van afscherming van processen door volledig autonome besturingssystemen naast elkaar te laten functioneren.

Jailing (***sandboxing***) is een mechanisme dat het concept van chroot verder doorvoert tot (vrijwel) alle aspecten van een besturingssysteem. Jailing bestaat voornamelijk op het Linux- en UNIX-platform, maar kan ook in andere omgevingen gerealiseerd worden.

Beveiligingsrichtlijn U/PW.04

Isolatie van processen/bestanden beschermen

Richtlijn (wie en wat)
Kritieke delen van systemen (bijv. subprocessen, bestanden) beschermen door isolatie van overige delen.

Doelstelling (waarom)
Beperk de impact bij misbruik van processen.

Risico
Beïnvloeding van andere processen en het weglekken van informatie.

Classificatie
Hoog

Richtlijn 2012
B2-3

Maatregelen

isolatie

01 Stel een ontwerp- en configuratiedocument vast dat beschrijft op welke wijze processen worden afgeschermd van bestanden waartoe zijn geen toegang mogen hebben.
Hiervoor kan een standaard hulpmiddel als 'chroot' en de rechtenstructuur van het besturingssysteem ingezet worden.

02 Stel een ontwerp- en configuratiedocument vast dat beschrijft op welke wijze processen van elkaar worden afgeschermd.
Hiervoor zal meestal virtualisatie noodzakelijk zijn, tenzij de webserver de enige applicatie is die op het onderliggende platform draait. In dat geval moet nog wel aandacht besteed worden aan de hardening van het platform, maar kan verdere isolatie meestal achterwege blijven.

U/PW.05
Toegang tot beheermechanismen

Omschrijving

Beheermechanismen stellen een beheerder in staat de werking van een platform of webserver te controleren en te wijzigen. Adequate bescherming van de toegang tot deze beheermechanismen is daarom essentieel voor de goede werking en beveiliging van platform, webserver en uiteindelijk de webapplicatie.

Het gebruik van 'backdoors' voor de toegang tot beheermechanismen moet absoluut uitgesloten zijn. Een backdoor voor beheer is bijvoorbeeld een beheerinterface waarvoor geen authenticatie nodig is en draait op poort 8888 en daardoor moeilijk te ontdekken zou moeten zijn ('security through obscurity'). De kans is echter groot dat kwaadwillenden backdoors vroeg of laat ontdekken en erin slagen om deze te misbruiken.

Beveiligingsrichtlijn U/PW.05

Toegang tot beheermechanismen gebruiken

Richtlijn (wie en wat)
Het beheer van platformen maakt gebruik van veilige (communicatie)protocollen voor het ontsluiten van beheermechanismen en wordt uitgevoerd conform het operationeel beleid voor platformen.

Doelstelling (waarom)
Voorkomen van misbruik van beheervoorzieningen.

Risico
Een aanvaller kan de controle over het platform of de webserver overnemen.

Classificatie
Hoog

Richtlijn 2012
B2-1

Maatregelen

veilige (communicatie)protocollen

01 Gebruik uitsluitend beveiligde (communicatie)protocollen voor de toegang tot beheermechanismen.
Vermijd in ieder geval het gebruik van onbeveiligde protocollen, zoals Telnet en FTP. SSH en SCP zijn goede vervangers.
Zorg er daarnaast voor dat beheerinterfaces alleen bereikbaar zijn vanaf een gescheiden beheernetwerk (zie richtlijn U/NW.05).

02 Gebruik sterke authenticatie voor de toegang tot de beheermechanismen.
Voor sterke authenticatie kan een combinatie gemaakt worden van de beschikbare toegangsvoorzieningsmiddelen (zie richtlijn U/TV.01).

U/PW.06 Platform-netwerkkoppeling

Omschrijving

Binnen het domein Netwerken (U/NW) is beschreven hoe centraal geplaatste firewalls de omgeving beschermen tegen kwaadwillenden (zie U/NW.03). Naast deze centrale firewalls is het gewenst om decentraal, op de verschillende machines, een aparte firewall te laten werken. Deze lokale (decentrale) firewalls, dit kan een aparte (host) firewall zijn of de firewall functionaliteit wordt aangeboden door het besturingssysteem zelf, vormen daarmee een extra laag in de beveiliging. Enkele voorbeelden van deze firewalls zijn: Ipfw, Pf, Iptables, Ipfilter (ipf) en Microsoft Windows Firewall.

Lokale firewalls hebben als voordeel dat deze zowel op poort- als procesniveau controles uitvoeren. Verder hebben lokale firewalls vaak meer inzicht in het binnenkomende verkeer omdat op de machine zelf ontsleuteling van versleutelde tunnels plaatsvindt. Daarnaast bevatten lokale firewalls vaak veel minder regels in de rulebase waardoor fouten in de configuratie minder aannemelijk zijn.

Tot slot bieden deze firewalls veelal ook uitgebreide mogelijkheden op het gebied van logging en Network Address Translation (NAT).

Beveiligingsrichtlijn U/PW.06

Platform-netwerkkoppeling filteren

Richtlijn (wie en wat)
Ieder platform filtert het netwerkverkeer met behulp van een lokale firewall, zodat het netwerkverkeer beperkt is tot de bekende, toegestane communicatiestromen.

Doelstelling (waarom)
Controleren van het netwerkverkeer, zowel op poort- als procesniveau, dat lokaal binnenkomt en uitgaat.

Risico
Een deel van de communicatie onttrekt zich aan controles, waardoor een restrisico in verschillende beveiligingsonderwerpen overblijft.

Classificatie
Hoog

Richtlijn 2012
B2-4

Maatregelen

bekende, toegestane communicatiestromen

01 Stel een (inrichtings)document op met de communicatiestromen van de op het systeem geïnstalleerde applicaties.
Dit document legt ook vast welke functie(s) het systeem vervult. Denk hierbij aan welke software (applicaties) geïnstalleerd zijn, welke (netwerk)protocollen noodzakelijk zijn, et cetera.
Zorg dat dit (inrichtings)document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatorische) niveau zijn verantwoord.

02 De ingestelde firewall-regels beperken communicatiestromen tot die van het (inrichtings)document.
Bovenstaande document bevat de configuratieregels van de firewall. De feitelijke configuratie dient hier exact mee overeen te stemmen.

U/PW.07 Hardening van platformen

Omschrijving

De hardening van platformen is een resultaat van de toepassing van kwetsbaarhedenbeheer (zie richtlijn B.01/05).

De meeste systemen voeren een beperkt aantal functies uit. Het is mogelijk om het aantal potentiële aanvallen te verminderen door het systeem te ontdoen van onder andere software, gebruikersaccounts en diensten die niet gerelateerd en vereist (strikt noodzakelijk) zijn voor het functioneren van het systeem. Wanneer dat niet mogelijk is, moeten alle niet strikt noodzakelijke faciliteiten zijn uitgeschakeld. Systeemhardening is een leverancier specifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het standaardinstallatieproces. Voorbeelden zijn:

» Indien (externe) systemen, zoals webservers en mailservers ‘reclame’ maken voor hun type en versie, wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren.
» Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

Bij het hardenen van het systeem is een belangrijke strategie om de communicatiemogelijkheden van het systeem tot een minimum (het strikt noodzakelijke) te beperken. Eén van de manieren om dit te bereiken is door onnodige services onbereikbaar te maken door ze te verwijderen of uit te schakelen. Door benodigde services in kaart te brengen en vervolgens de afhankelijkheden te bepalen, ontstaat er een lijst van services die minimaal op het systeem moeten staan. Alle overige services kunnen het beste verwijderd of uitgeschakeld worden. Niet-actieve maar wel aanwezige services op een systeem kunnen uiteindelijk toch tot een kwetsbaar systeem leiden aangezien ‘lekke’ programmacode op het systeem aanwezig is.

Beveiligingsrichtlijn U/PW.07

Hardening van platformen formuleren

Richtlijn (wie en wat)
Voor het configureren van platformen is een hardeningrichtlijn beschikbaar.

Doelstelling (waarom)
Beperken van de functionaliteit tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Risico
Bedoeld of onbedoeld negatief beïnvloeden van een platform, waardoor vertrouwelijkheid, integriteit en/of beschikbaarheid van dat platform niet gegarandeerd is.

Classificatie
Hoog

Richtlijn 2012
B0-5

Maatregelen

Hardeningrichtlijn

01 Richt ICT-componenten (aantoonbaar) volgens de instructies en procedures van de leverancier in.
Neem in de werkinstructies het toepassen van de instructies en procedures van de leverancier op. Houd tijdens het inrichten van een component een checklist bij en teken deze af na voltooiing van het inrichten van de component.
Als alternatief kan de inrichting door een geautomatiseerd proces plaatvinden. In dat geval volstaat het noteren van het versienummer van de gebruikte software en eventuele parameters.

02 Houd een actueel overzicht bij van de noodzakelijke protocollen, services en accounts voor de op het platform geïnstalleerde applicaties.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatorische) niveau zijn verantwoord.

03 Deactiveer of verwijder alle protocollen, services en accounts op het platform als die niet volgens het ontwerp noodzakelijk zijn.
Gebruik het ontwerp om te bepalen welke functies nodig zijn. Schakel alle andere functies uit, ook wanneer deze ‘leuk’ of ‘handig’ zijn.
Verwijder zo mogelijk deze functies van de ICT-component (deïnstallatie).
Tip: leg alle gevonden functies vast, met de vermelding of ze actief, uitgeschakeld of verwijderd zijn. Op die manier is het eenvoudiger vast te stellen of nieuwe functies zijn geïntroduceerd.

04 Toets periodiek of de in productie zijnde ICT-componenten niet meer dan de vanuit het ontwerp noodzakelijke functies bieden (statusopname). Afwijkingen worden hersteld.
Automatische controles kunnen een onderdeel van deze periodieke toetsing zijn, maar zijn in veel gevallen niet voldoende.

05 Pas de beveiligingsconfiguraties van netwerkservices en protocollen op het platform aan conform richtlijnen.
Het ‘tunen’ van de TCP/IP-stack kan helpen in het beveiligen tegen (distributed) denial-of-service ((D)DoS)-aanvallen.

U/PW.08 Platform- en webserverarchitectuur

Omschrijving

De architectuur van platformen en webservers beschrijft de functionele en beveiligingssamenhang en legt de relatie met (de architectuur van) het algemene ICT-landschap. Vanuit een eenduidig gemeenschappelijk beeld worden alle componenten conform deze architectuur gerealiseerd. Hiervoor worden de richtlijnen, instructies en procedures van U/PW.01 toegepast. Op deze manier wordt zeker gesteld dat iedere component aan de vereiste functionele en beveiligingsdoelen bijdraagt.

Beveiligingsrichtlijn U/PW.08

Platform- en webserverarchitectuur vastleggen

Richtlijn (wie en wat)
Voor het implementeren, integreren en onderhouden van platformen en webservers zijn architectuurvoorschriften en beveiligingsvoorschriften beschikbaar.

Doelstelling (waarom)
Een platform bieden dat een betrouwbare verwerking garandeert.

Risico
Onvoldoende beheersing van het platform, waardoor de stabiliteit van ondersteunde applicaties niet gegarandeerd is en mogelijkheden voor misbruik ontstaan.

Classificatie
Midden

Richtlijn 2012
-

Maatregelen

architectuurvoorschriften

01 Stel architectuurvoorschriften op die actief worden onderhouden.
Zorg dat deze voorschriften onderdeel zijn van het proces wijzigingsbeheer (zie richtlijn C.08). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatorische) niveau zijn verantwoord.
Het document:
» *heeft een eigenaar;*
» *is voorzien van een datum en versienummer;*
» *bevat een documenthistorie (wat is wanneer en door wie aangepast);*
» *is actueel, juist en volledig;*
» *is op het juiste (organisatorische) niveau vastgesteld/geaccordeerd.*
De ICT-afdeling en de ICT-securitymanager zijn in ieder geval deel van ‘het juiste (organisatorische) niveau’.

beveiligingsvoorschriften

02 Stel hardeningrichtlijnen op voor platformen, aantoonbaar afgeleid uit de architectuur.
Het gaat hier om de aantoonbare, navolgbare relatie tussen wat de architectuur beschrijft en de concretisering in richtlijnen. Bij de registratie van de inrichting wordt deze lijn doorgetrokken naar de daadwerkelijke configuratie en getroffen maatregelen.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08).

03 Leid de inrichtingsrichtlijnen voor registratie van (beveiligings) events (logging, zie richtlijn C.06) aantoonbaar af uit de architectuur.

UITVOERINGSDOMEIN
» NETWERKEN

Doelstelling

De doelstelling van de laag "Netwerken" is om te waarborgen dat de netwerkinfrastructuur ingericht is overeenkomstig specifieke beleidsuitgangspunten van de organisatie en voldoet aan de eisen die door de organisatie zijn gesteld ten aanzien van de kwaliteitsaspecten vertrouwelijkheid, integriteit, beschikbaarheid en controleerbaarheid.

Inleiding

Het netwerk omvat zowel de infrastructuur om de webapplicatie bereikbaar te maken (de koppeling van de webserver met het internet), als de infrastructuur om de webserver resources op te kunnen laten vragen (koppeling met interne systemen en andere systemen in de DMZ). Figuur 3 illustreert deze netwerkinfrastructuur, met daarin de afbakening van de Richtlijnen (het lichter gearceerde deel). Het uitvallen van het netwerk, of een succesvolle aanval daarop, kan ernstige gevolgen hebben voor de beschikbaarheid van de webapplicatie en in sommige gevallen voor de integriteit en vertrouwelijkheid van het netwerkverkeer en de data.

In het kader van deze Richtlijnen richt netwerkbeveiliging zich voornamelijk op het beveiligen van informatiestromen op het transport- en netwerkniveau en omvat:

» netwerkcomponenten zoals routers en firewalls;
» netwerkdiensten zoals DNS;
» ontwerp, implementatie en beheer van de (netwerk)infrastructuur.

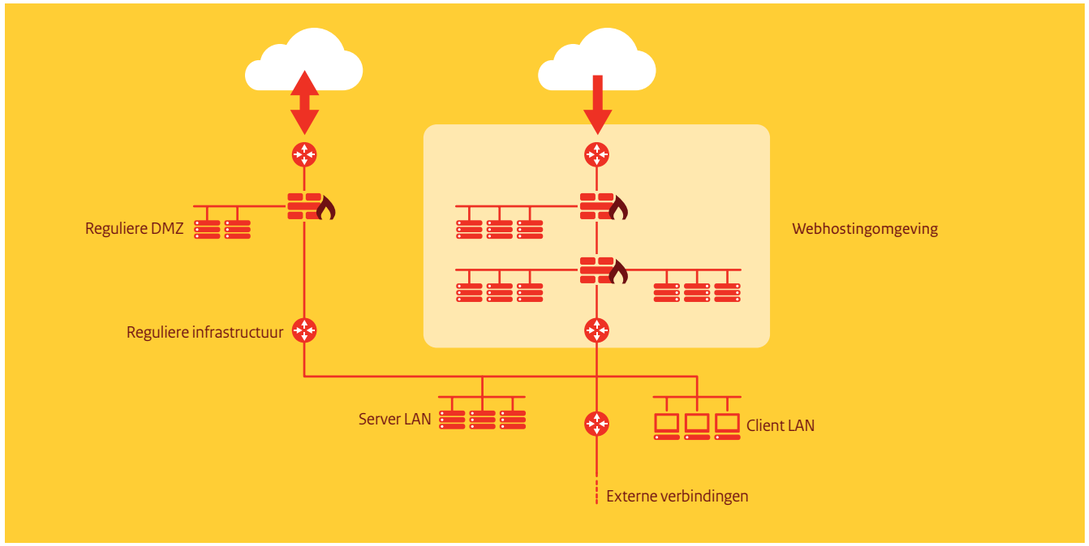
Risico's

De beoogde of vereiste betrouwbaarheid van de webapplicatie wordt ondermijnd door derden, doordat zij in staat zijn het netwerk (of componenten daarin) te manipuleren of verstoren. Oorzaken kunnen gelegen zijn in het niet (correct) of onvolledig toepassen van bekende richtlijnen en (beveiligings)technieken.

Beveiligingsrichtlijnen

Binnen de laag Netwerken worden onderstaande richtlijnen beschreven en per richtlijn worden conformiteitsindicatoren en de betreffende maatregelen uitgewerkt.

» Operationeel beleid voor netwerken (U/NW.01)
» Beschikbaarheid van netwerken (U/NW.02)
» Netwerkzonering (U/NW.03)
» Protectie- en detectiefunctie (U/NW.04)
» Beheer- en productieomgeving (U/NW.05)
» Hardening van netwerken (U/NW.06)
» Netwerktoegang tot webapplicaties (U/NW.07)
» Netwerkarchitectuur (U/NW.08)



Figuur 3. Reikwijdte ICT-Beveiligingsrichtlijnen voor Webapplicaties

U/NW.01 Operationeel beleid voor netwerken

Omschrijving

Het operationeel beleid voor netwerken beschrijft de manier waarop de organisatie omgaat met het inrichten en beschikbaar stellen van netwerken. Configuratie van netwerken vormt de basis voor beveiligde infrastructuur. Het operationeel beleid is een concretere uitwerking van het bovenliggende beleid, bijvoorbeeld zoals in B.01. Een solide operationeel beleid is daarom een randvoorwaarde voor een veilige inrichting van een webapplicatie-omgeving.

Beveiligingsrichtlijn U/NW.01

Operationeel beleid voor netwerken formuleren

Richtlijn (wie en wat)
Het operationeel beleid voor netwerken formuleert richtlijnen, instructies en procedures voor inrichting en beheer van netwerken.

Doelstelling (waarom)
Betrouwbare communicatie voor de systemen die binnen het netwerk geïnstalleerd zijn.

Risico
Ongewenst netwerkverkeer heeft een nadelige invloed op de performance en bedreigt de veiligheid van de aangesloten systemen.

Classificatie
Midden

Richtlijn 2012
-

Maatregelen

richtlijnen, instructies en procedures

01 Stel voorschriften (baselines) op voor de veilige inrichting en beheer van netwerken. De baseline dient ook aandacht te geven aan hardening, zie richtlijn U/NW.06.
Maak gebruik van bestaande richtlijnen van leveranciers en erkende kennisinstituten als NIST, SANS, et cetera.
02 Stel procedures en instructies op voor het inrichten van netwerkcomponenten aan de hand van beveiligingstemplates.
Dit is een inhoudelijke eis aan de richtlijn, gericht op configureren van netwerkcomponenten.
Besteed aandacht aan het regelmatig evalueren en bijstellen van de richtlijnen, procedures en instructies. Indien deze instructies en procedures ruimte bieden om af te wijken van de richtlijn, dient hieraan de vereiste van 'comply or explain' gekoppeld te zijn.
03 Stel aansluitvoorwaarden op die beschrijven wanneer een (nieuwe) component op het netwerk mag worden aangesloten.
De aansluitvoorwaarden kunnen verwijzen naar de beveiligingstemplates (/02).
Binnen verschillende netwerkzones (zie richtlijn U/NW.03) kunnen verschillende aansluitvoorwaarden gelden.

U/NW.02 Beschikbaarheid van netwerken

Omschrijving

Het netwerk vormt de basis(infrastructuur) voor webapplicaties, daarom is het van belang dat het netwerk te maken krijgt met een minimum aan storingen. Het ontwerp van het netwerk dient daarom zodanig te zijn dat deze zo min mogelijk (liefst geen) single-points-of-failure bevat. Loadbalancing en redundantie zijn twee technieken die ingezet kunnen worden om de beschikbaarheid van de infrastructuur te vergroten. Naast het feit dat het ontwerp van het netwerk zo moet zijn dat er zo min mogelijk (liefst geen) uitval zal plaatsvinden, is ook een adequate monitoring, alerting, bewaking en auditing van belang (zie het Beheersingsdomein).

Beveiligingsrichtlijn U/NW.02

Beschikbaarheid van netwerken garanderen

Richtlijn (wie en wat)
Het netwerk is gebaseerd op betrouwbare netwerkcomponenten, ondersteund door redundantie.

Doelstelling (waarom)
Zekerstellen dat er geen zwakke schakels (single-points-of-failure) in voorkomen en dat het netwerk te allen tijde beschikbaar is.

Risico
Onbeschikbaarheid van netwerkcomponenten leiden tot onbeschikbaarheid van het gehele netwerk. Dit leidt tot niet optimale ondersteuning van klanten en stagnatie in zowel productie en als realisatie van bedrijfsdoelstellingen.

Classificatie
Hoog

Richtlijn 2012
B1-6

Maatregelen

betrouwbare netwerkcomponenten

01 Configureer de netwerkcomponenten op basis van beveiligingstemplates.
Er zijn vastgestelde configuratiebaselines en beveiligingstemplates beschikbaar.

redundantie

02 Voer vooraf gekozen en ontworpen netwerkcomponenten meervoudig uit en configureer deze zodanig dat zij automatisch (zonder menselijke interactie) enkelvoudige storingen opvangen.
De inrichting van netwerkcomponenten is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp, waarin is vastgelegd welke uitgangspunten/principes gelden voor het netwerk.
De volgende aandachtspunten moeten worden geadresseerd in het inrichtingsdocument/ontwerp:
» *Welke maatregelen zijn geïmplementeerd zodat single-points-of-failure worden voorkomen of de gevolgen worden geminimaliseerd?*
» *Het netwerk-inrichtingsdocument/ontwerp is actueel en op het juiste (organisatie)niveau vastgesteld.*
» *De zakelijke behoeften moeten zijn vastgesteld en er moet een risicoanalyse (B.03/01) zijn uitgevoerd.*
Routering of redundante netwerkcomponenten (communicatieverbindingen, firewalls, loadbalancers, proxies, routers, switches) zijn mogelijkheden.
Extra redundantie kan worden verkregen door infrastructuur meervoudig uit te voeren en over meerdere datacenters te spreiden.
Gezien de bijkomende kosten die een dergelijke oplossing brengt, moet vanuit de zakelijke behoefte en de risicoanalyse hiervoor een degelijke onderbouwing zijn.

03 Signaleer automatisch opgevangen storingen (failover) aan de beheerders.
Beheerders ontvangen dit signaal, om te voorkomen dat een automatische failover onopgemerkt blijft. Zij dienen dan voor herstel van de uitgevallen component te zorgen, zodat opnieuw een redundante situatie ontstaat. Zonder herstel kan een single-point-of-failure ontstaan zijn.

Verdieping

Loadbalancers
Loadbalancers kunnen verkeer voor een webapplicatie over verschillende gelijkwaardige componenten verdelen. Voor webapplicaties bestaan twee belangrijke load balancing technieken:

Local Server Load Balancing (LSLB).
Een LSLB-loadbalancer verdeelt verkeer lokaal (dat wil zeggen binnen hetzelfde datacenter) over verschillende webservers. Uitval van een webserver zal in dit geval niet per definitie leiden tot het niet meer beschikbaar zijn van de website doordat een andere webserver nog wel beschikbaar is.

Global Server Load Balancing (GSLB).
Een GSLB-loadbalancer is een stuk complexer dan een LSLB-loadbalancer en heeft als doel om load balancing uit te voeren over geografisch gescheiden locaties. DNS functionaliteit is een mechanisme om GSLB voor webapplicaties te bewerkstelligen.

De GSLB-loadbalancer is hierbij autoritatief voor de zone waarin de webapplicatie zich bevindt en fungeert voor deze zone als DNS-server. Door verzoeken voor de zone te beantwoorden met steeds wisselende ip-adressen, komen gebruikers uit op de verschillende geografisch gescheiden locaties

Welke load balancing oplossing het meest geschikt is voor een bepaalde webapplicatie, is afhankelijk van verschillende variabelen zoals het beschikbare budget, het ontwerp van het netwerk (zie richtlijn U/NW.08) en de architectuur van de webapplicatie (zie richtlijn U/WA.09)

Redundantie
Veel netwerkcomponenten bieden standaard ondersteuning voor redundantie en bijbehorende statussynchronisatie.
Netwerkcomponenten die in aanmerking komen voor redundante uitvoering zijn:
» Communicatieverbindingen;
» Firewalls;
» Loadbalancers;
» Proxies;
» Routers;
» Switches;
» et cetera.

Maar denk ook aan redundant uitvoeren van componenten zoals:
» Energievoorziening;
» Koeling/klimaatbeheersing;
» Voeding;
» Controllers;
» et cetera.

Automatische failover
Wanneer er redundante componenten zijn, is een automatisch gebruik van deze redundantie (failover) aan te bevelen. Het heeft immers weinig zin om hiervoor menselijke tussenkomst te vereisen, omdat er dan nog steeds een periode van onbeschikbaarheid zal zijn. Echter, er is ook een risico dat de uitval van een component onopgemerkt blijft door de automatisch failover via redundante componenten. Een goede bewaking en signalering is daarom noodzakelijk.

U/NW.03 Netwerkzonering

Omschrijving
Een Demilitarised Zone (DMZ) is een apart stuk netwerk dat specifiek bedoeld is om webapplicaties – en andere vanaf het internet bereikbare applicaties – in onder te brengen. De DMZ vormt de scheiding tussen het internet enerzijds en het interne netwerk anderzijds. Op alle snijvlakken (internet-DMZ en DMZ-intern netwerk) worden beperkte verkeersstromen toegestaan, waardoor het risico op het binnendringen van het interne netwerk via het internet zo laag mogelijk wordt gehouden.
Een DMZ kan bestaan uit meerdere compartimenten. Uitgangspunt bij compartimenteren is dat servers, webapplicaties en toepassingen van een gelijk beveiligingsniveau in één gezamenlijk compartiment worden geplaatst. Zo komen bijvoorbeeld webproxies in één compartiment, webservers voor internetsites in één compartiment, webservers voor extranetten in één compartiment, databases in één compartiment, et cetera.

Beveiligingsrichtlijn U/NW.03

Netwerkzonering toepassen

Richtlijn (wie en wat)
Het netwerk is gescheiden in logische en fysieke domeinen (zones), in het bijzonder is er een DMZ die tussen het interne netwerk en het internet gepositioneerd is.

Doelstelling (waarom)
Een beveiligde (of robuuste) netwerkinfrastructuur bieden voor de bedrijfstoepassingen.

Risico
Een aanvaller krijgt ongelimiteerd toegang tot het interne netwerk en de daarop aangesloten systemen.

Classificatie
Hoog

Richtlijn 2012
B1-1, B1-2, B1-4

Maatregelen

logische en fysieke domeinen

01 Deel het netwerk in domeinen (of zones) op, op grond van gemeenschappelijke kenmerken van de systemen binnen een domein.
De gemeenschappelijke kenmerken kunnen gekozen zijn op basis van beveiligingsniveau, functionele taakverdeling, of een combinatie van verschillende dimensies. Het resulterende zone-ontwerp is actueel, gedocumenteerd en vastgesteld.

02 Sta alleen voor de beoogde diensten noodzakelijke verkeersstromen tussen zones toe.
De noodzakelijke verkeersstromen zijn bekend en gedocumenteerd. Op het koppelvlak van de zones worden andere verkeersstromen actief geblokkeerd. De manier waarop deze blokkade wordt ingevuld hangt af van de aard van het koppelvlak (router, firewall, DMZ).

03 Scheid netwerkzones fysiek of logisch van elkaar, zet een minimale hoeveelheid netwerkcomponenten in op koppelvlakken die deze scheiding handhaven.
Koppeling van netwerkzones kan plaatsvinden door een firewall of (reverse) proxy's.

04 Gebruik verschillende fysieke interfaces voor aansluiting van verschillende (logische) netwerkzones.
Het gaat erom dat een storing aan een netwerkcomponent er nooit toe mag leiden dat de (logische) indeling in zones doorbroken kan worden. De koppelingen tussen verschillende netwerkcomponenten, servers, firewall en andere apparatuur kunnen worden gerealiseerd door één connectiecomponent (switch of hub). Hiermee wordt een fysieke koppeling bewerkstelligd. Door deze fysieke koppeling tussen deze netwerkcomponenten is het in sommige gevallen mogelijk om de logische segmentering van het netwerk via deze netwerkcomponenten te omzeilen. Om te voorkomen dat logische scheidingen kunnen worden omzeild is het raadzaam om koppelingen tussen netwerkcomponenten zoveel mogelijk via separate en onafhankelijke componenten te realiseren.

DMZ

05 Scheid het interne bedrijfsnetwerk en het internet van elkaar door middel van een bufferzone ('demilitarised zone', DMZ) dat bestaat uit frontend-zones en backend-zones.
In de ontwerp- en configuratiedocumentatie is vastgelegd hoe de DMZ is ingericht en is geconfigureerd. De volgende aandachtspunten komen aan de orde:
» *welke webapplicaties worden ontsloten?*
» *welke informatie mag in de DMZ worden opgenomen?*
» *welke ondersteunende applicaties zijn noodzakelijk?*
» *welke compartimenten, koppelvlakken en verkeersstromen tussen de compartimenten zijn noodzakelijk?*
» *welke ip-adressen worden gebruikt (NAT, DHCP)?*
» *welke vaste routepaden om het verkeer door de DMZ te routeren kunnen worden toegepast?*
» *welk uitgaand verkeer vanaf de webserver is noodzakelijk?*
» *zijn aansluitvoorwaarden opgesteld?*
Om de realisatie van de koppelingen tussen netwerkcomponenten op juistheid te kunnen beoordelen kan worden uitgegaan van het

ontwerpdocument van de DMZ. De inrichting van de DMZ is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten/principes gelden voor de toepassing van de DMZ. Zorg dat het inrichtingsdocument of -ontwerp onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie) niveau zijn verantwoord.

06 Leg in een DMZ-inrichtingsdocument/ontwerp vast welke uitgangspunten en principes gelden voor de toepassing van de DMZ.
Het DMZ-inrichtingsdocument/ontwerp is actueel, onderbouwd, op het juiste (organisatie)niveau vastgesteld en onderdeel van het proces wijzigingsbeheer (zie richtlijn C.08). De volgende aandachtspunten moeten worden geadresseerd in het DMZ-inrichtingsdocument/ontwerp:
- *Hoe verloopt de interne/externe routering van webverkeer?*
- *Welke vaste routepaden om het verkeer door de DMZ te routeren kunnen worden toegepast?*
- *Worden koppelingen tussen netwerkcomponenten doormiddel van separate koppelmechanismen gerealiseerd?*
- *Welke beheermechanismen worden toegepast?*

07 Plaats alleen de systemen, (web)applicaties en diensten in de DMZ die in het DMZ-ontwerp voorkomen.

08 Configureer de filters en regels binnen een DMZ conform het DMZ-ontwerp.

09 Laat verkeersstromen tussen interne netwerken en externe netwerken lopen via een DMZ, en controleer en ontkoppel deze op applicatieniveau (sessiescheiding).

10 Sta alleen de voor de beoogde diensten noodzakelijke verkeersstromen tussen internet en de DMZ en tussen de DMZ en het interne netwerk toe.
Dit betekent bijvoorbeeld dat protocollen als RIP, OSPF, Proxy-ARP en ip-pakketten met source-routing en ICMP-redirect/-unreachable berichten vanaf het internet geblokkeerd worden.

Verdieping

Een netwerk kan topologisch fysiek en logisch worden beschreven. Een topologie illustreert de wijze waarop netwerkcomponenten (onder andere computers, servers, devices) met elkaar zijn verbonden. Er bestaan verschillende soorten typologieën: vermaasd netwerk (mesh), sternetwerk (star), busstructuur (bus), ringnetwerk (ring) en boomstructuur (tree).

Bij het ontwerpen/inrichten van de DMZ wordt tenminste een logische scheiding van netwerkzones rondom de firewall(s) gecreëerd. Deze logische scheiding betekent niet per definitie ook een fysieke scheiding van netwerkzones. Verschillende netwerkcomponenten, servers en andere apparatuur kunnen immers wel aangesloten zijn op dezelfde switch of hub. In dat geval vormt de hub of switch een fysieke koppeling (bypass). Hierdoor is het mogelijk om de logische compartimentering van het netwerk via deze netwerkcomponenten te omzeilen.

Maak voor de fysieke scheiding van netwerkzones gebruik van één van de twee onderstaande mogelijkheden:

1. Netwerkzones zijn gescheiden door een firewall en interfaces naar verschillende netwerkzones (bijvoorbeeld naar de DMZ en naar de backoffice) gebruiken verschillende (fysieke) netwerkcomponenten.
2. Er worden (reverse) proxies inline geplaatst. Inline plaatsing houdt in dat de proxies twee interfaces krijgen: één interface voor het externe netwerk (buitenkant) en één interface voor het interne netwerk (binnenkant). Al het verkeer van en naar de webapplicatie is in dit geval verplicht om via de proxy te lopen. Het nadeel van een dergelijke plaatsing van een proxy is dat alle webapplicaties via deze proxy moeten verlopen, waardoor men afhankelijk is van ondersteuning van de proxy voor het specifieke type verkeer (bijvoorbeeld een http-proxy voor webverkeer, een SMTP-proxy voor e-mailverkeer, et cetera). De mogelijkheid tot het inline plaatsen van een proxy is dan ook zeer afhankelijk van de andere webapplicaties die de organisatie via de DMZ ontsluit.

Opmerking 1
Bij het gebruik van inline proxies is het van belang dat de twee interfaces aangesloten zijn op verschillende switches. Verbindt men de componenten uit de compartimenten die de proxy van elkaar scheidt met dezelfde switches, dan kan de logische compartimentering van het netwerk alsnog worden omzeild.

Opmerking 2
Bij de toepassing van twee interfaces binnen één server is in strikte zin nog niet echt sprake van een fysieke scheiding.

De mate van gewenstheid van deze beveiligingsrichtlijn hangt af van de risicoanalyse (B.03/01) en zakelijke behoeften. Daarbij wordt gekeken naar de kans op optreden van bedreigingen en de mogelijke impact hiervan op de bedrijfsvoering.

Door compartimentering toe te passen, wordt voorkomen dat het compromitteren van een server, applicatie of toepassing in één compartiment, directe gevolgen heeft voor servers, webapplicaties en toepassingen in een ander compartiment. Slaagt een kwaadwillende erin een server binnen een compartiment aan te vallen, dan heeft de kwaadwillende vanaf deze server alleen toegang tot andere systemen in datzelfde compartiment. De impact van een succesvolle aanval op een systeem wordt hierdoor verkleind. De impact is uiteraard afhankelijk van de verkeersstromen die zijn toegestaan tussen de verschillende compartimenten. Zo bestaat de kans dat een kwaadwillende via een succesvol aangevallen webserver alsnog een databaseserver in een ander compartiment kan benaderen omdat de firewall bepaalde databaseverbindingen vanaf de webserver richting de databaseserver toestaat. Een veilige inrichting van de DMZ is daarom van groot belang om te voorkomen dat kwaadwillenden via internet toegang krijgen tot verschillende compartimenten en uiteindelijk het interne netwerk van de organisatie.
Hieronder een indicatie van systemen die *niet* in een DMZ mogen worden geplaatst:
- databaseserver;
- mailserver;
- directory-services zoals LDAP en Active Directory.

Hieronder een indicatie van systemen die *wel* in een DMZ kunnen worden geplaatst:
- webservers;
- mailgateway (MTA);
- (reverse) proxy.

Onderstaande aandachtspunten/overwegingen dienen als input voor het ontwerp van de DMZ. De gemaakte beslissingen moeten worden onderbouwd, op het juiste (organisatie) niveau worden vastgesteld, zijn gedocumenteerd en worden onderhouden. Hierdoor is altijd over een actueel ontwerp/inrichting van de DMZ beschikbaar. Het uitgangspunt moet steeds zijn: plaats alleen in de DMZ wat absoluut noodzakelijk is om de gewenste functionaliteit te kunnen bieden.
- Stel vast welke webapplicaties ontsloten worden.
- Stel vast welke informatie in de DMZ opgenomen mag worden.
- Stel vast welke ondersteunende applicaties nodig zijn (functioneel).
- Stel de indeling van de compartimenten vast.
- Stel de koppelvlakken tussen de compartimenten vast.
- Stel de (gecontroleerde) verkeersstromen tussen de compartimenten vast.
- Stel vaste routepaden vast om het verkeer door de DMZ te routeren.
- Stel vast welk uitgaand verkeer vanaf de webserver mogelijk is.
- Stel de regels van de firewall (rulebase) vast.
- Zorg voor een actueel en geaccordeerd DMZ-inrichtingsdocument/ontwerp.
- Maak gebruik van het dual-vendor concept.

Bovenstaande aandachtspunten/overwegingen zullen hierna kort worden toegelicht.

Stel vast welke webapplicaties ontsloten worden
Welke webapplicaties worden ontsloten via de DMZ, bepaalt mede het ontwerp van de DMZ. Ondersteunt de DMZ alleen webapplicaties, dan bestaat er bijvoorbeeld de mogelijkheid om al het binnenkomende verkeer af te laten handelen door een reverse proxy. Als de DMZ echter ook andere diensten naar het internet ontsluit (bijvoorbeeld e-mail), dan is deze mogelijkheid er wellicht niet of moet deze op een andere manier binnen de DMZ worden ingebouwd.

Stel vast welke informatie in de DMZ opgenomen mag worden
In een DMZ worden hooguit openbare gegevens van een organisatie opgeslagen.

Stel vast welke ondersteunende applicaties nodig zijn (functioneel)
Welke ondersteunende applicaties nodig zijn in verband met de functionele werking van de webapplicatie, bepaalt mede het ontwerp van de DMZ. De verschillende typen applicaties bepalen onder andere hoeveel compartimenten er gecreëerd moeten worden. Als de wens bestaat om al het verkeer te filteren, moet voor elk type applicatie intelligentie binnen de DMZ worden ingebouwd.

Stel de indeling van de compartimenten vast
Compartimentering maakt het mogelijk om met verschillende beveiligingsniveaus binnen een netwerkinfrastructuur te werken en verkeersstromen te monitoren en controleren. Elk compartiment heeft andere risico's, die afhankelijk zijn van de diensten of ICT-voorzieningen die erin zijn ondergebracht. Er wordt dan ook een ander compartiment ingericht als het risicoprofiel dat vereist. Dit kan bijvoorbeeld noodzakelijk zijn om verschillende productieomgevingen uit elkaar te houden, die niet hetzelfde beveiligingsniveau hebben. Door deze compartimentering wordt een directe verbinding naar de backoffice vanaf het internet voorkomen. De backoffice is het interne netwerk (LAN) waarin systemen staan waarvan de webapplicatie gebruik maakt.

Stel nummerplan vast
Bepaal welke private en publieke ip-adressen worden toegepast en of er gebruik van Dynamic Host Configuration Protocol (DHCP) en/of Network Address Translation (NAT) wordt gemaakt. Leg dit vast in een ip-nummerplan.

Stel de koppelvlakken tussen de compartimenten vast
Aandachtspunten bij het vaststellen van de koppelvlakken zijn onder andere de beschikbaarheid van de verbinding en de mogelijkheid om alle verkeer tussen de compartimenten te monitoren.

Stel de verkeersstromen tussen de compartimenten vast
Welke verkeersstromen (dit bevat zowel bron- en bestemmings-ip-adressen als netwerkprotocollen) zijn noodzakelijk voor het ontsluiten van webapplicaties via de DMZ en de ondersteunende applicaties. Deze verkeerstromen bepalen mede het ontwerp van de DMZ.

Volstaat http-verkeer vanaf het internet richting de webapplicatie of zijn ook koppelingen nodig vanuit de DMZ naar het interne netwerk? Op het koppelvlak tussen compartimenten zijn filterfuncties gepositioneerd voor het gecontroleerd doorlaten van gegevens; niet-toegestane gegevens worden tegengehouden.

Stel aansluitvoorwaarden op
Leg in aansluitvoorwaarden (eisen, criteria) vast wat binnen de compartimenten (DMZ) geplaatst mag worden. In deze aansluitvoorwaarden staat beschreven waaraan de ICT-omgeving moet voldoen om gebruik te mogen maken van de geboden ICT-faciliteiten

Stel vaste routepaden vast om het verkeer door de DMZ te routeren
De vastgestelde compartimentering van de DMZ vormt de basis voor het opstellen van routepaden. Een routepad beschrijft een toegestane verkeersstroom door de DMZ. Door routepaden vast te stellen wordt het omzeilen van verplichte beveiligingsmechanismen voorkomen. Hierdoor worden maatregelen voor elke webapplicatie afgedwongen.

Stel uitgaand verkeer vanaf de webserver vast
Het is bij compartimentering niet alleen belangrijk om aandacht te besteden aan inkomend verkeer, maar ook aan uitgaand verkeer. Veel aanvallen maken misbruik van het feit dat een webserver de

mogelijkheid heeft om een verbinding met een ander systeem op te zetten via internet. Het beste is om geen enkel verkeer vanuit de webomgeving naar andere omgevingen toe te staan. Als het absoluut noodzakelijk is, zorg dan dat dit op een gecontroleerde wijze wordt uitgevoerd. Denk hierbij aan het gebruik van een proxy voor het toestaan van http-verkeer vanaf een webserver richting een beperkte set systemen op internet. Door verkeer vanaf een webserver richting het internet te blokkeren, wordt misbruik van een kwetsbaarheid bemoeilijkt of de schade door misbruik van deze kwetsbaarheid beperkt.

Stel de regels van de firewall (rulebase) vast
Het is belangrijk om overzicht te houden over de verkeersstromen die de firewall toestaat. Bij nieuwe verkeersstromen moeten de bijbehorende toegangsregels beheerst worden ingepast in de bestaande rulebase. Bij nieuwe webapplicaties moet een helder en gefundeerd overzicht worden aangeleverd van de verkeersstromen die de te implementeren webapplicatie nodig heeft. Maak hierbij gebruik van 'verkeersoverzichten'. Het verkeersoverzicht bevat alle firewalls en servers die betrokken zijn bij het aanbieden van de webapplicatie. Dit betekent dat naast de webserver ook alle andere servers waarvan de webapplicatie gebruik maakt (zoals databaseservers), onderdeel uit moeten maken van het verkeersoverzicht. In dit overzicht zijn alle verkeersstromen tussen de componenten ingetekend. Hierdoor ontstaat een overzicht van de regels die op de firewalls nodig zijn om de webapplicatie te kunnen laten functioneren.

Zorg voor een actueel en geaccordeerd DMZ-inrichtingsdocument/ontwerp
Het is van cruciaal belang om een actueel en geaccordeerd overzicht te hebben van het DMZ-ontwerp, waarin de antwoorden op bovenstaande overwegingen zijn beschreven. Dit is noodzakelijk zodat impactanalyses van voorgestelde wijzigingen altijd zijn gebaseerd op de huidige netwerkinfrastructuur.

Maak gebruik van het dual-vendor concept
Voorkom dat kwaadwillenden gebruik kunnen maken van dezelfde kwetsbaarheid bij functioneel vergelijkbare producten. Hierdoor wordt de impact van een kwetsbaarheid beperkt. Het concept dual-vendor, maar geldt voor alle functioneel vergelijkbare producten. Door de centrale plaatsing van de firewall(s) kan een kwetsbaarheid op deze firewall(s) grote gevolgen hebben. Door een dual-vendor concept te implementeren wordt de schade bij een dergelijke kwetsbaarheid beperkt. Het dual-vendor concept houdt in dat twee firewalls de netwerkbeveiliging in de DMZ uitvoeren en dat deze firewalls van verschillende makelij (merken) zijn.

Zonder het dual-vendor concept, firewalls van dezelfde makelij (merk), kan een kwaadwillende, na het compromitteren van de eerste firewall, op eenzelfde manier de tweede firewall compromitteren. Dit vanwege het feit dat een potentiële kwetsbaarheid dan op beide systemen aanwezig zal zijn. Opmerking: Het toepassen van een dual-vendor concept hoeft niet automatisch te betekenen dat je twee typen centrale firewalls in de omgeving plaatst. Dit concept kan ook ingevuld worden door, naast de centraal geplaatste firewalls, firewalls lokaal op de machines te installeren (zie richtlijn U/PW.06).

U/NW.04 Protectie- en detectiefunctie

Omschrijving
De inrichting van ICT-componenten, het netwerkverkeer en de gehanteerde protocollen dienen een robuuste eenheid vormen om bescherming te kunnen bieden tegen aanvallen en/of aanvallen te kunnen detecteren (onder andere (D)DoS). Dit zorgt ervoor dat beschikbaarheid van de te leveren services is gegarandeerd. Hiervoor zijn detectie- en protectiemechanismen geïmplementeerd.

Beveiligingsrichtlijn U/NW.04

Protectie- en detectiefunctie toepassen

Richtlijn (wie en wat)
De netwerkcomponenten en het netwerkverkeer worden beschermd door middel van protectie- en detectiemechanismen.

Doelstelling (waarom)
Het detecteren van aanvallen (onder andere (D)DoS) om te voorkomen dat de vertrouwelijkheid, integriteit en/of beschikbaarheid van geleverde services negatief wordt beïnvloed.

Risico
Via netwerkcomponenten of netwerkverkeer wordt vertrouwelijkheid, integriteit en/of beschikbaarheid aangetast, zonder dat dit (tijdig) gedetecteerd wordt en zonder dat hier adequaat op geacteerd kan worden.

Classificatie
Hoog

Richtlijn 2012
B1-5, B7-1

Maatregelen

protectiemechanismen
01 Zorg voor een actueel DMZ-inrichtingsdocument/ontwerp dat inzicht geeft welke protectiemechanismen zijn betrokken.
Het DMZ-inrichtingsdocument/ontwerp (zie richtlijn U/NW.03/05) geeft onder andere inzicht in: gehanteerde uitgangspunten/principes, inrichtingskeuzes, geïmplementeerde maatregelen tegen (D)DoS-aanvallen, vaststelling van het document op het juiste (organisatie)niveau.
02 Pas anti-spoofingmechanismen toe in het netwerk.
Unicast Reverse-Path Forwarding (URPF) controleert op een interface of een ip-pakket afkomstig is van een bron ip-adres dat volgens de routeringstabel bereikbaar is via datzelfde interface.
Ip-adressen die nog niet door IANA zijn uitgegeven worden geblokkeerd (bogon lists).

03 Reguleer dataverkeer met access control lists (ACL's) op basis van bijvoorbeeld ip-adres of poortnummer.
04 Stel de firewall-regels op en configureer deze via een proces en review dit periodiek.
De regels zijn opgesteld door aangewezen functionaris, rekening houdend met informatiebeveiligingsbeleid en gebaseerd op 'least privilege'.

detectiemechanismen
05 Monitor inkomend en uitgaand verkeer in het netwerk.
06 Monitor de infrastructuur zodat detectie van ((D)DoS-) aanvallen mogelijk is.
Inzet van tools als Netflow.
07 Implementeer Intrusion Detection Systemen (IDS) of Intrusion Prevention Systemen (IPS).
In de ontwerp- of configuratiedocumentatie is vastgelegd waar en hoe IDS'en of IPS'en worden ingezet.
» *De zakelijke behoeften en maatregelen. Rapportage van de risicoanalyse (B.03/01) waarop de beslissing is gebaseerd.*
» *Een plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.*
» *Leg voor een IPS duidelijk vast welke acties op basis van welke bevindingen automatisch worden uitgevoerd.*
08 Richt de IDS'en en IPS'en in op basis van een geaccordeerd inrichtingsdocument/ontwerp.
Zorg dat het inrichtingsdocument of -ontwerp onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08).
09 Houd rapportage(tool)s beschikbaar voor analyses van de door detectiemechanismen vastgelegde gegevens.

Verdieping

Protectiefunctie
Het NCSC whitepaper 'Aanbevelingen ter bescherming tegen Denial-of-Service aanvallen' [12] beschrijft een aantal maatregelen om zichzelf tegen (D)DoS-aanvallen te beschermen. De maatregelen die dit whitepaper voorstelt, zijn hieronder kort samengevat:
» Maak gebruik van anti-spoofingmechanismen:
› Unicast Reverse-Path Forwarding (URPF). URPF controleert op een interface of een ip-pakket afkomstig is van een bron-ip-adres dat volgens de routeringstabel bereikbaar is via de betreffende interface.
› Bogon-lijst. Een bogon-lijst[53] bevat een overzicht van alle ip-blokken die nog niet door Internet Assigned Numbers Authority[54] (IANA) zijn uitgegeven en waarvandaan dus ook nooit verkeer afkomstig kan zijn. Een dergelijke bogon-lijst kan als basis voor de rulebase van elke firewall gebruikt worden.
› Access Control Lists (ACL). Reguleer dataverkeer op basis van bijvoorbeeld ip-adres of poortnummer.
» Zet firewalls in. Voorkom dat Stateful firewalls en Intrusion Prevention apparatuur gebruikt worden als beschermingsmaatregel direct voor de website. Deze apparatuur kan namelijk een DoS versterken. Het is beter om netwerk policies te implementeren op routers en switches. Als toch gebruik wordt gemaakt van firewalls die kunnen meekijken en ingrijpen op applicatieniveau, maak dan gebruik van software op de webserver zelf (zie richtlijn U/PW.06).
» Harden systemen. Vooral het 'tunen' van de TCP/IP-stack kan helpen in het beveiligen tegen (D)DoS-aanvallen (zie richtlijn B.01/05 en U/PW.07).
» Besteed aandacht aan de netwerkomgeving (zie richtlijn U/NW.03), bijvoorbeeld:
› Implementeer IDMS[55] (Intelligent DDoS Mitigation System) en RTBH[56] (Remotely-Triggered Black Hole). Deze maatregelen voorkomen overbelasting van web-, DNS- en mailservers. Ze zijn ook een goede oplossing als stateful apparatuur om wat voor reden dan ook, niet uit het netwerk verwijderd mag of kan worden. Daarnaast zijn ze in staat om loadbalancers te beschermen.
› Zorg ervoor dat authorative DNS-servers en recursive/caching DNS-servers logisch gescheiden zijn, door ze in aparte netwerken te plaatsen.
» Maak afspraken met (hosting) providers.
De rol van de provider wordt soms over het hoofd gezien of onderschat. De meeste (hosting) providers kunnen op de volgende gebieden helpen en maak hierover afspraken:
› Een goed anti-spoofing mechanisme blokkeert verkeer dat afkomstig is van RFC19185, ip-adressen of van adressen die de IANA nog niet heeft gealloceerd.[57]
› Een detectiemechanisme, zoals Netflow, kan een DoS-aanval signaleren.
› Krachtige systemen, zoals routers, kunnen effectief een DoS-aanval stoppen of beperken.
› Upstream-providers en andere netwerkrelaties van uw provider kunnen aanvallen uit andere netwerken blokkeren.
» Monitor actief het inkomende en uitgaande verkeer in het netwerk zodat in een vroeg stadium gereageerd kan worden op (D)DoS-aanvallen. Maak hiervoor gebruik van bijvoorbeeld een tool als Netflow. Voorbeelden van open source software voor de analyse van Netflow-data zijn NFSen[58] en NFDump[59].
De afweging in welke mate aan deze maatregel wordt voldaan, hangt af van de risicoanalyse (B.03/01) en zakelijke behoeften.

53 Team Cymru, een non-profit beveiligingsorganisatie, biedt via haar website een bogon lijst aan. De actuele lijst wordt dor Team Cymru aangeboden via de volgende URL: http://www.cymru.com/Documents/bogon-list.html
54 http://www.iana.org/
55 http://www.arbornetworks.com/en/docman/the-growing-need-for-intelligent-ddos-mitigationsystems/download.html
56 http://tools.ietf.org/pdf/rfc5635.pdf
57 Een overzicht van ip-blokken die door IANA nog niet zijn uitgedeeld aan een Local Routing Registry (LIR) is te vinden op http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
58 http://nfsen.sourceforge.net
59 http://nfdump.sourceforge.net

Daarbij wordt gekeken naar de kans op optreden en de mogelijke impact. Het NCSC factsheet 'FS 2013-01: Continuïteit van onlinediensten'[60] zet doelwitten en gevolgen van DoS-aanvallen uiteen en legt uit hoe u zich kunt beschermen.

Detectiefunctie

Intrusion Detection Systemen (IDS) helpen bij het detecteren van aanvallen op (netwerk)infrastructuren en webapplicaties. IDS'en monitoren continu het verkeer dat zich door de DMZ-compartimenten verplaatst en kunnen, veelal op basis van aanvalspatronen, misbruik van webapplicaties en andere infrastructuurcomponenten detecteren. De volgende soorten IDS'en worden onderkend:

» Network-based Intrusion Detection System (NIDS). Een NIDS wordt als losstaand component in het netwerk geplaatst waarna deze component netwerkverkeer opvangt. Host-based Intrusion Detection System (HIDS). Een HIDS wordt op een server geïnstalleerd waarna het HIDS continu de activiteiten op deze server monitort. Het HIDS kijkt hierbij niet alleen naar het netwerkverkeer (zoals het NIDS) maar ook naar logging en veranderingen op het systeem zelf.
» Application-based IDS (APIDS). Een application-based IDS wordt specifiek ingezet voor het monitoren van misbruik van een specifieke webapplicatie of een specifiek protocol.
» Een Intrusion Prevention System (IPS). Dit is een appliance die naast detectie ook automatisch beschermende acties kan ondernemen bij gedetecteerd misbruik. Denk hierbij bijvoorbeeld aan het droppen van ip-pakketten, het blokkeren van ip-adressen.

Het detecteren van aanvallen gebeurt veelal op basis van bekende aanvalspatronen. Deze manier van detectie, op basis van 'handtekeningen' van bekende aanvallen, wordt ook wel signature-based genoemd. Tegenover de signature-based IDS'en staan de anomaly-based systemen. Deze systemen werken niet op basis van handtekeningen, maar op basis van afwijkingen (anomalieën).

Bij het inrichten van een NIDS is het belangrijk goed te bekijken welke meetpunten interessant zijn voor het NIDS om op die manier een zo compleet mogelijk beeld te krijgen van aanvallen op de omgeving. Bekijk daarbij aan de hand van de DMZ-opbouw en de compartimentering (zie richtlijn U/NW.03) in het algemeen wat interessante meetpunten zijn.

Om kwalitatief hoogwaardige informatie te verzamelen en deze effectief te verwerken, is het belangrijk om aandacht te schenken aan de volgende zaken:

» Voorzie signature-based systemen regelmatig van de nieuwste aanvalspatronen (bij voorkeur automatisch).
» Zorg ervoor dat databases voldoende ruimte bieden om de grote hoeveelheid gegevens die een NIDS produceert, in onder te kunnen onderbrengen.
» Beslis hoelang logging moet worden opgeslagen en hoe deze moet worden gearchiveerd.
» Tune de alarmering van het NIDS. Beheerders zullen een NIDS dat continu alarmen uitzendt, niet meer serieus nemen. Onderschat daarbij de hoeveelheid mankracht die nodig is voor het monitoren en onderzoeken van anomalieën en false positives niet.
» Het kan een zeer intensieve klus blijken te zijn om de filters van het IDS optimaal in te richten.

Eisen aan loginformatie

Regel een goede beheerprocedure in voor het IDS. Leg bijvoorbeeld vast wie regelmatig (bijvoorbeeld elke ochtend) de logging van het IDS bekijkt. Daarnaast is het, ter verbetering van de leesbaarheid van de logging, aan te raden filters op de logging te plaatsen (zie ook richtlijn C.06).

Opvolging

Er moet actie worden ondernomen indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren (zie ook richtlijn C.07).

U/NW.05 Beheer- en productieomgeving

Omschrijving

Binnen het netwerk bestaat een onderscheid tussen het productie- en het beheerdomein. Het productiedomein is in feite het gedeelte van de DMZ waarop verkeer vanaf internet terecht komt. Het onderscheid is aangebracht om te voorkomen dat beheer- en productieverkeer door elkaar gaan lopen. Beheer werkt vaak via webinterfaces en door beheer toe te staan via het productiedomein, wordt het risico gelopen dat de bijbehorende webinterfaces en andere beheervoorzieningen te benaderen zijn vanaf het internet. Met betrekking tot beheer moet onderscheid gemaakt worden tussen drie vormen met ieder hun eigen maatregelen:

» Contentbeheer (bijvoorbeeld web en database content)
Contentbeheer wordt over het algemeen door de organisatie zelf, vanaf hun eigen werkplek, uitgevoerd en hiervoor gelden dan de aandachtspunten zoals die zijn benoemd in richtlijn U/NW.03. De contentbeheerders moeten op een veilige en gecontroleerde wijze toegang krijgen tot de systemen waar de content is opgeslagen. Denk hierbij aan webservers, databases en Content Management Systemen (CMS).Afhankelijk van de mogelijkheden die de contentbeheerders hebben, bijvoorbeeld het ontwikkelen van formulieren en dynamische content, moet rekening worden gehouden met andere relevante maatregelen zoals die in deze Richtlijn zijn beschreven.
» Applicatiebeheer (bijvoorbeeld het ontwikkelen en onderhouden van webapplicaties)
Voor applicatiebeheer gelden in hoofdlijnen de richtlijnen zoals die zijn beschreven in U/WA.
» Technisch beheer (bijvoorbeeld besturingssystemen en netwerk)
Deze beheerders benaderen de systemen die zij beheren veelal via terminal-emulatie of soortgelijke applicaties. Vaak hebben ze de mogelijkheid om willekeurige commando's uit te laten voeren en configuraties naar eigen inzicht aan te passen.

Onderstaande aandachtspunten/overwegingen dienen als input voor de scheiding tussen beheer en productie. De gemaakte beslissingen moeten worden onderbouwd, op het juiste (organisatie) niveau worden vastgesteld, zijn gedocumenteerd en worden onderhouden zodat altijd over een actueel ontwerp/inrichting van het netwerk wordt beschikt. Het uitgangspunt moet steeds zijn, wat minimaal noodzakelijk (hoogst nodig) is om de gewenste functionaliteit te kunnen bieden.

Beveiligingsrichtlijn U/NW.05

Beheer- en productieomgeving afschermen

Richtlijn (wie en wat)
Binnen de productieomgeving zijn beheer- en productieverkeer van elkaar afgeschermd.

Doelstelling (waarom)
Het voorkomen van misbruik van de beheervoorzieningen vanaf het internet.

Risico
Door het ontbreken van afdoende afscherming kunnen eindgebruikers beheerdersautorisaties verwerven.

Classificatie
Hoog

Richtlijn 2012
B1-2

Maatregelen

beheer- en productieverkeer

01 Geef in een inrichtingsdocument aan op welke wijze contentbeheer (web- en database-content), applicatiebeheer en technisch beheer worden uitgeoefend.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.
02 Stel een overzicht op van de ontsluiting van storage en de aansluiting op een back-upinfrastructuur.
03 Stel een overzicht op van ondersteunende communicatieprotocollen voor beheer.
Gebruik SSH, SCP, SFTP (niet FTP), https (niet http).
04 Stel een overzicht op van ondersteunende applicaties voor beheer.
05 Leg vast op welke wijze beheerders toegang krijgen tot de beheeromgeving.

Verdieping

Toegepaste beheermechanismen

Maak gebruik van bewezen standaardprotocollen die geen beveiligingsrisico's bevatten of waarvan de beveiligingsrisico's bekend en beheersbaar zijn. Het is dan ook noodzakelijk om vooraf vast te stellen welke beheermechanismen juist wel en welke juist niet toegepast mogen worden. Maak gebruik van versleutelde beheermechanismen en verbied verbindingen die de informatie in clear-text (in onversleutelde vorm) over het netwerk versturen. Voorbeelden van veilige verbindingen zijn:

» Secure Shell (SSH) in plaats van Telnet;
» Secure Copy (SCP), SSH File Transfer Protocol (SFTP) of FTP over SSL (FTPS) in plaats van File Transfer Protocol (FTP);
» https in plaats van http voor webinterfaces (zie ook B.04).

Beheerderstoegang tot het beheerdomein

Er moet vastgesteld worden hoe beheerders toegang krijgen tot het beheerdomein. Hier zijn verschillende mogelijkheden voor:

» Implementeer beheerclients in het beheerdomein, die alleen te gebruiken zijn in een afgeschermde ruimte. Beheer over de omgeving kan alleen plaatsvinden via deze fysiek afgeschermde beheerclients.
» Implementeer beheerclients in het beheerdomein die op basis van een remote interface (bijvoorbeeld Citrix of Microsoft RDP) te benaderen zijn voor een beperkte groep werkstations in het interne netwerk. Beheerders maken vanaf hun werkstation in het LAN een verbinding met de beheerclients en kunnen vervolgens via deze beheerclients het beheer over de omgeving uitvoeren.
» Implementeer een apart beheer-LAN binnen het interne netwerk en sta verbindingen richting het beheerdomein alleen toe vanuit dit beheer-LAN.
» Implementeer een Virtual Privat Network (VPN)-tunnel op het moment dat het beheer remote via het internet wordt uitgevoerd. Een VPN-tunnel kan natuurlijk ook toegepast worden als het beheer vanaf het bedrijfsnetwerk wordt uitgevoerd.

U/NW.06 Hardening van netwerken

Omschrijving

De hardening van netwerken is het resultaat van de toepassing van het hardeningsproces (zie richtlijn B.10).
De meeste systemen voeren een beperkt aantal functies uit. Het is mogelijk om het aantal potentiële aanvallen te verminderen door het systeem te ontdoen van onder andere software, gebruikersaccounts en diensten die niet gerelateerd en vereist (strikt noodzake-

60 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-continuiteit-van-online-diensten.html

lijk) zijn voor het functioneren van het systeem. Wanneer dat niet mogelijk is, moeten alle niet strikt noodzakelijke faciliteiten zijn uitgeschakeld. Systeem hardening is een leverancier specifiek proces, aangezien de verschillende leveranciers het systeem op verschillende manieren configureren en voorzien van verschillende diensten tijdens het standaard (default) installatie proces.
Voorbeelden zijn:

» Indien (externe) systemen, zoals webservers en mailservers 'reclame' maken voor hun type en versie, wordt het een aanvaller makkelijker gemaakt om bekende zwakke plekken van deze systemen te exploiteren.
» Systemen die onnodige diensten draaien en poorten open hebben die niet open hoeven te staan zijn makkelijker aan te vallen omdat deze diensten en poorten mogelijkheden bieden om het systeem aan te vallen.

Bij het hardenen van het systeem is een belangrijke strategie om de communicatiemogelijkheden van het systeem tot een minimum (het strikt noodzakelijke) te beperken. Eén van de manieren om dit te bereiken is door onnodige services onbereikbaar te maken door ze te verwijderen of uit te schakelen. Door benodigde services in kaart te brengen en vervolgens de afhankelijkheden te bepalen, kom je tot een minimale lijst van services die op het systeem moeten staan. Alle overige services kunnen het beste worden verwijderd of uitgeschakeld. Bedenk dat niet-actieve maar wel aanwezige services op een systeem uiteindelijk toch tot een kwetsbaar systeem kunnen leiden aangezien 'lekke' programmacode op het systeem aanwezig is. Veiliger is het daarom om onnodige services volledig van het systeem te verwijderen.

Beveiligingsrichtlijn U/NW.06

Hardening van netwerken configureren

Richtlijn (wie en wat)
Voor het configureren van netwerken is een hardeningrichtlijn beschikbaar.

Doelstelling (waarom)
Beperken van het netwerkverkeer tot hetgeen noodzakelijk is voor het correct functioneren van de geleverde ICT-diensten.

Risico
Bedoeld of onbedoeld negatief beïnvloeden van het netwerkverkeer, waardoor vertrouwelijkheid, integriteit en/of beschikbaarheid van het netwerkverkeer niet gegarandeerd is.

Classificatie
Hoog

Richtlijn 2012
Bo-5

Maatregelen

hardeningrichtlijn

01 Houd een actueel overzicht bij van de noodzakelijke netwerkprotocollen, -poorten en -services.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08).
02 Schakel op de netwerkcomponenten alle netwerkprotocollen, -poorten en –services uit, behalve de noodzakelijke.
Bij voorkeur worden uitgeschakelde netwerkprotocollen, -poorten en -services geheel verwijderd.
03 Pas de (beveiligings)configuraties van netwerkprotocollen, -poorten en -services op de netwerkcomponenten aan conform richtlijnen.
04 Wijs op switches netwerkpoorten toe aan Virtual LANs (VLANs) op basis van het MAC-adres van de aangesloten systemen (port security).

Verdieping

Hardeningsmaatregelen op netwerkniveau

Onderstaand enkele voorbeelden van hardeningsmaatregelen op netwerkniveau:

» Sluit beheermogelijkheden zoveel mogelijk af. Bied webinterfaces voor beheerfuncties alleen aan via beheercompartimenten (zie richtlijn U/NW.05).
» Sta beheer alleen toe vanaf vooraf gedefinieerde ip-adressen.
» Maak gebruik van complexe wachtwoorden en/of sterke authenticatiemechanismen voor het uitvoeren van beheer op de componenten.
» Maak gebruik van logon banners.
Een logon banner verschijnt op het moment dat een gebruiker een beheersessie opstart met een netwerkcomponent. Deze banner bevat een waarschuwing die de toegangsvoorwaarden tot het systeem beschrijft. De banner kan daarnaast waarschuwen voor juridische acties wanneer de gebruiker misbruik van het systeem maakt.
» Maak gebruik van versleutelde verbindingen bij beheerwerkzaamheden.
Verbied verbindingen die de informatie in clear-text (in onversleutelde vorm) over het netwerk versturen. Maak gebruik van Secure Shell (SSH) in plaats van Telnet, Secure Copy (SCP), SSH File Transfer Protocol (SFTP) of FTP over SSL (FTPS) in plaats van File Transfer Protocol (FTP) en https in plaats van http voor webinterfaces.
» Harden het onderliggende besturingssysteem.
Veel leveranciers leveren netwerkcomponenten in de vorm van appliances waarop weinig extra hardeningsmaatregelen mogelijk zijn. In de gevallen dat een netwerkcomponent echter niet gebaseerd is op een appliance, is het van belang dat je het onderliggende systeem hardent (zie richtlijnen met betrekking tot platformbeveiliging).
» Besteed voldoende aandacht aan de beveiligingsconfiguratie van netwerkservices en -protocollen: Simple Network Management Protocol (SNMP), Network Time Protocol (NTP), SYSLOG, Trivial FTP (TFTP), finger en routeringsprotocollen zoals Border Gateway Protocol (BGP) en Open Shortest Path First (OSPF).
» Schakel alle ongebruikte protocollen, services en netwerkpoorten uit (en verwijder ze).
Op deze wijze wordt de kans op misbruik via niet noodzakelijke protocollen, services en netwerkpoorten voorkomen.
Voorbeelden van protocollen die veelal standaard zijn ingeschakeld op netwerkcomponenten maar in veel gevallen niet nodig zijn, zijn Cisco Discovery Protocol (CDP) en Spanning Tree Protocol (STP). Bedenk dat niet-actieve maar wel aanwezige services op een systeem uiteindelijk toch tot een kwetsbaar systeem kunnen leiden aangezien 'lekke' programmacode op het systeem aanwezig is. Veiliger is het daarom om onnodige services volledig van het systeem te verwijderen.
» Maak op switches gebruik van Virtual LANs (VLAN) en beperk de toegang tot netwerkpoorten op basis van MAC-adres (port security).

Harden de (externe) DNS-infrastructuur

Door de vitale rol die het Domain Name System (DNS[61]) speelt in het bereikbaar houden van webapplicaties, verdient de beveiliging van DNS-services extra aandacht. Door de DNS-infrastructuur te hardenen, wordt DNS-misbruik voorkomen. Aandachtspunten bij het beveiligen van DNS-services zijn:[62]

» Maak gebruik van de meest recente software (zie ook richtlijn C.09 Patchmanagement), zodat het misbruik van bekende beperkingen[63] en kwetsbaarheden[64] zoveel mogelijk wordt voorkomen. Het maskeren van oudere versies door bijvoorbeeld het blokkeren van 'hostname.bind' queries is niet afdoende, aangezien er tal van andere manieren zijn om de versie van uw software te achterhalen (DNS-fingerprintingtechnieken).
» Overweeg een onderscheid te maken tussen 'authoritative nameservers' (waar de domeinnamen/zonefiles op draaien) en 'recursive resolvers' (waar client-systemen hun DNS-vragen aan stellen). Sommige DNS-software kan beide functies combineren, maar het is goed dat u zich bewust bent van het onderscheid.
» Zorg dat alleen geautoriseerde systemen een zonetransfer kunnen uitvoeren van authoritative nameservers. Doorgaans betekent dit dat alleen primaire en secundaire nameservers dit onderling mogen. Dit kan door in de configuratie de betreffende ip-adressen op te geven. Eventueel kan dit extra beveiligd worden via TSIG (RFC2845[65]). Zonetransfers blokkeren door TCP-poort 53 te blokkeren op de firewall, is niet de geëigende methode. TCP-poort 53 is een essentieel onderdeel van het DNS-protocol en dient enkel te worden geblokkeerd in de firewall als daar zwaarwegende redenen voor zijn. Blokkeer het in geen geval als manier om zonetransfers te voorkomen (daarvoor zijn andere manieren) en blokkeer het evenmin wanneer op de authoritative nameservers gebruik wordt gemaakt van DNSSEC of wanneer DNS-antwoorden om een andere reden groter (kunnen) zijn dan 512 bytes. Blokkeer TCP-poort 53 ook niet op resolvers.
» Maak gebruik van meerdere authoritative nameservers per zone en plaats deze netwerk-topologisch van elkaar gescheiden. Zodoende is de kans groter dat domeinnamen bereikbaar blijven bij gedeeltelijke uitval van uw netwerk of servers. Wanneer de impact van een DDoS-aanval op nameservers groot is en het risico daarop niet ondenkbaar, maak dan de authoritative-nameserver-infrastructuur nog robuuster. Met meer servers, al dan niet op basis van 'DNS Anycast' (derden kunnen dit leveren als commerciele dienst). Maak ook gebruik van minimaal twee resolvers.
» Overweeg maatregelen tegen DNS-rebindingaanvallen, door resolvers dusdanig te configureren dat zij nooit externe domeinnamen zullen resolven naar interne ip-adressen.
» Maak gebruik van DNSSEC[66,67] (DNS Security Extensions) hiermee kan de authenticiteit van DNS-antwoorden worden gewaarborgd. Hiermee wordt voorkomen dat deze onderweg worden gemanipuleerd ('Kaminsky aanval' of 'DNS cache pollution'[68]).Op authoritative nameservers worden DNS-gegevens met DNSSEC voorzien van een waarmerk, een digitale handtekening. Deze worden aan de kant van de resolvers gevalideerd (let op: vergeet ook daar niet om DNSSEC te activeren).
» Wanneer u beslist geen zonetransfers wilt toestaan, moet u in geval van DNSSEC niet kiezen voor Next Secure (NSEC)[69] (kies in plaats daarvan voor NSEC3, waarmee het zogenaamde 'zone walking' of 'zone enumeration', dat kenmerkend is voor NSEC, aanzienlijk wordt bemoeilijkt).
» Zorg dat resolvers alleen ter beschikking staan aan uw (interne) gebruikers en stel ze in geen geval open voor de rest van het internet.
» Beperk de beheerderstoegang tot nameservers en laat alleen de noodzakelijke beheerders toe (zie ook richtlijn B.02). Overweeg eventueel gescheiden systemen, waar uitsluitend DNS-beheerders toegang toe krijgen.
» Verwijder onnodige records uit de zone. Dergelijke records

61 Zie voor meer informatie https://www.sidn.nl/ en http://www.iana.org/
62 Aanvullende informatie over de manier waarop men DNS kan beveiligen is te vinden in de publicatie 'Secure Domain Name System (DNS) Deployment Guide' van het National Institute of Standards and Technology (NIST) <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf>.
63 https://www.dns-oarc.net/oarc/services/dnsentropy
64 http://www.dnssec.nl/wat-is-dnssec/faq.html#kaminsky
65 http://www.ietf.org/rfc/rfc2845.txt
66 http://www.dnssec.nl/home.html
67 DNSSEC staat op de 'pas-toe-of-leg-uit' lijst http://forumstandaardisatie.nl/dnssec. Overheden zijn verplicht de open stan-daarden, die op de lijst met 'pas toe of leg uit'-standaarden staan, bij aanschaf of (ver)bouw van ICT-systemen/-diensten te eisen ('pas toe'). is in die zin verplicht gesteld.
68 http://www.iana.org/about/presentations/davies-viareggio-entropyvuln-081002.pdf
69 http://www.dnssec.nl/wat-is-dnssec/faq.html#nsec_nsec3

(bijvoorbeeld HINFO- en TXT records) leveren een kwaadwillende extra informatie.
» Ruim zones waarvoor u niet meer verantwoordelijk bent, op van de authoritative nameservers.
» Houd het (netwerk)verkeer op nameservers nauwlettend in de gaten (zie ook richtlijnen C.06 en C.07). Wees alert op afwijkende patronen in logging en overweeg het gebruik van een Intrusion Prevention System (IPS). Omdat DNS vaak open staat in firewalls, wordt het bijvoorbeeld door kwaadwillenden misbruikt als manier om interne informatie naar buiten weg te sluizen. Maar het kan ook zijn dat kwaadwillenden uw name servers misbruiken bij een DDoS aanval gericht aan derden (zogenaamde 'DNS amplification attack'[70]). Met monitoring kunt u ook zien of men een 'Kaminsky-aanval' probeert op uw resolvers.

U/NW.07 Netwerktoegang tot webapplicaties

Omschrijving

Als webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk moet hiervoor een koppeling tot stand gebracht worden, wat een extra verkeersstroom introduceert (zie richtlijn U/NW.03). Deze extra verkeersstroom mag natuurlijk geen (nieuwe) beveiligingsrisico's introduceren.

Er moet worden voorkomen dat beveiligingsbeperkingen die zijn opgelegd door componenten in de DMZ (onbedoeld) door interne medewerkers worden omzeild. Gebruikers binnen de organisaties moeten dezelfde netwerkmaatregelen voorgeschoteld krijgen als gebruikers van buiten de organisatie. Het is dan ook van belang om vastgestelde routepaden (zie richtlijn U/NW.03) ook voor intern netwerkverkeer te bekrachtigen. Hierdoor zal intern netwerkverkeer in grote lijnen dezelfde weg moeten volgen als internetverkeer, met als gevolg dat intern netwerkverkeer op dezelfde plek de DMZ moet binnenkomen als regulier internetverkeer. Dit geldt voor productieverkeer en niet voor netwerkverkeer in verband met beheerdoeleinden, zoals in richtlijn U/NW.05 beschreven.

Beveiligingsrichtlijn U/NW.07

Netwerktoegang tot webapplicaties garanderen

Richtlijn (wie en wat)
De opzet van het netwerk garandeert dat alle gebruikers langs dezelfde netwerkpaden toegang krijgen tot webapplicaties, ongeacht hun fysieke locatie.

Doelstelling (waarom)
Voorkom (nieuwe) beveiligingsrisico's omdat de webapplicaties ook bereikbaar moeten zijn vanaf het interne netwerk voor gebruikers binnen de organisatie.

Risico
Een aanvaller krijgt mogelijkheden om de toegangsbeveiliging voor externe gebruikers te omzeilen.

Classificatie
Hoog

Richtlijn 2012
B1-3

Maatregelen

netwerkpaden

01 Bied gebruikers slechts één netwerkpad om een webapplicatie te bereiken.
Dit blijkt uit het netwerkontwerp.
Het is toegestaan voor verschillende gebruikersgroepen van verschillende (fysieke) netwerkpaden gebruik te maken, zolang deze qua logische opzet maar identiek zijn. Dit kan bijvoorbeeld een oplossing zijn in geval van (zeer) drukbezochte websites.

U/NW.08 Netwerkarchitectuur

Omschrijving

De architectuur van netwerken beschrijft de functionele en beveiligingssamenhang en legt de relatie met (de architectuur van) het algemene ICT-landschap. Vanuit een eenduidig gemeenschappelijk beeld worden alle netwerkcomponenten conform deze architectuur gerealiseerd. Hiervoor worden de richtlijnen, instructies en procedures van richtlijn U/NW.01 toegepast. Op deze manier wordt zeker gesteld dat iedere netwerkcomponent aan de vereiste functionele en beveiligingsdoelen bijdraagt.

De architectuur documenteert gemaakte ontwerp en inrichtingskeuzen en verantwoordt en onderbouwt deze keuzen. Het architectuurdocument beperkt zich dus niet tot het vastleggen wat de huidige situatie (as-is) is, maar ook waarom deze zo is, dus wat de noodzaak van toepassing is. Om dit gefundeerd te onderbouwen zullen er verwijzingen naar functionele eisen, risicoanalyses (zie richtlijn B.03/01), best practices en (mogelijke) alternatieven opgenomen moeten worden. Alle gedocumenteerde ontwerpen en inrichtingskeuzen moeten te herleiden zijn naar functionele eisen. Documentatie speelt ook een (belangrijke) rol bij het bepalen van de impact van wijzigingen en het voorkomen van ontwerpbeslissingen (fouten). Documentatie moet dan ook na elke wijziging worden bijgewerkt en oude documentatie moet worden gearchiveerd. Dit geldt zowel voor systeem- als gebruikersdocumentatie.

Documentatie moet goed leesbaar zijn, voorzien zijn van een datum (evenals de revisiedata), een eigenaar hebben, op een ordelijke manier worden onderhouden en gedurende een bepaalde periode worden bewaard. Er moeten procedures en verantwoordelijkheden worden vastgesteld en bijgehouden voor het opstellen en aanpassen van documentatie.

Documentatie kan gevoelige informatie bevatten en er moeten dan ook maatregelen zijn getroffen om de documentatie te beveiligen tegen ongeautoriseerde toegang (inzien en wijzigen).

De documentatie beschrijft onder andere:
» hoe wordt omgegaan met risicomanagement, de benodigde bedrijfsmiddelen, de geïmplementeerde maatregelen en noodzakelijke mate van zekerheid, kortom de vastgelegde en vastgestelde procedures en processen;
» de plaatsing van servers en aansluiting van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken, zodat de werking van de ICT-infrastructuur begrijpelijk is en de impact van wijzigingen goed kunnen worden bepaald;
» de (beveiligings)instellingen van de ICT-componenten, zodanig dat duidelijk is waarom voor bepaalde instellingen gekozen is (verantwoording en onderbouwing). Hierbij wordt speciale aandacht besteed aan de defaultwaarden voor systeeminstellingen.

Voor elke maatregel wordt documentatie onderhouden, daarnaast wordt afhankelijk van de gevoeligheid van de webapplicatie regelmatig het bestaan van maatregelen gecontroleerd en gedocumenteerd. De mate van compliance wordt aan de verantwoordelijke voor de webapplicatie en de beveiligingsfunctionaris gerapporteerd.

Beveiligingsrichtlijn U/NW08

Netwerkarchitectuur vastleggen

Richtlijn (wie en wat)
Voor het implementeren, integreren en onderhouden van netwerken zijn architectuurvoorschriften, beveiligingsvoorschriften en de benodigde documentatie beschikbaar.

Doelstelling (waarom)
Een netwerklandschap bieden dat een betrouwbare verwerking garandeert.

Risico
Een aanvaller krijgt mogelijkheden om de toegangsbeveiliging voor externe gebruikers te omzeilen.

Classificatie
Hoog

Richtlijn 2012
-

Maatregelen

architectuurvoorschriften

01 Onderhoud architectuurvoorschriften actief.
Zorg dat dit document onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08).

beveiligingsvoorschriften

02 Stel hardeningrichtlijnen op voor netwerken, aantoonbaar afgeleid uit de architectuur.
Het gaat hier om de aantoonbare, navolgbare relatie tussen wat de architectuur beschrijft en de concretisering in richtlijnen. Bij de registratie van de inrichting wordt deze lijn doorgetrokken naar de daadwerkelijke configuratie en getroffen maatregelen.
Zie ook U/NW.06.
03 Stel inrichtingsrichtlijnen op voor registratie van beveiligingsevents (logging) , aantoonbaar afgeleid uit de architectuur.
04 Stel inrichtingsrichtlijnen op voor de restricties van faciliteiten/utilities en de uitschakeling van features en poorten van netwerkcomponenten.
05 Stel richtlijnen op voor periodieke security-updates, herstelbaarheid van netwerkcomponenten en bescherming (van de stroomvoorziening) van kritieke netwerkcomponenten (zoals UPS/no-breaks voor de stroomvoorziening op de core-switches).

documentatie

06 Documenteer de plaatsing van servers en aansluitingen van interne netwerkcomponenten en netwerkkoppelingen met externe netwerken.
De documentatie is begrijpelijk en voorzien van relevante schema's, zodat de werking van de ICT-infrastructuur duidelijk is en de impact van wijzigingen goed kan worden bepaald.

70 Zie NCSC factsheet FS-2013-03 "DNS-amplificatie: Laat uw deur niet wagenwijd openstaan" https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-dns-amplificatie.html

Beheersingsdomein (control)

Doelstelling

De doelstelling van het beheersingsdomein is er voor te zorgen en/of vast te stellen dat:

» de webapplicatie-omgeving afdoende is ingericht voor het leveren van het gewenste niveau van webapplicatie-diensten,
» het juiste beveiligingsniveau van technische componenten op de lagen toegangsvoorziening, webapplicatie, platformen en webservers en netwerken wordt gegarandeerd.

Inleiding

Dit houdt onder meer in dat een adequate beheerorganisatie moet zijn ingericht, waarin beheerprocessen zijn vormgegeven. De beheerprocessen die voor de webapplicatie relevant worden beschouwd zijn:

Compliancemanagement
Dit is een proces waarbij wordt vastgesteld in hoeverre aan de wettelijke, organisatorische en technische verplichtingen wordt voldaan en/of in hoeverre die worden nagekomen.

Vulnerability assessment
Dit is een proces waarbij met behulp van technische hulpmiddelen wordt nagegaan in hoeverre in de ICT-componenten kwetsbaarheden voorkomen waarvan ongeautoriseerden gebruik zouden kunnen maken.

Penetratietest
Dit is een specifieke vorm vulnerability-assessment. Het is een proces waarbij met behulp van technische hulpmiddelen specifieke componenten of specifieke delen van de ICT-infrastructuur op zwakheden gecontroleerd worden.

Technische controlefunctie
Dit is een proces waarbinnen verschillende technische activiteiten (geautomatiseerd danwel niet geautomatiseerd) worden uitgevoerd gericht op de gehele ontwikkelcyclus van een webapplicatie.

Logging
Dit is een proces van registreren (loggen) van informatie over menselijke en systeemactiviteiten voor analyse- en bewakingsdoeleinden.

Monitoring
Dit heeft te maken met bewaken (monitoring), detecteren van gebeurtenissen (detectie), alarmeren over de gebeurtenissen (alerting), analyseren van de vastgelegde informatie (auditing) en het rapporteren van de resultaten (reporting).

Wijzigingenbeheer
Dit is een beheerproces voor het controleren en beheren van wijzigingsvoorstellen en de eventuele doorvoering van wijzigingen voor alle configuratie-items van de ICT-infrastructuur.

Patchmanagement
Dit is een proces dat ervoor zorgt dat ICT-systemen systematisch voorzien worden van de vereiste versie van patches (systeemwijzigingen).

Beschikbaarheidbeheer
Dit is een beheerproces met alle activiteiten om de beschikbaarheid van de geleverde webdiensten te waarborgen en voorzieningen te treffen om de beschikbaarheid binnen de afgesproken grenzen bij storingen en calamiteiten te behouden.

Configuratiebeheer
Dit is een beheerproces voor het identificeren van de configuratie-items, het registreren van de configuratie-items inclusief de status en de verificatie van de volledigheid en juistheid van configuratie-items.

Deze beheerprocessen zorgen ervoor dat ICT-componenten steeds veilig zijn geconfigureerd en dat het gewenste beveiligingsniveau behouden blijft. Deze ICT-beheerprocessen moeten op basis van servicemanagementbeleid zijn ingericht.

Risico's

Door het ontbreken van noodzakelijke maatregelen binnen het beheersingsdomein is het niet zeker dat de webapplicatie-omgeving blijvend aan de beoogde beveiligingsvoorwaarden voldoet en dat de governance van die omgeving toereikend is ingericht.

Kwetsbaarheden en bedreigingen

In bijlage E wordt een overzicht gegeven van de mogelijke kwetsbaarheden en bedreigingen die van belang zijn voor webapplicaties. De volgende kwetsbaarheden en bedreigingen spelen een rol op deze laag: ontbreken van toezicht, de gehele keten wordt niet meegenomen waardoor de impact onbekend is en het gebrek aan coördinatie en samenwerking.

Beveiligingsrichtlijnen

Binnen het beheersingsdomein worden onderstaande richtlijnen beschreven en per richtlijn worden conformiteitsindicatoren en de betreffende maatregelen uitgewerkt.

» Servicemanagementbeleid (C.01)
» Compliancemanagement (C.02)
» Vulnerability assessments (C.03)
» Penetratietestproces (C.04)
» Technische controlefunctie (C.05)
» Logging (C.06)
» Monitoring (C.07)
» Wijzigingenbeheer (C.08)
» Patchmanagement (C.09)
» Beschikbaarheidbeheer (C.10)
» Configuratiebeheer (C.11)

C.01 Servicemanagementbeleid

Omschrijving

Het servicemanagementbeleid geeft richting aan de wijze waarop de beheersingsorganisatie moet zijn ingericht en de wijze waarop deze moet functioneren. Hiernaast bestaan procedures en instructies voor de ondersteuning van de specifieke beheerprocessen. De beheerorganisatiestructuur geeft de samenhang van de ingerichte processen weer.

Beveiligingsrichtlijn C.01

Servicemanagementbeleid formuleren

Richtlijn (wie en wat)
Het servicemanagementbeleid formuleert richtlijnen voor beheerprocessen, controleactiviteiten en rapportages ten behoeve van het beheer van ICT-diensten.

Doelstelling (waarom)
Effectieve beheersing, door samenhangende inrichting van processen en controle hierover door middel van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.

Risico
Onvoldoende mogelijkheden om vast te stellen of de getroffen maatregelen in voldoende mate invulling geven aan beleidsdoelstellingen en onvoldoende mogelijkheden om de beheerorganisatie op de juiste wijze in te richten en bij te sturen.

Classificatie
Midden

Richtlijn 2012
-

Maatregelen

richtlijnen voor beheerprocessen

01 Stel richtlijnen op voor de inrichting van de servicemanagementorganisatie.
02 Stel een beschrijving op van de relevante beheerprocessen.
03 Richt de processen in conform een vastgestelde cyclus.
Bijvoorbeeld: registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.
04 Gebruik geautomatiseerde middelen voor effectieve ondersteuning van beheerprocessen.

richtlijnen voor controleactiviteiten en rapportages

05 Stel richtlijnen op voor het uitvoeren van registratie, statusmeting, monitoring, analyse, rapportage en evaluatie.
06 Stel richtlijnen op voor het uitvoeren van controle-activiteiten ten aanzien van identiteit en toegangsbeheer, webapplicatie, platformen en webservers en netwerken.
Hieronder vallen ook penetratietests.
07 Stel richtlijnen op voor het evalueren van de organisatie, kwaliteit, effectiviteit, borging en informatievoorziening van de beheerprocessen.
08 Leg de taken, verantwoordelijkheden en bevoegdheden (TVB's) van beheerders vast.
09 Leg de relaties met ketenpartijen vast.

C.02 Compliancemanagement

Omschrijving

Compliancemanagement richt zich op het naleven van de verplichtingen die voortkomen uit (a) wet- en regelgeving en (b) door de organisatie zelf gekozen standaarden en richtlijnen.

Vanuit beveiligingsoptiek is het van belang dat via policycompliancechecks wordt gecontroleerd of de ICT-omgeving na verloop van tijd nog steeds voldoet aan de vastgestelde en geïmplementeerde security policies, die voortvloeien uit deze verplichtingen (naleving).

De resultaten van de policycompliancecheck worden vastgelegd in de vorm van een rapportage. Wanneer duidelijk wordt dat geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen, is opvolging met corrigerende acties noodzakelijk. De literatuur kent dit samenstel als een PDCA-cyclus.[71]

Wanneer uitvoeren?

De frequentie voor het uitvoeren van policycompliancechecks dient voort te komen uit het risicoprofiel. Er zijn meerdere momenten waarop een policycompliancecheck zinvol is. Enerzijds als onderdeel van een regulier, periodiek controleproces, anderzijds gekoppeld aan ontwikkelen in verdedigings- en aanvalstechnieken (dreigingen), veranderingen in beleid en techniek en optreden van incidenten.

Periodieke controles (maandelijks/per kwartaal/halfjaarlijks/jaarlijks) dienen om bestaande systemen te testen op naleving van de security policy en/of als onderdeel van de PDCA-cyclus.

71 Plan-Do-Check-Act.

In de loop van de tijd veranderen technieken en inzichten. Ook zal het ICT-landschap gaandeweg veranderen. Deze ontwikkelingen kunnen aanleiding zijn het beleid bij te stellen en de controles aan te passen. Elke (groep van) verandering(en) is aanleiding om een policycompliancecheck uit te voeren.

Tot slot zullen er (vermoedens van) incidenten zijn, die aanleiding geven tot het uitvoeren van ad hoc policycompliancechecks.

Beveiligingsrichtlijn C.02

Compliancemanagement vastleggen

Richtlijn (wie en wat)
De inrichting en de beveiliging van de webapplicaties (scope) wordt procesmatig en procedureel gecontroleerd (compliancechecks) op basis van vastgestelde beveiligingsrichtlijnen en een vastgestelde webapplicatie-architectuur.

Doelstelling (waarom)
Vaststellen in hoeverre de implementatie van de webapplicatie voldoet aan de vooraf vastgestelde beveiligingsrichtlijnen en geldende wet- en regelgeving.

Risico
Aansprakelijkheid in geval van beveiligingsincidenten en niet halen van bedrijfs- en beveiligingsdoelstellingen.

Classificatie
Midden

Richtlijn 2012
Bo-10

Maatregelen

scope

01 Zorg voor een beschrijving van de webapplicatie-omgeving, waarin de configuratie-elementen genoemd worden.
De scope beperkt zich tot dat deel van de totale keten, dat onder de formele verantwoordelijkheid van de organisatie valt.
Indien er sprake is van uitbesteding[72] valt ook het uitbestede deel van de keten onder de formele verantwoordelijkheid van de uitbestedende organisatie. Met de dienstverlener dienen sluitende procedurele en technische afspraken gemaakt te worden om de vereiste waarborgen tot stand te brengen. In die zin mag er geen verschil zijn met de situatie waarbij alles in eigen huis gerealiseerd is.
De scope dient aantoonbaar gebaseerd te zijn op het actuele ICT-landschap.

procesmatig en procedureel

02 Stel een planning op voor de reguliere policycompliancechecks ten aanzien van de webapplicatie-omgeving.
De planning toont de activiteiten die zullen worden uitgevoerd (wie, wat en wanneer).
Policycompliancechecks betreffen zowel de procedurele als de technische compliance.
03 Registreer de uitvoering van en rapporteer over de resultaten van de periodieke policycompli-ancechecks.
De registratie bevat in ieder geval:
» *het controlemoment;*
» *de aanleiding voor de controle;*
» *wie de controle heeft uitgevoerd;*
» *de omgeving waarop de controle is uitgevoerd;*
» *de middelen waarmee de controle is uitgevoerd.*
Indien voor het laatste gebruikgemaakt is van programmatuur: naam, versie en parameters.
04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken over de afwijkingen.
Afwijkingen worden toegelicht, waarbij de ernst van de afwijking wordt uitgedrukt in een risico voor de organisatie en haar partners. Verbetervoorstellen worden geprioriteerd op basis van dit risico.
05 Beleg implementatieacties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.
Het gaat om de daadwerkelijke uitvoering. Dit vereist een registratie van verbeteringen die al zijn uitgevoerd en een planning (wie, wat en wanneer) van nog uit te voeren verbeteringen.

C.03 Vulnerability-assessments

Omschrijving

Kwaadwillenden maken gebruik van kwetsbaarheden en zwakheden in ICT-componenten (zowel ICT-systemen als netwerken). Zonder inzicht in de huidige stand van zaken, tast de beheerder in het duister en kan hij niet goed anticiperen op nieuwe ontwikkelingen. Vragen die hierbij een rol spelen:
» Hoe is de ICT-omgeving opgebouwd en geconfigureerd?
» Wat zijn bekende kwetsbaarheden en zwakheden?

Vulnerability assessments zijn noodzakelijk om zwakheden van in ICT-componenten op verschillende lagen van de ICT-infrastructuur vast te stellen.

72 Onder uitbesteding vallen nadrukkelijk ook cloud(-achtige) diensten als software-as-a-service (SaaS), platform-as-a-service (PaaS) en infrastructure-as-a-service (IaaS).

Bij een vulnerability assessment (VA) wordt met behulp van een scanner een (geautomatiseerde) scan uitgevoerd op een van te voren bepaald aantal ip-adressen. Hierbij worden de servers en services onderzocht op alle bekende kwetsbaarheden en zwakheden en worden de gevonden kwetsbaarheden en zwakheden gerangschikt naar risico (hoog, midden en laag). De te analyseren ip-adressen worden door de beheerder opgegeven of automatisch bepaald door een netwerkscan. Door een VA uit te voeren over de ICT-componenten (zowel op ICT-systemen als op netwerken), komen aanwezige kwetsbaarheden en zwakheden naar boven en worden deze weergegeven in een rapportage.

Netwerkgebaseerde VA's worden uitgevoerd door netwerkscanners. Netwerkscanners zijn in staat om open poorten te detecteren, services te identificeren die op deze poorten draaien, mogelijke kwetsbaarheden van deze services te detecteren en aanvallen op deze services te simuleren.

Hostgebaseerde VA's worden uitgevoerd door hostscanners. Hostscanners zijn in staat om kwetsbaarheden op systeemniveau te herkennen, waaronder onjuist toegekende rechten en configuratiefouten. In tegenstelling tot de netwerkscanners, is voor hostscanners een account op de betreffende host (computersysteem) nodig met voldoende toegangsrechten.

Op basis van de rapportage kan de organisatie een afweging maken welke kwetsbaarheden relevant zijn en verholpen moeten worden en welke geaccepteerd worden. Het kan voorkomen dat bepaalde kwetsbaarheden niet verholpen kunnen worden omdat dan de webapplicatie niet meer functioneert.

De frequentie voor het uitvoeren van vulnerability assessments dient vastgesteld te worden op basis van het risicoprofiel. Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Beveiligingsrichtlijn C.03

Vulnerability-assessments uitvoeren

Richtlijn (wie en wat)
Vulnerability assessments (security scans) worden procesmatig en procedureel uitgevoerd op de ICT-componenten van de webapplicatie (scope).

Doelstelling (waarom)
Identificeren van de kwetsbaarheden en zwakheden in de ICT-componenten van de web applicatie zodat tijdig de juiste beschermende maatregelen kunnen worden getroffen.

Risico
Onvoldoende zicht op aanwezige kwetsbaarheden en zwakheden van ICT-componenten, onvoldoende zicht op de effectiviteit van reeds getroffen maatregelen en onvoldoende mogelijkheden om te kunnen anticiperen op de nieuwe dreigingen.

Classificatie
Hoog

Richtlijn 2012
Bo-9

Maatregelen

procesmatig en procedureel

01 Stel een planning op voor het uitvoeren van reguliere vulnerability assessment van de webapplicatie-omgeving.
Vermeld hierin welke soort VA op welk moment (periode) uitgevoerd moet worden.

02 Registreer de uitvoering van de vulnerability assessments.
De registratie bevat in ieder geval (a) het VA-moment, (b) wie de VA heeft uitgevoerd, (c) de omgeving waarop de VA is uitgevoerd en (d) de middelen (naam, versie en parameters) waarmee de VA is uitgevoerd.

03 Stel rapportages op met de resultaten van de vulnerability assessments.
Maak gebruik van richtlijnen/format over de VA-rapportage. In zo'n rapportage-format is duidelijk vastgelegd welke informatie de rapportage moet bevatten.

04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken/eigenaren van systemen waarin kwetsbaarheden en zwakheden gevonden zijn.
Afwijkingen worden toegelicht, waarbij de ernst van de afwijking wordt uitgedrukt in een risico voor de organisatie en haar partners. Verbetervoorstellen worden geprioriteerd op basis van dit risico en er wordt een actielijst samengesteld.

05 Beleg implementatieacties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.
Het gaat om de daadwerkelijke uitvoering. Dit vereist een registratie van verbeteringen die al zijn uitgevoerd en een planning (wie, wat en wanneer) van nog uit te voeren verbeteringen.
Er is aantoonbaar follow-up gegeven; verbeteringen zijn doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen.

scope

06 Zorg voor een actueel overzicht van te onderzoeken componenten, zoals webapplicaties, webservers, netwerk(componenten) en ip-adressen.
Geef aan welke componenten in deze scope een rol spelen en hoe deze met elkaar samenhangen. Bijvoorbeeld: webapplicaties, webservers, netwerk(component) en ip-adressen.

07 Stel een overzicht op van kwaliteitseisen en –criteria waarover gerapporteerd moet worden.
De kwaliteitseisen en -criteria moeten gekoppeld zijn aan de componenten binnen de scope van de VA. Het wel of niet voldoen aan deze kwaliteitseisen en -criteria moet binnen de invloedsfeer van de organisatie liggen.

C.04 Penetratietestproces

Omschrijving

Penetratietestproces richt zich op het geven van inzicht in de mate waarin de ICT-componenten kwetsbaar is voor inbraken. Daarmee is een penetratietest een specifieke vorm van een vulnerablity assessment.

Penetratietestproces is een impliciet onderdeel van wijzigingsbeheer (zie richtlijn C.08), maar wordt in verband met de belangrijkheid afzonderlijk geadresseerd. Vanuit beveiligingsoptiek is het van belang dat wordt gecontroleerd of het mogelijk is de webapplicatie en/of de infrastructuur op enigerlei wijze binnen te dringen. Een penetratietest[73] (ook pentest genoemd) is daarom een waardevolle aanvulling op de beveiliging van webapplicaties. Het uitvoeren van een penetratietest kan echter een uitdaging zijn. De aan de test verbonden risico's moeten minimaal zijn, de kwaliteit van de test optimaal en resultaten moeten bruikbaar zijn om kwetsbaarheden effectief te verhelpen.

Penetratietests kennen verschillende varianten zoals black box tests, grey box, white box of crystal box. Het verschil zit onder meer in de hoeveelheid kennis en achtergrondinformatie die de tester krijgt. Als een tester minimale voorkennis heeft, is er sprake black box; krijgt een tester van tevoren inzicht in alle aspecten van de systeemarchitectuur, dan wordt het een white box genoemd. Een grey box zit tussen een white box en black box in. Met crystal box wordt meestal bedoeld dat de tester ook de broncode van de applicatie heeft en beschikt over alle mogelijke configuratie-informatie.

Ook het testperspectief leidt tot varianten. Wordt er getest vanuit het perspectief van een interne medewerker, dan gaat het om een 'privileged test'. Het perspectief van een aanvaller vanaf internet heet een 'non-privileged test'.

Er kunnen meerdere momenten zijn waarop een penetratietest zinvol is:
» in de acceptatiefase van een nieuw systeem of een nieuwe applicatie;
» bij significante wijzigingen van een belangrijk systeem of een belangrijke applicatie;
» periodiek (jaarlijks/tweejaarlijks), om bestaande systemen te testen op nieuwe inbraaktechnieken en/of als onderdeel van de PDCA-cyclus;
» als er een andere reden is om te denken dat de beveiliging van een systeem minder goed is dan gedacht;

De frequentie dient vastgesteld te worden op basis van het risicoprofiel. Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

De kwaliteit van de penetratietest wordt mede bepaald door de methodiek. Denk hierbij aan:
» stappenplan waarin de activiteiten in volgorde worden beschreven en op welke methodiek de aanpak is gebaseerd;
» testplan waarbij per test staat vermeld wat de risico's zijn.

Beveiligingsrichtlijn C.04

Penetratietestproces uitvoeren

Richtlijn (wie en wat)
Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de webapplicatie (scope).

Doelstelling (waarom)
Het verkrijgen van inzicht in de weerstand die een webapplicatie kan bieden aan pogingen om het te compromitteren (binnendringen of misbruiken van webapplicatie).

Risico
Onbekendheid met bestaande kwetsbaarheden en zwakheden, waardoor hiertegen geen actie ondernomen wordt.

Classificatie
Hoog

Richtlijn 2012
Bo-8

Maatregelen

procesmatig en procedureel

01 Plan het uitvoeren van reguliere penetratietests van de webapplicatie inclusief de infrastructuur waarop deze draait.
Een pentest moet ruim van tevoren gepland worden. Houd rekening met bijvoorbeeld de volgende aspecten:
» *Zijn er momenten waarop er niet getest mag worden?*
» *Vermijd kritieke periodes, zoals een pentest van een salarisverwerkend systeem aan het eind van de maand.*
» *Doe geen pentest als een systeem tijdens de test veranderingen ondergaat.*

73 Meer informatie en tips over het uitvoeren van penetratietests is na te lezen in de NCSC whitepaper 'pentesten doe je zo' https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/pentesten-doe-je-zo.html.

02 Registreer de uitvoering van de penetratietest.
03 Rapporteer over de resultaten van de penetratietest.
Het rapportageformat legt duidelijk vast welke informatie de rapportage moet bevatten.
De resultaten van de pentest worden vastgelegd in een vorm van een rapportage. Geef duidelijk aan welke informatie de rapportage moet bevatten, bijvoorbeeld:
» type penetratietest (white, grey, back of crystal box);
» het tijdstip waarop de test is uitgevoerd;
» de gebruikte applicaties (inclusief versienummer);
» de parameters die zijn gebruikt bij de tests;
» het ip-adres waarvandaan de test is uitgevoerd;
» op welke omgeving de penetratietest heeft plaatsgevonden (ontwikkel, test, acceptatie of productie);
» een toelichting per gevonden verbeterpunt;
» een inschatting van de prioriteit per verbeterpunt.
04 Communiceer de rapportages met verbetervoorstellen met verantwoordelijken/eigenaren van systemen waarin kwetsbaarheden en zwakheden gevonden zijn.
05 Beleg implementatie-acties en stel uitvoerings- of systeemdocumenten beschikbaar waaruit blijkt dat de verbetervoorstellen zijn geïmplementeerd.
Plan de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

scope

06 Definieer het object van onderzoek in een scopedefinitie.
Een ander belangrijke aspect is de inkadering van de test. Wat is het object van onderzoek?
» *Geef goed aan om welke componenten het gaat. Denk hierbij aan firewalls, databases, applicaties, et cetera.*
» *Geef goed aan om welke omgeving het gaat. Hoeveel systemen en apparaten moeten worden getest en zijn ze vergelijkbaar?*
» *Als u van het te testen object een ontwikkel-, test- en/of acceptatieomgevingen heeft, dan kan het verstandig zijn om één van die omgevingen voor de duur van de pentest precies zo in te richten als de productieomgeving en de test daarop laten plaatsvinden.*
» *Wordt de penetratietest van buiten via het internet (non- privileged) of vanaf het interne netwerk uitgevoerd (privileged)?*
Geef vooraf de diepgang van de penetratietest aan. Valt bijvoorbeeld het gebruiken van exploits binnen scope of niet? Wordt de scope beperkt tot de OWASP Top 10 [2], CWE/SANS Top 25 [14] of worden hier geen beperking aan gesteld?
Voer voorafgaand een risicoanalyse uit waaruit blijkt dat kwetsbaarheden in een systeem een groot risico zijn en vervolgens wordt dan de penetratietest uitgevoerd om in kaart te brengen welke kwetsbaarheden er zijn en hoe ze opgelost kunnen worden.
07 Stem de opdracht af met en accordeer deze door een voldoende gemandateerde vertegenwoordiger.
Essentieel in de (offerte)aanvraag is de opdrachtomschrijving met daarin een heldere onderzoeksvraag. Welke informatie moet de pentest opleveren; welke vraag moet beantwoord worden? Het moet voor aanbieders duidelijk zijn wat er van hen wordt verwacht. Denk hierbij aan de volgende vragen:
» *Is het mogelijk om toegang tot het systeem te krijgen?*
» *Is het mogelijk om, eenmaal binnengedrongen, toegang te verkrijgen tot vertrouwelijk materiaal?*
» *Kan een geautoriseerd gebruiker met beperkte toegangsrechten misbruik maken van een andere geautoriseerde gebruiker meer toegangsrechten?*
08 Zorg voor een vrijwaringsverklaring voor penetratietesters, met eventuele beperkingen beschikbaar.

C.05 Technische controlefunctie

Omschrijving

De technische controlefunctie betreft technische controleactiviteiten aangaande de webapplicatie. Deze controles kunnen zowel in ontwikkelfase als in de implementatiefase worden uitgevoerd. In de ontwikkelfase worden verschillende technische controles uitgevoerd, zoals:
» codereview tijdens ontwikkelingstrajecten om in een vroegtijdig stadium potentiële kwetsbaarheden te ontdekken;
» periodieke (geautomatiseerde) blackboxscan om te testen of er kwetsbaarheden in de webapplicatie bestaan.

Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Beveiligingsrichtlijn C.05

Technische controlefunctie evalueren

Richtlijn (wie en wat)
De functionaris verantwoordelijk voor de technische controlefunctie van de webapplicaties voert periodiek (technische) evaluaties van de beveiligingsfunctionaliteit van de webapplicaties uit.

Doelstelling (waarom)
Het vaststellen van de juiste werking van de webapplicaties en het tijdig signaleren van afwijkingen/kwetsbaarheden.

Risico
Geen inzicht in de status van de operationele implementatie en beveiliging van ICT-componenten.

Classificatie
Midden

Richtlijn 2012
B3-14, B3-15

Maatregelen

(technische) evaluaties

01 Voer periodiek reviews of geautomatiseerde scans op de volledige broncode uit.
Het scannen is mogelijk voor wie betrokken is bij het ontwikkeltraject en/of beschikt over de broncode van de programmatuur, door het uitvoeren van codereviews.
Als de software door een externe partij is ontwikkeld, dan wordt de broncode door die softwareleverancier beschikbaar gesteld of de softwareleverancier geeft hierover een verklaring van een onafhankelijke derde af.
Er is documentatie beschikbaar waaruit blijkt dat:
- *dat er een codereview is uitgevoerd;*
- *de bevindingen/rapportage van de codereview;*
- *op welke wijze de bevindingen verwerkt zijn.*

02 Voer periodieke (blackbox-)scans uit, waarbij de volledige functionaliteit van de webapplicatie geraakt wordt.
Er moet aantoonbaar follow-up worden gegeven; verbeteringen worden doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.
Zorg voor afspraken, met de leverancier, over het uitvoeren van een blackbox scan.

Verdieping

Codereview

Om een codereview uit te voeren zijn op hoofdlijnen twee mogelijkheden:
» Geautomatiseerd scannen van de broncode
Met behulp van geautomatiseerde tools scannen van de broncode (ook bekend als 'statische analyse') op zoek naar patronen die mogelijke kwetsbaarheden en zwakheden vormen.
» Handmatige codereview
Handmatige codereview bestaat uit het zoeken in en analyseren van de broncode op zoek naar patronen die mogelijke kwetsbaarheden en zwakheden vormen. Bij een handmatige codereview wordt de broncode gescand door een ander persoon dan de ontwikkelaar.

Deze aanpak, ook wel een whitebox scan of statische analyse genoemd, kan problemen aan het licht brengen die men via een blackbox scan niet zal ontdekken. Beter nog is het om de codereview in verschillende stadia van het ontwikkelproces uit te voeren om op die manier fouten in een vroeg stadium en dus vaak gemakkelijker, te kunnen verhelpen. Een codereview vergt over het algemeen meer inspanning dan een blackbox scan.

Tools voor het uitvoeren van geautomatiseerde codereviews bestaan er in vele soorten en maten. Onderstaande – niet uitputtende – lijst geeft enkele punten weer waarop een geautomatiseerde tool kan controleren:
» het afvangen van excepties;
» de mogelijkheid tot het genereren van buffer overflows;
» de aanwezigheid van type mismatches;
» gebruik van potentieel gevaarlijke functies;
» juiste toepassing van invoervalidatie;
» datastromen door een webapplicatie.

De noodzaak van de beveiligingsrichtlijn neemt toe naar mate de complexiteit van de webapplicatie toeneemt.

Identificeren en verwijderen van 'dode code'[74]

In de broncode verwijst dode code of onbereikbare code naar stukken code die nooit uitgevoerd (kunnen) worden maar wel in de broncode aanwezig zijn. Deze code kan worden verwijderd zonder dat daarbij semantische eigenschappen van de applicatie veranderen, denk hierbij aan code die uitsluitend gebruikt is voor debuggen. Deze code kan door een kwaadwillende mogelijk worden misbruikt en zou verwijderd moeten worden.

Het verwijderen van 'dode code' heeft zowel voordelen tijdens het compileren als het uitvoeren van de applicatie en verbetert bovendien de onderhoudbaarheid van de applicatie.

Voor het opsporen van dode code is het nodig om de broncode te analyseren. Dit kan met behulp van statische of dynamische codeanalyse en een analyse van de control flow om te kijken welke stukken code niet uitgevoerd (kunnen) worden.

Standaardsoftware, software-as-a-service (SaaS) of ontwikkeling van software is uitbesteed

Als het gaat om standaardsoftware, software-as-a-service (SaaS) of de ontwikkeling van de software is uitbesteed en er geen handmatige codereview uitgevoerd kan/mag worden, kan worden gedacht aan de volgende aandachtspunten:
» externe certificering van de extern ontwikkelde software;
» afspraken in een overeenkomst vastleggen om de software te auditen;
» afspraken over het dynamisch scannen, bij het dynamisch scannen wordt met behulp van geautomatiseerde tools via de (web)interface van de applicatie, terwijl de applicatie draait, gezocht naar kwetsbaarheden en zwakheden in de applicatie;
» afspraken over het uitvoeren van andere tests, bijvoorbeeld penetratietest (zie richtlijn C.04) of blackboxscan (zie hierna), om mogelijke kwetsbaarheden op te sporen.

Blackboxscan

Een blackboxscan benadert de aanpak van een kwaadwillende het best, aangezien een tester zonder voorkennis gaat kijken of er

74 Bron: 'The revival transformation, Proceedings of the 21st ACM SIGPLANSIGACT symposium on Principles of programming language', The Association, d.d. 1994

kwetsbaarheden in de webapplicatie bestaan. Tools om blackbox-scans uit te voeren zijn bekend onder de noemer Web Application Scanner (WAS). Een WAS voert een groot aantal tests uit op een webapplicatie zoals het uitproberen van verschillende varianten van SQL-injectie en XSS.

Een WAS kent enkele beperkingen die belangrijk zijn om in het achterhoofd te houden. Zo is het voor een WAS vaak moeilijk om ingelogd te blijven in webapplicaties die authenticatie vereisen. Door de grote verscheidenheid aan tests die een WAS uitvoert, bestaat de mogelijkheid dat de webapplicatie na een aantal tests de sessie beëindigt. Het is voor een WAS vaak moeilijk om te bepalen dat deze sessie is beëindigd en bijvoorbeeld een cookie niet meer geldig is. Gevolg is dat het testen van websites die authenticatie vereisen problematisch en onbetrouwbaar kan zijn.

Daarnaast kunnen sterk dynamische websites voor uitdagingen zorgen. Zo zal een WAS JavaScript moeten begrijpen om effectieve tests uit te kunnen voeren. In het bijzonder technologieën als Ajax kunnen in dit kader moeilijk testbaar zijn. Tot slot kunnen de scans die een WAS uitvoert, leiden tot een groot aantal false positives. Het is dus belangrijk dat een persoon met kennis van zaken beoordeelt in hoeverre een gemelde vermeende kwetsbaarheid ook daadwerkelijk een kwetsbaarheid is, hoe eenvoudig deze uit te buiten is en wat de schade zou zijn als gevolg van misbruik.

Wanneer blackboxscans?

Er kunnen meerdere momenten zijn waarop een blackbox scan zinvol is:

- in de acceptatiefase van een nieuw systeem of een nieuwe applicatie;
- bij significante wijzigingen van een belangrijk systeem of een belangrijke applicatie;
- periodiek (jaarlijks/tweejaarlijks), om bestaande systemen te testen op nieuwe inbraaktechnieken en/of als onderdeel van de PDCA-cyclus;
- als er een andere reden is om te denken dat de beveiliging van een systeem minder goed is dan gedacht.

De frequentie dient vastgesteld te worden op basis van het risicoprofiel.

C.06 Logging

Omschrijving

Logging is een proces voor het registreren van activiteiten en gebeurtenissen in systemen om achteraf de rechtmatigheid van de resourcebenaderingen, evenals vroegtijdige ongeautoriseerde toegangspogingen van systemen en netwerken te kunnen signaleren. Omdat systemen uitgebreide loggingsfunctionaliteit kennen moet vooraf een beperkte maar wel representatieve selectie van de te loggen systeemgegevens worden gemaakt, om de controlewerkzaamheden zo doelmatig mogelijk te laten verlopen. Hierbij dient men met een aantal organisatorische en technische aspecten rekening te houden.

Relevante organisatorische en technische aspecten

- detecteren – het signaleren van aanvallen (behandeld in U/NW.04);
- centraliseren – op één punt samenbrengen van loggingsgegevens;
- correlaties (analyse) – het leggen van correlaties tussen de geregistreerde gegevens;
- synchroniseren – het synchroniseren van systeemklokken;
- alternatieven – het beschikken over alternatieven bij uitval van loggingmechanismen;
- bewaartermijnen – het vaststellen van bewaartermijnen van logging;
- integriteit – het beveiligen van loggingsgegevens tegen achteraf wijzigen;
- (pro)actieve controles – het actief uitvoeren van controles op logging.

Beveiligingsrichtlijn C.06

Logging bijhouden

Richtlijn (wie en wat)
In de webapplicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief en efficiënt, effectief en beveiligd ingericht.

Doelstelling (waarom)
Het maakt mogelijk eventuele schendingen van functionele en beveiligingseisen te kunnen detecteren en achteraf de juistheid van de uitgevoerde acties, zowel op strategisch als operationeel niveau te kunnen vaststellen.

Risico
Tekortkomingen en zwakheden in de geleverde producten/diensten kunnen niet gesignaleerd worden en herstel acties kunnen niet tijdig worden genomen.

Classificatie
Hoog
Richtlijn 2012
B7-1, B7-2, B7-4, B7-5, B7-6, B7-7

Maatregelen

registratie en detectie

01 Bepaal welke gebeurtenissen en/of beheeractiviteiten aan de webapplicatie vastgelegd moeten worden.
Stel regelgeving op over vast te leggen gebeurtenissen en handelingen. De regels hierover worden onderhouden. Voorbeelden van vast te leggen gegevens zijn:
- *verdachte gebeurtenissen en wijzigingen aan de webapplicatie;*
- *succesvolle en geweigerde toegangspogingen;*
- *(on)geoorloofde activiteiten door functionarissen.*

Eventueel worden ten behoeve van leesbaarheid en efficiency filters gebruikt.

02 Detecteer aanvallen met detectiesystemen in de webapplicatie-infrastructuur.
In de ontwerp- of configuratiedocumentatie is vastgelegd waar en hoe IDS'en worden ingezet (zie richtlijn U/NW.04/08). Dit is gebaseerd op een risicoanalyse.

efficiënt en effectief

03 Leg in de ontwerp- of configuratiedocumentatie vast waar en hoe centralisering van logging is ingericht (inclusief configuratie-instellingen).
De inrichting is gebaseerd op een vastgesteld inrichtingsdocument/ontwerp waarin is vastgelegd welke uitgangspunten gelden voor logging. Zorg dat dit inrichtingsdocument/ontwerp onderdeel is van het proces wijzigingsbeheer (zie richtlijn C.08). De ontwerp- en inrichtingskeuzes moeten zijn onderbouwd en op het juiste (organisatie)niveau zijn verantwoord.
Er is een plan met daarin activiteiten die worden uitgevoerd (wie, wat en wanneer) indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.

04 Configureer de systemen zodanig dat interne systeemklokken automatisch gesynchroniseerd worden.
Systemen gebruiken interne systeemklokken voor "time stamps" bij het vastleggen van loggegevens. De ontwerp- of configuratiedocumentatie is vastgelegd hoe het synchroniseren van de systeemklokken is geconfigureerd.

beveiligd

05 Bepaal vooraf wat te doen bij het uitvallen van loggingmechanismen (alternatieve paden).
Er wordt aangegeven welke actie een component moet nemen op het moment dat het centrale loggingmechanisme niet meer beschikbaar is. Er is een procedurebeschrijving van het loggingmechanisme en getest dat het mechanisme van alternatieve actie bij uitvallen loggingmechanismen ook daadwerkelijk werkt.

06 Stel de (online of offline) bewaartermijn voor logging vast en laat dit tot uitdrukking komen in de configuratie-instellingen van de systemen.
Er zijn bewaartermijnen vastgesteld voor de loginformatie. Dit zal moeten blijken uit de configuratie instellingen.

07 Bescherm de loggegevens tegen toegang door onbevoegden beveilig deze tegen achteraf wijzigen/verwijderen.
Ontwerpdocumentatie, configuratie-instellingen en autorisatieprofielen geven aan hoe logfiles beschermd zijn tegen achteraf of ongeautoriseerd wijzigen/verwijderen.

Verdieping

Centraliseren van loggingsgegevens

Logging en ICT-landschap
Vaak worden verschillende loggingmechanismen naast elkaar gebruikt. Zo ondersteunt het ene systeem alleen logging op basis van SYSLOG, maakt een ander systeem alleen lokaal logbestanden aan en stelt weer een ander systeem alleen informatie beschikbaar via SNMP. Al deze verschillende loggingmechanismen zorgen ervoor dat logging versnipperd raakt en een organisatie het overzicht over alle gebeurtenissen gemakkelijk kwijtraakt. Om aanvallen efficiënt te kunnen detecteren is het van belang deze logging op één centraal punt weer bijeen te brengen. Beperk het aantal loggingmechanismen zoveel mogelijk.

Door de logging op een centraal punt bijeen te brengen en deze intelligent te combineren en te filteren ontstaat een heldere blik op alle informatie vanuit de verschillende componenten uit de infrastructuur.

In een centrale loggingdatabase komt de loginformatie uit verschillende onderdelen van het ICT-landschap samen. Denk hierbij aan de volgende typen informatie: logging op het niveau van netwerk-, platform- en webapplicatiebeveiliging; logging op het niveau van identiteit- en autorisatiebeheer (zie paragraaf 10.10 'Controle' in NEN-ISO/IEC 27002 'Code voor informatiebeveiliging'.); en logging op het niveau van vertrouwelijkheid en onweerlegbaarheid.

De centraal opgeslagen informatie is zeer interessant voor kwaadwillenden aangezien ze 1) veel kunnen leren over de opbouw van de infrastructuur en 2) ze via deze centrale plek eventuele sporen van misbruik kunnen wissen. Daarom is het van belang veel aandacht te besteden aan de beveiliging van deze centrale database, zodat onbevoegden hiertoe geen toegang hebben en hierin geen wijzigingen kunnen aanbrengen.
Een andere mogelijke beveiligingsmaatregel in dit kader kan ook zijn om logbestanden digitaal te ondertekenen.

Aandachtspunten loggingsinformatie:

- Bepaal welke gebeurtenissen worden gelogd en onderhoud deze regels.
- Onderhoud kennis van correlaties die op misbruik duiden.
- Daarnaast is het, ter verbetering van de leesbaarheid van de logging, aan te raden filters op de logging te plaatsen.
- Voorkom dat het herkennen van verdachte patronen in de logging afhangt van de kunde van de operationeel beheerder.

Opvolging
Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Synchroniseren van systeemklokken

Om gebeurtenissen uit verschillende componenten te correleren worden de timestamps van deze gebeurtenissen gebruikt. Deze timestamps zijn afhankelijk van de juiste instelling van de tijd op de betreffende componenten. Met behulp van het Network Time Protocol (NTP) kan worden bereikt dat de tijd op alle servers en andere componenten overeen komt (zie paragraaf 10.10.6 'Synchronisatie van systeemklokken' in NEN/ISO-IEC 27002 'Code voor informatiebeveiliging').

Alternatieven voor beschikbaarheid van registraties (logbestanden)

Het gebruik van centrale loggingmechanismen brengt een belangrijk vraagstuk met zich mee: wat doen we op het moment dat dit centrale loggingmechanisme uitvalt? Op het moment dat een component zijn logging niet meer kwijt kan, bestaat de kans dat deze logging verloren gaat. Dit zou kunnen betekenen dat componenten aanvallen van kwaadwillenden niet meer registreren, of dat transacties niet meer onweerlegbaar zijn. Bepaal daarom op voorhand welke actie een component moet nemen op het moment dat het centrale loggingmechanisme niet meer beschikbaar is. Er bestaan op dit gebied grofweg de volgende mogelijke acties:

» De component normaal laten functioneren terwijl deze de logging niet kan opslaan. Dit betekent dat logging verloren gaat.
» De component normaal laten functioneren en de logging lokaal laten opslaan. Veel componenten beschikken over een lokaal mechanisme om logging tijdelijk op te slaan. Op het moment dat het centrale loggingmechanisme weer beschikbaar komt, sluist de component de verzamelde logging alsnog door. Dit voorkomt dat de component niet meer beschikbaar is en voorkomt tevens dat logging verloren gaat. Dit is echter wel een tijdelijke oplossing. Op het moment dat de lokale opslag vol loopt, moet opnieuw besloten worden wat de component hierna doet (blijven functioneren - zie bovenstaande optie - of stoppen met functioneren - zie volgende optie).
» De component acuut laten stoppen met functioneren. Dit betekent dat gebruikers hoogst waarschijnlijk niet meer kunnen doorwerken. Dit voorkomt wel dat aanvallen op de component onopgemerkt blijven doordat de component ze niet meer logt.

Vanuit het oogpunt van beveiliging en beschikbaarheid heeft het de voorkeur om – zodra het centrale loggingmechanisme uitvalt - componenten eerst lokaal gebeurtenissen te laten opslaan om vervolgens de component te laten stoppen met functioneren zodra deze opslag vol is. Bij de selectie van een nieuw beveiligingscomponent is het daarom zaak goed te evalueren of deze voldoet aan de eisen op het gebied van logging en tijdelijke opslag van logging.

Integriteit van registraties

Om te voorkomen dat kwaadwillende sporen uitwissen moeten logfiles zo zijn ingesteld dat deze achteraf niet kunnen worden aangepast. Deze beveiligingseis is essentieel bij reconstructie vraagstukken in relatie tot opgetreden issues/incidenten.

Bewaartermijnen van registraties

Er moet worden bepaald hoe lang logging online en offline beschikbaar moet en mag zijn. Online beschikbaarheid van logging kan essentieel zijn voor het efficiënt verhelpen van beveiligingsincidenten. De duur van offline beschikbaarheid kan beperkt worden door wet- en regelgeving. Voordat wordt besloten om gebeurtenissen in een omgeving te loggen, moet zijn vastgesteld hoe lang en op welke manier logging beschikbaar moet blijven. Dit bepaald welke media nodig zijn en hoeveel capaciteit je voor de logging moet reserveren. Het systeem, waarmee gegevens opgeslagen en behandeld worden, dient dusdanig te zijn dat de gegevens duidelijk geïdentificeerd kunnen worden gedurende hun wettelijke of reglementaire bewaartermijn. De gegevens dienen op een passende wijze vernietigd te kunnen worden na afloop van die termijn voor zover ze niet meer nodig zijn voor de organisatie.

In sommige gevallen is de bewaartermijn voor informatie en het type informatie dat bewaard moet worden geregeld in de nationale wetgeving of voorschriften. Deze beveiligingseis is tevens essentieel bij reconstructie vraagstukken in relatie tot opgetreden issues/incidenten.

C.07 Monitoring

Omschrijving

Het monitoren (ofwel bewaken/controleren) van systemen heeft tot doel ongeautoriseerde toegangspogingen tot systeem- en netwerk resources en ongeautoriseerd gebruik van deze resources tijdig te signaleren en op basis van de ernst van de signalering acties te ondernemen. De monitoringfunctie moet voorbehouden zijn aan een daartoe verantwoordelijke functionaris. Monitoring vindt mede plaats op basis van geregistreerde gegevens (logging). De geregistreerde gegevens dienen te worden geanalyseerd (auditing) en te worden gerapporteerd (alerting). Alerting kan ook automatisch door een systeem zelf worden gegevens op basis van vastgestelde overschrijding van drempelwaarden.

Beveiligingsrichtlijn C.07

Monitoring rapporteren

Richtlijn (wie en wat)
De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.

Doelstelling (waarom)
Tijdig inzetten van correctieve maatregelen en informatie verschaffen over activiteiten van gebruikers en beheerders van de ICT-diensten en de status van de componenten waarmee deze worden voortgebracht.

Risico
Onvoldoende mogelijkheden om tijdig bij te sturen om organisatorisch en technisch te (blijven) voldoen aan de doelstellingen.

Classificatie
Hoog

Richtlijn 2012
B7-3, B7-8, B7-9

Maatregelen

registraties

01 Breng de door verschillende beheerdisciplines gelogde informatie samen voor analysedoeleinden.
Afhankelijk van de typologie van de organisatie is het raadzaam om gelogde gegevens te centraliseren.

alarmeringen

02 Laat de signaleringssystemen (detectie) tijdig melding maken van ongewenste gebeurtenissen.
In de ontwerp- of configuratiedocumentatie is vastgelegd welke drempelwaarden gelden voor alarmeringen.
Bij alarmeringen gaat het om automatische rapportages gegenereerd door het systeem.

bewaken (controleren)

03 Voer periodiek actief controles uit op:
» wijzigingen aan de configuratie van webapplicaties;
» optreden van verdachte gebeurtenissen en eventuele schendingen van de beveiligingseisen;
» ongeautoriseerde toegang tot en wijzigingen/verwijderen van logbestanden.
Procedurebeschrijving met daarin beschreven hoe en wanneer controles op logging moeten plaatsvinden en hoe taken op dit gebied belegd zijn.
Plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.
04 Voer periodiek reviews uit van toegangslogs.

analyseren (auditing)

05 Analyseer de verzamelde loggingsinformatie in samenhang.
In de ontwerp- of configuratiedocumentatie is vastgelegd waar en hoe correlaties worden aangebracht.
Er is een plan met daarin de activiteiten die worden uitgevoerd (wie, wat en wanneer) indien logrecords op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet aan de gestelde eisen en/of verwachtingen hebben voldaan of tekortkomingen hebben opgeleverd.
06 Analyseer periodiek de geregistreerde menselijke en systeemacties.
De menselijke acties zijn herleidbaar naar individuele personen.
07 Analyseer periodiek op ongebruikelijke situaties (incidenten) die de werking van webapplicaties kunnen beïnvloeden.

rapporteren (alerting)

08 Rapporteer periodiek de geanalyseerde en beoordeelde gelogde gegevens aan de systeemeigenaren en/of aan het management.
09 Analyseer en evalueer de rapportages uit de beheerdisciplines compliancemanagement, vulnerability assessment, penetratietest en logging en monitoring op aanwezigheid van structurele risico's.
De resultaten uit deze evaluatie worden geconsolideerd en gerapporteerd naar het hoogste management.
10 Geef aantoonbaar opvolging en voer verbeteringen door indien logrecords op misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen of verwachtingen, of tekortkomingen opleveren.
11 Actualiseer beveiligingsplannen en wijs verantwoordelijken toe voor het realiseren van (delen) van het beveiligingsplan op basis van de geconsolideerde rapportages.

Verdieping

Voor zowel monitoring, auditing als alerting geldt dat de verschillende technologieën op meerdere lagen informatie aanleveren die monitoring, auditing en alerting mogelijk maken. Heel belangrijk is dat ze niet los op elke laag beschouwd worden, maar dat (causale) verbanden kunnen worden gelegd tussen de afzonderlijke logging- en monitoringmechanismen. Dit soort denken is vooral van belang door de steeds verder voortschrijdende ketenintegratie, waarbij componenten aan elkaar gekoppeld worden en de sterkte en het functioneren van de keten bepaald worden door de zwakste schakel

Uit efficiency en beheeroverwegingen moet de monitoringsfunctie zoveel mogelijk vanuit een centrale locatie plaatsvinden. De toegang tot de centrale monitoringsconsole, die in een afgeschermde omgeving staat, moet voldoen aan de toegangsbeveiligingscriteria. Inbreuken, zoals onjuiste inlogpogingen, worden direct gedetecteerd, en doorgegeven aan de daartoe verantwoordelijke (onder andere de securitymanager). Verslaglegging vanuit de monitoringconsole maakt deel uit van de periodieke rapportage.

(Pro)actieve controles

Er moeten (pro)actieve controles uitgevoerd worden op de verzamelde logging (denk hierbij aan applicatie-, database-, host- en netwerklogging), zodat misbruik van de omgeving en inbraakpogingen detecteren. De verantwoordelijke moet ondersteund worden door een adequate filtering op de logging. Alleen bij een adequate filtering is het mogelijk om aanvallen te detecteren uit de grote hoeveelheid logging die verschillende componenten op een dag zullen genereren. Filtering van de logging zal dynamisch zijn; door het filter continu aan te passen, ontstaat een behapbaar en bruikbaar overzicht van gebeurtenissen die zich in de omgeving hebben voorgedaan. Deze beveiligingseis is tevens essentieel bij reconstructie vraagstukken in relatie tot opgetreden issues/incidenten.

Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Correlaties tussen gelogde gegevens

Nadat alle loggingsinformatie over webapplicaties bijeen gebracht is (zie richtlijn C.06/01), is de volgende stap het aanbrengen van

correlaties tussen de verschillende gebeurtenissen. De uitdaging hierbij is om alle gebeurtenissen op de verschillende niveaus aan elkaar te correleren en aan een specifieke webapplicatie te koppelen. Op deze manier kun je het pad dat een kwaadwillende heeft doorlopen, achterhalen en tevens inzicht krijgen in de aanvallen die gedurende een bepaalde periode op een webapplicatie zijn uitgevoerd.

Een goed ingerichte Configuration Management Database (CMDB), zie richtlijn C.11, waarin componenten en de afhankelijkheden daartussen zijn gedefinieerd, kan het leggen van correlaties voor een belangrijk gedeelte vereenvoudigen.

Aandachtspunten loggingsinformatie:
» Bepaal welke gebeurtenissen worden gelogd en onderhoud deze regels.
» Onderhoud kennis van correlaties die op misbruik duiden.
» Daarnaast is het, ter verbetering van de leesbaarheid van de logging, aan te raden filters op de logging te plaatsen.
» Voorkom dat het herkennen van verdachte patronen in de logging afhangt van de kunde van de operationeel beheerder.

Opvolging
Er moet actie worden ondernomen indien log records op kwaadwillend misbruik duiden, geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

C.08 Wijzigingenbeheer

Omschrijving

Wijzigingenbeheer richt zich op het effectief doorvoeren van wijzigingen in ICT-middelen en ICT-diensten zodanig dat de kans op verstoring van de dienstverlening wordt geminimaliseerd en blijvend voldoet aan de functionele en beveiligingseisen van belanghebbenden.

Wijzigingenbeheer zorgt ervoor dat alle instellingen van de ICT-infrastructuur gecontroleerd en geautoriseerd gewijzigd worden, dit geldt dus ook voor de hardeningsmaatregelen. Wijzigingen moeten eerst worden getest in een test- of acceptatieomgeving om de impact van de maatregelen vast te stellen. Dit zorgt ervoor dat de ICT-infrastructuur aan de gestelde maatregelen blijft voldoen.

Het aanbrengen van bijvoorbeeld nieuwe verbindingen tussen netwerkcomponenten kan ervoor zorgen dat routepaden en compartimenteringen 'plotseling' ongewenst wijzigen.
Het proces configuratiebeheer (zie richtlijn C.11) is voorwaardenscheppend voor wijzigingsbeheerproces en heeft een beveiligingsbelang in het kader van de integriteits-handhaving, doordat het kan ondersteunen dat updates van ICT-componenten overal worden aangebracht waar ze worden gebruikt.
Voordat een webapplicatie in productie wordt genomen, is het van belang dat eerst een uitgebreide test wordt uitgevoerd op de webapplicatie en de omliggende infrastructuur.
Het uitvoeren van tests is niet alleen belangrijk bij de initiële ingebruikname van de webapplicatie, maar ook na het doorvoeren van belangrijke wijzigingen in de webapplicatie of de infrastructuur.

Ook voor alle maatregelen die in deze Richtlijn worden beschreven, geldt dat deze altijd eerst in een representatieve testomgeving moeten worden uitgeprobeerd voordat ze in een productieomgeving toegepast kunnen worden. Systemen moeten opnieuw worden beoordeeld en getest wanneer wijzigingen plaatsvinden.
Wijzigingen kunnen een onvoorziene negatieve impact hebben op de werking van de ICT-infrastructuur en daarom is het belangrijk te verifiëren of een systeem, ook na het effectueren van wijziging, goed blijft functioneren. Dit geldt natuurlijk voor alle maatregelen zoals hardeningsmaatregelen.

Ontwikkel- en testactiviteiten kunnen verstoringen veroorzaken, bijvoorbeeld onbedoelde wijzigingen in bestanden of systeemomgeving, of storingen in het systeem. Ontwikkel- en testactiviteiten kunnen ook onbedoelde wijzigingen in software en informatie veroorzaken als dezelfde ICT-omgeving wordt gedeeld.
Als ontwikkel- en testmedewerkers toegang hebben tot de productieomgeving en - informatie, zouden zij ongeoorloofde en niet geteste software kunnen invoeren of bedrijfsgegevens kunnen wijzigen. Voorzieningen voor ontwikkeling, testen en productie moeten zijn gescheiden om het risico van onbedoeld wijzigingen of ongeautoriseerde toegang tot productiesystemen en bedrijfsgegevens te verkleinen.

Op het moment dat een kwaadwillende een (kwetsbaar) systeem compromitteert, kunnen door de kwaadwillende wijzigingen op dit systeem worden aangebracht. Door wijzigingen op de ICT-infrastructuur (bijvoorbeeld besturingsniveau) te auditen worden eventuele problemen of compromittering van de ICT-omgeving gedetecteerd. Het auditen van ongeautoriseerde wijzigingen op systemen, kan daarom helpen bij het waarnemen van misbruik van de ICT-omgeving. Door geautomatiseerde hulpmiddelen in te zetten kunnen deze wijzigingen adequaat worden gemonitord (zie richtlijnen C.06 en C.07).

Beveiligingsrichtlijn C.08

Wijzigingenbeheer uitvoeren

Richtlijn (wie en wat)
Wijzigingenbeheer is procesmatig en procedureel zodanig uitgevoerd dat wijzigingen in de ICT-voorzieningen van webapplicaties tijdig, geautoriseerd en getest worden doorgevoerd.

Doelstelling (waarom)
Zekerstellen dat wijzigingen op een correcte en gecontroleerde wijze worden doorgevoerd waardoor de veilige werking van ICT-voorziening wordt gegarandeerd.

Risico
Er kunnen ongeautoriseerde acties worden doorgevoerd of acties zijn onvoldoende op elkaar afgestemd, waardoor de betrouwbaarheid van de ICT-voorziening in het geding kan komen.

Classificatie
Hoog

Richtlijn 2012
Bo-6

Maatregelen

procesmatig en procedureel

01 Laat wijzigingen systematische processtappen doorlopen, zoals intake, acceptatie, impactanalyse, prioritering en planning, uitvoering, bewaking en afsluiting.
In het document wijzigingsbeheerproces zijn onder andere de volgende aspecten vermeld:
» *eigenaar;*
» *afgiftedatum en versienummer;*
» *documenthistorie (wat is wanneer en door wie aangepast);*
» *vastgesteld/geaccordeerd op het juiste organisatorische niveau;*
» *de changekalender.*
Er is een overzicht met alle wijzigingsverzoeken inclusief autorisatie en impactanalyse met betrekking tot informatiebeveiliging.
Er zijn wijzigingsprocessen beschreven die de gehele sequentie van wijzigingen, vanaf initiatie tot afsluiting, weergeven, zoals:
» *impactanalyse van een wijzigingsverzoek;*
» *acceptatie van wijzigingsverzoeken;*
» *categoriseren en prioriteren van wijzigingen;*
» *planning van wijzigingen;*
» *ontwikkelen, inclusief testen, van wijzigingen;*
» *doorvoeren, inclusief validatie, van wijzigingen;*
» *bewaking van wijzigingen;*
» *afsluiten van wijzigingen.*
Er is vastgelegd wie de prioriteit van wijzigingen bepaalt en wie toestemming verleent, bijvoorbeeld een beslissingsforum (Change Advisory Board).
Realisatie en implementatie van wijzigingen worden gepland en deze planningsgegevens worden gepubliceerd (changekalender).
Wijzigingen worden geëvalueerd, waarbij in elk geval vastgesteld wordt of de wijziging niet tot incidenten heeft geleid.
02 Laat alle wijzigingsverzoeken verlopen volgens een formele wijzigingsprocedure (voorkomen van ongeautoriseerde wijzigingen) en OTAP-procedures.
Er zijn procedures gedocumenteerd en vastgesteld voor het overdragen van de ene naar de andere omgeving (van ontwikkel naar test, van test naar acceptatie en van acceptatie naar productie).
03 Sluit functioneel beheer aan op het generiek proces van wijzigingenbeheer.
04 Lever (beheer)documentatie van wijzigingen op conform vastgestelde eisen.
05 Stel wijzigingsprocedures op voor hardware, software en parameterinstellingen (configuratie).
06 Richt configuratiebeheer in en geef daarmee inzicht in gegevens van de kritieke systemen en applicaties.

tijdig, geautoriseerd

07 Registreer en neem wijzigingen binnen een afgesproken tijdslimiet in behandeling op een gestructureerde wijze.
08 Neem alleen geautoriseerde wijzigingsverzoeken (Request for Change (RFC)) in behandeling.
Vanuit efficiëntie en integriteitsoogpunt is vastgesteld welke functionarissen wijzigingen mogen aanvragen.
09 Neem autorisatie van doorvoeren van wijzigingen in de verschillende OTAP-omgevingen op in het proces van wijzigingenbeheer.
Voor de overgangen van ontwikkel, test, acceptatie en productieomgeving (OTAP) zijn regels en procedures voor het overdragen van systemen van de ene naar de andere omgeving (van ontwikkel naar test, van test naar acceptatie en van acceptatie naar productie).

testen

10 Test alle wijzigingen altijd eerst voordat deze in productie worden genomen en neem ze via vastgestelde wijzigings- en releaseprocedures in productie.
Bij de testactiviteit zijn onder andere volgende aandachtpunten van belang:
» *acceptatiecriteria voor nieuwe systemen;*
» *de datasets en testscripts die worden gebruikt om de tests uit te voeren;*
» *de resultaten van de uitgevoerde tests;*
» *de autorisatie dat de tests met goed gevolg zijn doorlopen en dat de wijziging in productie mag worden genomen.*

Webapplicaties worden getest voordat deze in de productie worden genomen:
» *Voor nieuwe systemen, upgrades en nieuwe versies moeten acceptatiecriteria zijn vastgesteld.*
» *Er zijn procedures opgesteld voor de omvang en diepgang van de tests. Als de wijziging impact heeft op de informatiebeveiliging, is bepaald of er specifieke beveiligingstests uitgevoerd moeten worden (bijvoorbeeld penetratietests (zie richtlijn C.04), codereviews et cetera).*
» *Penetratietesten maken onderdeel uit van de testen (zie richtlijn C.04).*
» *Als het gaat om standaardsoftware of software-as-a-service (SaaS) kan worden gedacht aan de volgende aandachtspunten:*
› *externe certificering van de extern ontwikkelde software;*
› *afspraken in het contract vastleggen om de software te mogen auditen;*
› *uitvoeren van andere tests, bijvoorbeeld penetratietest (zie richtlijn C.04) of blackbox scan (zie richtlijn C.05), om mogelijke kwetsbaarheden op te sporen.*
11 Scheid ontwikkel, test en acceptatievoorzieningen van productievoorzieningen (OTAP).
In bepaalde situaties (omgevingen) kan een OTP-omgeving een afdoende maatregel zijn.
12 Audit de productieomgeving op ongeautoriseerde wijzigingen.

C.09 Patchmanagement

Omschrijving

Patchmanagement is een proces dat zorgt voor het verwerven, testen en installeren van patches (wijzigingen in de code) op (verschillende softwarecomponenten van) een computersysteem.

Een solide updatemechanisme is essentieel om voldoende beschermd te zijn tegen bekende beveiligingsproblemen in software. Een updatemechanisme voor alle applicatieplatformen, applicaties, databases, et cetera die bovenop dit platform draaien, is minstens zo belangrijk. De noodzaak van patchen staat vaak niet ter discussie. Er ontstaat echter wel vaak discussie over de urgentie waarmee deze patches uitgevoerd moeten worden. De tijdsduur tussen het uitkomen van een patch en de implementatie van een patch is hierbij afhankelijk van de gevoeligheid van de webapplicatie en de ernst van de patch. Daarom is het van belang vast te stellen welke doelstelling en prioriteit nagestreefd worden met patchmanagement. Het kan voorkomen dat systemen die niet meer ondersteund worden, (tijdelijk) operationeel gehouden moeten worden. Het is van belang om te weten welke systemen dat zijn en welke aanvullende maatregelen getroffen zijn om deze systemen voor het uitbuiten van kwetsbaarheden te behoeden.

Grofweg bestaat een ingericht patchmanagementproces uit de volgende stappen:
3. stel vast dat een patch beschikbaar is;
4. berdeel de impact van de uitgebrachte patch en de bijbehorende kwetsbaarheid;
5. verkrijg de patch via de leverancier;
6. test de patch in een test- en/of acceptatieomgeving;
7. rol de patch uit in de productieomgeving;
8. volg berichtgeving rondom de patch;
9. evalueer het gehele proces.

Het proces configuratiebeheer (zie richtlijn C.11) is voorwaardenscheppend voor het patchmanagementproces en heeft een beveiligingsbelang in het kader van de integriteitshandhaving, doordat het kan ondersteunen dat updates van ICT-componenten overal worden aangebracht waar ze worden gebruikt.

Beveiligingsrichtlijn C.09

Patchmanagement uitvoeren

Richtlijn (wie en wat)
Patchmanagement is procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings) patches tijdig zijn geïnstalleerd in de ICT-voorzieningen.

Doelstelling (waarom)
Zekerstellen dat technische en software kwetsbaarheden tijdig en effectief worden aangepakt en zo een stabiele omgeving wordt gecreëerd.

Risico
Technische en software kwetsbaarheden brengen stabiliteit en betrouwbaarheid van systemen in gevaar.

Classificatie
Hoog

Richtlijn 2012
Bo-7

Maatregelen

Procesmatig en procedureel

01 Beschrijf het patchmanagementproces en laat het goedkeuren door het management en toekennen aan een verantwoordelijke functionaris.
Het beschreven patchmanagementproces geeft aan hoe de organisatie omgaat met updates: hoe snel implementeert de organisatie een kritieke patch, welke stadia moet de patch doorlopen, wie draagt de verantwoordelijkheid.
Zorg voor een actueel overzicht van systemen die in productie draaien maar niet meer worden onderhouden.

02 Voorzie alle ICT-componenten van de meest recente, relevante patches.

03 Stel de rollen en verantwoordelijkheden voor patchmanagement vast.

04 Voer registratie over de verworven patches, hun relevantie, besluit tot wel/niet uitvoeren, datum patch-test, resultaat patch-test, datum uitvoeren patch en patch-resultaat.

richtlijnen

05 Stel een patchrichtlijn op voor de ondersteuning van patchactiviteiten die op het juiste (organisatorische) niveau is vastgesteld en is geaccordeerd.
Er is een document beschikbaar waarin het patchrichtlijn is beschreven.
Er wordt hierbij ook aangegeven dat patchactiviteiten verband houden met de activiteiten van het configuratiebeheer.
De patchrichtlijn heeft betrekking op het vaststellen van de wenselijkheid van het installeren van patches, het correct installeren van de patches en het testen van de geïnstalleerde patches.

C.10 Beschikbaarheidbeheer

Omschrijving

Beschikbaarheidbeheer is een proces dat ervoor zorgt dat de aangeboden ICT-diensten beschikbaar zijn voor de klant.
Er moeten hersteltijden worden vastgesteld op basis van de gevoeligheid van de webapplicaties.

Herstelmaatregelen moeten zijn geborgd, bijvoorbeeld back-up en restore en een calamiteitenplan.
Er moeten regelmatig back-ups (reservekopieën) worden gemaakt van essentiële informatie en systemen of webapplicaties om de integriteit en beschikbaarheid van systemen of webapplicaties te waarborgen. Hiervoor moeten goede voorzieningen beschikbaar zijn, zodat alle essentiële gegevens en systemen tijdig hersteld kunnen worden na een incident.

Dagelijkse back-ups zijn vaak voldoende maar voor sommige dynamische componenten (zoals databases) is dit wellicht niet afdoende. Bij dergelijke componenten kan worden overwogen om de transactielog van de database beschikbaar te stellen op een uitwijklocatie ('remote journaling'). In het geval dat een component crasht, kan een up-to-date versie van de component worden gecreëerd door de laatste back-up hiervan terug te zetten en hierop het transactielog toe te passen.

Het is aan te raden om back-ups te versleutelen. Valt een back-up onverhoopt in handen van een kwaadwillende, dan kan deze in dit geval geen toegang krijgen tot de informatie in de back-up.

Tot slot is het van belang om regelmatig te testen of de gemaakte back-ups de mogelijkheid bieden om een verloren gegaan systeem opnieuw op te bouwen. Maak back-ups onderdeel van een Disaster Recovery Plan (DRP). De frequentie voor het testen dient vastgesteld te worden op basis van het risicoprofiel. Er moet actie worden ondernomen indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen en/of verwachtingen of tekortkomingen opleveren.

Het kan voorkomen dat voor een gecompromitteerde server, gecompromitteerde bestanden worden gerestored. Om de integriteit van systemen of webapplicaties te garanderen moet in sommige gevallen een 'clean install' van het systeem of webapplicatie worden uitgevoerd en alleen de data vanuit een back-up wordt teruggehaald. Als de informatieverwerking, en de bijbehorende verantwoordelijkheid, is uitbesteed aan een andere organisatie moeten hierover afspraken worden vastgelegd in een overeenkomst (contract en/of SLA) tussen beide partijen. Dit geldt ook op het moment dat software-as-a-service diensten worden ingekocht, denk dan bijvoorbeeld aan cloud escrow.[75]

Beveiligingsrichtlijn C.10

Beschikbaarheidbeheer inrichten

Richtlijn (wie en wat)
Beschikbaarheidbeheer wordt is procesmatig ingericht, zodat bij calamiteiten de webapplicaties binnen de gestelde termijn wordt hersteld en voortgezet.

Doelstelling (waarom)
Waarborgen van beschikbaarheid van informatieverwerkende systemen of webapplicaties.

Risico
Onnodig lange uitval van businessactiviteiten na calamiteiten, waardoor bedrijfsdoelstellingen niet worden gehaald.

Classificatie
Hoog

Richtlijn 2012
Bo-11

Maatregelen

procesmatig

01 Beschrijf het beschikbaarheidbeheerproces en laat het goedkeuren door het management en toekennen aan een verantwoordelijke functionaris.

02 Documenteer de back-up- en herstelprocessen en -procedures voor de hele webapplicatie-omgeving.
Er is goede en recente back-up van de bestanden aanwezig op een beveiligde locatie. In het geval van een calamiteit moeten deze gegevens eenvoudig toegankelijk gemaakt kunnen worden.

03 Stel een beschikbaarheidsplan op, met daarin beschikbaarheidseisen per systeem, activiteiten, rollen en verantwoordelijkheden, uit te voeren validaties en escalatiepaden.

04 Test en evalueer het beschikbaarheidplan periodiek.
De back-up- en restoreprocedures worden regelmatig getest op doelmatigheid.

hersteld en voortgezet

05 Stel hersteltijden van webapplicaties vast.
Er zijn recoveryprocedures vastgesteld en geïmplementeerd, en back-up en restore maken hier onderdeel vanuit.
De restoreprocedure wordt periodiek getest.

75 http://www.computable.nl/artikel/producten/cloud_computing/4279284/2333364/escrow-alliance-introduceert-cloud-escrow.html

Er worden aantoonbaar follow-up gegeven; verbeteringen doorgevoerd indien geïmplementeerde maatregelen niet voldoen aan de gestelde eisen of verwachtingen, of tekortkomingen opleveren.

C.11 Configuratiebeheer

Omschrijving

Configuratiebeheer draagt zorg voor de vastlegging van gegevens over de ICT-middelen en ICT-diensten mede voor het beschikbaar stellen van deze gegevens aan andere ICT-beheerprocessen. In deze richtlijnen voor webapplicaties beperken we ons specifiek tot het configuratie-item website. Organisaties kunnen er voor kiezen om websites als configuratie-item gedetailleerder op te delen in meerdere webcomponenten.

Websites die niet meer worden gebruikt,[76] dienen niet meer live te staan en te worden verwijderd. Ook de informatie die op de 'oude' website(s) is gepubliceerd en koppelingen met backoffice systemen moeten worden verwijderd.

Beveiligingsrichtlijn C.11

Configuratiebeheer inrichten

Richtlijn (wie en wat)
Het configuratiebeheer is procesmatig ingericht en zorgt ervoor dat slechts operationele websites in gebruik zijn.

Doelstelling (waarom)
Het voorkomen van misbruik van 'oude' en niet meer gebruikte websites en/of informatie.

Risico
Oude websites kunnen enerzijds de dienstverlening aan de klanten negatief beïnvloeden en kunnen anderzijds misbruikt worden.

Classificatie
Hoog

Richtlijn 2012
Bo-4, Bo-13

Maatregelen

procesmatig

01 Neem websites conform wijzigingsbeheerprocessen in productie.

operationele websites

02 Voer periodiek controles uit of de operationele websites nog worden gebruikt of informatie bevatten die kan worden verwijderd.
03 Houd een overzichtslijst bij van de websites die operationeel zijn inclusief de daarbij vermelde eigenaren.

76 Denk hierbij aan oude marketingacties, verlopen promotiecampagnes of testdoeleinden

Bijlagen

BIJLAGE A
» CONFORMITEITSINDICATOREN

aanmelden
Bij het aanmelden verandert het autorisatieniveau van de gebruiker. Op dat ogenblik vervalt de sessie die geldig was voor het oude autorisatieniveau, en wordt die vervangen door een nieuwe sessie (en nieuwe sessie-identifier).

analyseren
Het ontleden en onderzoeken van de vastgelegde loggingsgegevens op bedreigingen en of ongeoorloofde activiteiten.

architectuurvoorschriften
De architectuurvoorschriften zijn een levend document, dat bijdraagt aan een samenhangend en consistent geheel van technieken en maatregelen.

automatiseren van arbeidsintensieve taken (workflow)
Het automatiseren van arbeidsintensieve taken heeft betrekking procesmatige en procedurele inrichting van toegangsvoorzieningsomgeving. De processen die hierbij een rol spelen zijn bijvoorbeeld aanmaken, wijzigen en verwijderen van gebruikersinformatie en bijbehorende autorisaties (de complete levenscyclus). Hiermee is het op- afvoeren van gebruikers eenvoudiger te regelen en te beheren. Het identiteit- en toegangsmanagementsysteem dat hiervoor wordt ingezet zal deze processen moeten ondersteunen.

baseline
Een baseline geeft het afgewogen minimale beveiligingsniveau waaraan een organisatie moet (willen) voldoen.

bedrijfsprocessen
Alle bedrijfsprocessen, functies, rollen, et cetera die bij het aanbieden, gebruiken en onderhouden van een webapplicatie betrokken zijn, zijn geïnventariseerd en gekarakteriseerd.

beheer- en productieverkeer
Binnen de netwerkinfrastructuur zijn compartimenten aangebracht. Binnen deze compartimenten geldt een gelijk beveiligingsniveau voor het netwerkverkeer en de aangesloten systemen. Voor het beheer wordt een apart beheercompartiment gebruikt. Beheerverkeer vanuit het beheercompartiment blijft logisch gescheiden van het normale netwerkverkeer, door toepassing van cryptografische technieken.

beleid
Het beleid beschrijft hoe een organisatie haar missie op en visie richting wil geven. Een beleid is algemeen of specifiek van aard zijn. Een specifiek beleid is bijvoorbeeld een internetbeleid. Dit internetbeleid beschrijft hoe een organisatie op internet aanwezig wil zijn, bijvoorbeeld met een website. Hierin spelen inhoud, presentatie en veiligheid een hoofdrol.

bekende, toegestane communicatiestromen
Alles wat niet noodzakelijk is voor de (web)applicatie is verboden, om problemen met ongebruikte functionaliteit en protocollen te voorkomen. De veronderstelling is dat van de (web)applicatie bekend is wat deze nodig heeft en dat dit gedocumenteerd is. Het gevolg is dat alleen het verkeer dat gedocumenteerd is de lokale firewall mag passeren.

betrouwbare netwerkcomponenten
Netwerkcomponenten zijn alle typen systemen (zoals: router, firewall) die in de netwerk zijn opgenomen voor het verzorgen van juiste en veilige netwerkverbindingen. Deze systemen dienen adequaat op basis van een configuratiebaseline te zijn geconfigureerd. Niet relevante en niet noodzakelijke services zijn binnen deze systemen moeten uit voorzorg worden uitgeschakeld.

beveiligd
Beveiligde inrichting is gerelateerd aan maatregelen met betrekking tot juiste en tijdige werking en beschikbaarheid van de registratie en detectiefunctie, beveiliging van logbestanden tegen manipulaties, alternatieve paden bij uitval, veilig stellen van loggingbestanden. Juiste en tijdige werking houdt verband met bijtijds activeren van de registratiefunctie. Hiervoor is het van belang dat systeemklokken van systemen gesynchroniseerd zijn.

beveiligingseisen en -wensen
Beveiligingseisen ten aanzien van webapplicaties betreffen de te treffen maatregelen voor het beveiligen van webapplicaties zelf en het beveiligen van systemen, services en data bij het schenden van beveiligingsprocedures en bij het optreden van beveiligingsincidenten.

beveiligingsorganisatie
De beveiligingsorganisatie beschrijft de structuur van een divisie (of een entiteit) die verantwoordelijk is voor het vormgeven en effectief en efficiënt inzet van ICT-middelen. Hierbij dienen de

rollen, de uit te voeren activiteiten en de relaties tussen actoren als units te worden beschreven. Tevens is van belang dat binnen de beveiligingsorganisatie de procedurebeschrijving beschikbaar is die aangeven hoe functies en verantwoordelijkheden voor de beveiliging worden ingevuld. Een overzicht van de benoemde functies en daarbij behorende verantwoordelijkheden dient ook beschikbaar te zijn.

beveiligingsvoorschriften
De beveiligingsvoorschriften zijn een specifiek onderdeel van de architectuur, die eventueel in een losstaand document zijn vastgelegd. Zij dragen bij aan een veilige basis voor de realisatie van webapplicaties.

bewaken
Het (controleren) waarnemen en analyseren (proactief beheren) van informatie ten aanzien vastgelegde acties in het systeem (trendanalyse). Hierbij worden ook meetwaarden ten opzichte norm/planwaarden bewaakt bedoeld om uitzonderingen te signaleren (alarmeringen). Alarmeringen zijn automatische mededelingen door het detectie systeem voor een naderend gevaar of ongewenste situatie.

condities
Condities beschrijven de grenzen waarbinnen actoren op verschillende hiërarchische lagen mogen opereren. Zoals schillende beleid soorten (beveiligingsbeleid, PKI-beleid) waarin de beperkingen, richtinggevende adviezen en opties voor toepassingen worden vermeld.

configuratie-baseline
Voorschrift voor de configuratie van de webserver. Dit voorschrift zal in ieder geval enkele basale instellingen beschrijven om onnodig lekken van informatie tegen te gaan.

contract
Een formeel document waarin onder meer de overeengekomen functionele en beveiligingseisen zijn vermeld. De contracten worden slechts door daartoe bevoegde functionaris afgesloten. De contracten die hieruit voortkomen, dienen steeds actueel en geldig te zijn. Het verloop van de levering van diensten en middelen wordt, op basis van het contract, geëvalueerd.

controleerbaar maken van het gebruik
De toegang van gebruikers tot systemen moeten worden door het systeem geregistreerd voor controle doeleinden. Er moet kunnen worden vastgelegd, met name in fraude gevoelige omgevingen, welke gebruiker op basis van zijn/autorisatie welke acties heeft uitgevoerd.

cryptografische technieken
Gegevens worden beschermd tegen ongeautoriseerde kennisname en/of manipulatie door toepassing van cryptografische technieken.

periodiek proces
Het proces bevat een terugkoppel-mechanisme, zodat het beleid kan worden bijgestuurd en gecorrigeerd. Bekende voorbeelden zijn Plan-Do-Check-Act (PDCA) of Observe-Orient-Do-Act (OODA).

dataclassificatie
Informatie dient te worden geclassificeerd, om de behoefte aan, de prioriteit en de mate van beveiliging aan te geven. Het informatiebeveiligingsbeleid definieert gegevensgroepen (of -klassen). Hiervoor kan het teruggrijpen op de eisen uit wet- en regelgeving en de kenmerken van gegevensopslag en -verwerking binnen de organisatie. Binnen een gegevensklasse gelden naar aard en gewicht dezelfde beschermingsmaatregelen.

detectiemechanismen
Detectiemechanismen detecteren problemen of aanvallen in de communicatie. Voorbeelden zijn intrusion detection systeem en monitoringsystemen.

DMZ
In het kader van webapplicatie wordt met fysieke en logische domeinen de fysieke en logische inrichting van een sub-netwerk (een Demilitarised Zone (DMZ)) bedoeld die uit een verzameling hardware en software componenten bestaat en die fysiek en logisch met elkaar zijn verbonden. Door deze connecties is dit sub-netwerk in staat om specifieke (beveiligings)diensten te bieden.

documentatie
Vastleggen van de daadwerkelijk toegepaste inrichting, configuratie, samenhang en afhankelijkheden van (technische) componenten.

efficiënt en effectief
In het webapplicatiedomein worden vaak verschillende loggingmechanismen (registraties) naast elkaar gebruikt. Om de loggingsinformatie niet omslachtig, met beperkte inspanning en doeltreffend te kunnen analyseren is van belang deze te centraliseren.

eisen en wensen
Eisen en wensen bepalen zakelijke behoeften (functionele eisen) en niet-functionele eisen (beveiligingseisen) met betrekking tot toegangsvoorziening. De functionele eisen zijn gerelateerd aan de faciliteiten voor de medewerkers om op een efficiënte en effectieve manier zijn/haar taken te kunnen uitvoeren en de juiste resources (data) te kunnen benaderen. De niet-functionele eisen zijn gerelateerd aan de faciliteiten om beveiliging te kunnen realiseren.

functieprofielen
De taken binnen het beheer zijn bekend en verdeeld in verschillende groepen, de functieprofielen. Deze profielen zijn bedoeld om enerzijds tot een effectief takenpakket te komen, anderzijds tot een adequate functiescheiding (zie ook richtlijn U/TV.01en U/TV.01/02). De functieprofielen komen tot uitdrukking in de autorisaties van beheerders.

functionarissen
Binnen de informatiebeveiligingsorganisatie worden verschillende functionarissen, met specifieke beveiligingsrollen, onderscheiden.

fysieke en logische domeinen
De netwerk componenten kunnen, om onder andere beveiligingsredenen of fault tolerance, fysiek of logisch gegroepeerd worden in bepaalde domeinen. Een fysiek domein geeft aan hoe netwerkcomponenten fysiek met elkaar zijn verbonden, terwijl een logisch domein weergeeft hoe netwerkcomponenten door middel van protocollen zijn verbonden. De logische connecties kunnen over de grenzen van de fysieke domeinen heen gaan.

gegevensleveringen en transacties
De organisatie beschrijft welke gegevensleveringen en transacties onderdeel zijn van de reguliere en ad hoc processen, procedures en verwerkingen. De organisatie kan hierin zowel de leverende als de ontvangende partij zijn.
Bij elk van de leveringen en transacties wordt vastgelegd wat de voorwaarden zijn en welke zekerheden gerealiseerd moeten worden.
In plaats van concrete, individuele leveringen en transacties te benoemen kan de organisatie er ook voor kiezen het transactiebeleid te laten verwijzen naar de classificatie van hetgeen wordt uitgewisseld. Voor gegevensuitwisseling kan de dataclassificatie uit B.01/03 gebruikt worden.

hardeningbeleid
Het informatiebeveiligingsbeleid bevat een onderdeel expliciet gericht op hardening. De meeste computer- en netwerkapparatuur en softwarepakketten bevatten meer functionaliteit dan een organisatie nodig heeft voor het doel waarvoor deze is aangeschaft. Het hardeningbeleid beschrijft hoe de organisatie hiermee wil omgaan.

hardeningrichtlijn
Hardeningrichtlijnen geven voorschriften en/of aanwijzingen voor het veilig configureren van netwerken, platformen en webservers.

hersteld en voortgezet
Maatregelen zoals redundante actieve componenten en back-ups, om beschikbaarheidsincidenten te kunnen oplossen, zodat de dienstverlening gecontinueerd kan worden.

ICT-beveiligingsarchitectuur
Een ICT-beveiligingsarchitectuur bestaat uit een gelaagde architectuur. Deze gelaagde architectuur zorgt ervoor dat op elke laag de juiste maatregelen zijn genomen en noodzakelijke procedures beschikbaar zijn om de doelstellingen van de organisatie te realiseren.

instructies
De beschrijving van een reeks met elkaar verbonden activiteiten voor het configureren van infrastructuurcomponenten en periodiek controleren van deze componenten.

internetbeleid
Het internetbeleid beschrijft hoe een organisatie op internet aanwezig wil zijn, bijvoorbeeld met een website. Hierin spelen inhoud, presentatie en veiligheid een hoofdrol.

isolatie
Mechanismen om een proces af te schermen van zijn omgeving. Dit voortkomt dat het proces andere processen beïnvloedt casu quo door ander processen wordt beïnvloedt. Het voorkomt ook ongewenste toegang tot informatie doordat ook bestanden worden afgeschermd.

levensduur
Er dient een limiet gesteld te worden aan de maximale tijd dat een gebruiker inactief is. In voorkomende gevallen kan het ook gewenst zijn de maximale totale sessieduur te beperken. Hiermee worden de mogelijkheden voor een ongeautoriseerde derde om de sessie 'over te nemen' van de geautoriseerde gebruiker beperkt.

manipulatie
Manipulatie kan via de inhoud van de invoer tot stand komen, via het systeem waarop de webapplicatie is geïnstalleerd en via de geprogrammeerde controles. Manipulatie via de inhoud wordt door normaliseren en valideren afgevangen. Manipulatie op het niveau van de programmering en het systeem stelt eisen aan de manier waarop de webapplicatie is opgebouwd.

netwerkpaden
Beslissingen om een gebruiker toe te laten tot een webapplicatie zijn aan de toegangsvoorzieningen, niet aan de netwerkroutering. Het netwerk (de netwerkpaden en de routering) dient er voor te zorgen dat er geen manieren zijn om de toegangsvoorzieningen te omzeilen.

noodzakelijke functionaliteit
Functies die niet nodig zijn voor de functionaliteit van een (web) applicatie vormen een onnodig risico en dienen daarom achterwege te blijven.

normaliseren
Door invoer en uitvoer te normaliseren wordt voorkomen dat het ontvangende systeem gemanipuleerd kan worden via de webapplicatie. Normaliseren van inhoud betekent dat de inhoud gaat voldoen aan een aantal beperkende regels. Hierdoor wordt de mogelijkheid weggenomen om de validaties te omzeilen.

onderlinge samenhang
De samenhang tussen technische componenten en bedrijfsprocessen is gedocumenteerd. Dit geldt zowel voor de horizontale samenhang (gelijksoortige elementen) als verticale samenhang (ondersteunende elementen).

onweerlegbaarheid
Een belangrijke zekerheid ten aanzien van transacties is onweerlegbaarheid dat de transacties hebben plaatsgevonden. Er zijn verschillende redenen waarom een organisatie onweerlegbaarheid kan wensen. Denk hierbij aan financiële transacties of de levering van goederen of informatie.
Ook binnen het kader van een werkende keten, audit-trails en (de mogelijkheid voor) forensisch onderzoek kan onweerlegbaarheid een gewenste eigenschap zijn.

operationele websites
Alle websites die actief bijdragen in de dienstverlening van de organisatie.

opslag en distributie
Naast zorgvuldige processen en procedures voor het omgaan met sleutels, dienen de sleutels ook veilig te worden opgeslagen en gedistribueerd.

organisatorische inrichting
De aspecten ten aanzien van de organisatorische inrichting betreffen alle activiteiten van identiteit- en toegangsbeheer die moeten worden uitgevoerd om gebruikers en autorisaties voor webapplicaties te administreren en de naleving van regels hierover af te dwingen.
Gebruikersidentiteiten en autorisaties op webapplicaties zijn continue aan veranderingen onderhevig. Nieuwe gebruikers moeten worden aangemaakt en autorisaties worden uitgedeeld, bestaande gebruikers en autorisaties worden verwijderd of autorisaties van bestaande gebruikers worden ingeperkt. Vandaar dat deze toegangsvoorzieningsomgeving procesmatig en procedureel ingericht moet zijn.

organisatorische positie
De informatiebeveiligingsorganisatie dient zodanig gepositioneerd te zijn binnen de gehele organisatie, dat zij effectief invulling kan geven aan haar rol.

preventieve en detectieve instrumenten
Preventieve en detectieve instrumenten refereren naar intrusion- en detectie systemen die in de infrastructuur zijn opgenomen met als doel deze operationeel te bewaken. In het kader van governance is het van belang dat de informatie uit deze systemen gerelateerd wordt aan informatie uit andere bronnen. Hierdoor kunnen structurele risico's geïdentificeerd worden die om aandacht van het hoger management vragen.

procedure(el)
Het uitvoeren van handelingen volgens vast omschreven stappen.

procesmatig
Het uitvoeren activiteiten op basis van vooraf vastgestelde stappen of fasen die logisch met elkaar samenhangen om een doel te bereiken.

processen en procedures
Processen en procedures nodig zorgen ervoor dat handelingen volgens vast omschreven stappen en in vaste volgorde worden uitgevoerd, zodat de kwaliteit van uitvoering en daarmee de beveiliging van systemen geborgd kan worden.

protectiemechanismen
Protectiemechanismen zijn maatregelen die tot doel hebben te voorkomen dat bedreigingen tot verstoringen in de communicatie leiden. Voorbeelden zijn tunneling, hardening van componenten, anti-spoofingmechanismen en anti-virus.

protocollen
De webserver ondersteunt het http-protocol. Http kent methoden, headers en foutinformatie, die mogelijk misbruikt kunnen worden. Daarom is het gebruik hiervan beperkt tot het minimum dat noodzakelijk is voor de goede werking van de ontsloten webapplicaties.

queries en commando's
Bij het gebruik van geparameteriseerde queries is de syntax van de query statisch en wordt invoer alleen gebruikt om vooraf gedefinieerde variabelen te vullen. Door te voorkomen dat de syntax van de query wijzigt, voorkomt de webapplicatie SQL-injectieaanvallen. Geparametriseerde queries zijn ook efficiënter: doordat ze voorgedefinieerd zijn, gebruiken ze bekende tabelstructuren optimaal. Toch geven ze de gebruiker geen volledige vrijheid.
Op dezelfde manier voorkomen statisch geprogrammeerde commando's ervoor dat de gebruiker geen mogelijkheid heeft de aard van de commando's te beïnvloeden.

rapportages
Rapportages uit verschillende beheerdisciplines, zoals vulnerability assessment, penetratie testen en compliance assessment moeten aan elkaar gerelateerd en in samenhang geanalyseerd worden. Op basis van geconstateerde structurele risico's kunnen verbeterplannen worden opgesteld dan wel worden bijgesteld.

rapporteren
Het verschaffen van informatie door middel van een uitgebracht verslag over de geanalyseerde situatie.

redundantie
In de ICT-infrastructuur kunnen additionele systemen worden opgenomen die voor alternatieve paden zorg dagen. Zo kan bij falen van een netwerkcomponent de beschikbaarheid van de dienstverlening gegarandeerd worden.

registratie en detectie
De registratiefunctie houdt verband met het vastleggen van menselijke- en systeemgerichte acties en informatie over gebeurtenissen voor controle en analyse doeleinden. De detectiefunctie houdt verband met het (selectief) waarnemen van signalen voor het opsporen en blootleggen van ongewenste gebeurtenissen in de webapplicatie omgeving.

registratie-instrumenten
Registratie-instrumenten refereren naar logging en monitoring systemen. In de praktijk worden gescheiden logging en monitoring systemen per ICT-diensten laag (beveiligingslaag) geïmplementeerd. Voor analyse doeleinden is het effectiever om de geregistreerde informatie te centraliseren.

richtlijnen
Richtlijnen zijn nadere concretisering van diverse beleidstypen, zoals toegangsvoorzieningsbeleid en internetbeleid. Richtlijnen geven voorschriften en/of aanwijzingen voor de uitvoering van taken die leiden tot de invulling van deze beleidstypen.

risicoanalyse
Risicoanalyse levert inzicht in een situatie rondom een object, zoals een webapplicatie en infrastructuur. Het is van belang dat deze risicoanalyses gestructureerd en consequent worden uitgevoerd om op basis van de resultaten de juiste acties te nemen.

scope
De scope beschrijft de afbakening van de webapplicatie-omgeving. Hierin wordt vastgelegd welke onderdelen van het ICT-landschap deel uit maken van de webapplicatie-omgeving.

sessie zelf beëindigen
Wanneer de gebruiker besluit het werken met de (web)applicatie te beëindigen dient hij dit kenbaar te kunnen maken, zodat de sessie afgesloten kan worden. Hiermee wordt voorkomen dat een ongeautoriseerde derde de sessie kan 'overnemen' van de geautoriseerde gebruiker, nadat de laatste is gestopt met zijn werkzaamheden.

specifieke protocolkenmerken
Protocolkenmerken zijn de zogenaamde features van protocollen waarmee bepaalde functionaliteiten of diensten kunnen worden geboden. Zo kent het http-protocol ook een verzameling features. Slechts een beperkte deelverzameling van deze features levert veilige en betrouwbare communicatie. Onjuist gebruik geeft kwaadwillende derden mogelijkheden de communicatie te verstoren of de ontsloten webapplicaties te misbruiken, bijvoorbeeld door sessies van legitieme gebruikers te 'kapen'. Daarom is het noodzakelijk dat de webserver http alleen op een veilige en correcte manier ondersteunt.

taken, verantwoordelijkheden en bevoegdheden
De rol van de informatiebeveiligingsorganisatie worden vertaald naar taken, verantwoordelijkheden en bevoegdheden van de informatiebeveiligingsorganisatie en haar functionarissen.

technische componenten
Technische componenten representeren infrastructuur en software componenten. Elke technische en of applicatie omgeving ken een verzameling componenten die gezamenlijke een dienst leveren. Zo heeft een webapplicatie omgeving een verzameling technische componenten op basis waarvan webapplicatieve diensten worden geleverd. Het is van belang inzicht te hebben in deze verzameling componenten.

(technische) evaluaties
Het uitvoeren van evaluaties van technische aspecten van webapplicatie,
» zoals codereview tijdens ontwikkelingstrajecten en
» het uitvoeren van periodieke (geautomatiseerde) blackbox scan.

technische inrichting
De technische inrichting betreft de technische vormgeving van de toegangsvoorzieningen van de webapplicatie. Een juiste inrichting kan risico's van (systeem)misbruik aanzienlijk verminderen door rechten op een systeem te beperken. De manier waarop rechten op het systeem beperkt kunnen worden, is afhankelijk van het besturingssysteem en de technische richtlijnen met betrekking tot toegangsbeheer.
Zaken die bij de technische inrichting een rol spelen zijn onder meer:
» inrichting van toegangsvoorziening en beheer (identificatie, authenticatie en autorisatie) Hierbij zijn organisatorische aspecten: rollen en profielen van belang,
» centraal of decentraal van opzet,
» inrichting van gebruikers- en beheerdersaccounts,
» beperkte toegang tot accounts met hoge privileges,
» technische configuratie van onderliggende infrastructurele systemen.

testen
Het testen van doorgevoerde wijzigingen in de test omgeving. Hierbij is het van belang te weten wat er getest gaat worden (het testobject), waarmee er vergeleken gaat worden; (de testbasis), wanneer er getest gaat worden en hoe er getest gaat worden.

tijdig en geautoriseerd
Wijzigingen worden bijtijds ingediend en in behandeling genomen anders bestaat het risico dat noodzakelijke verbeteringen of de instandhouding van de beveiliging van de webapplicatie in het gedrang komt. Wijzigingen worden geautoriseerd anders bestaat het risico dat ongewenste (neven)effecten hebben op de webapplicatie. De initiator van de wijziging overziet niet altijd alle wijzigingen. Het is daarom van belang alle wijzigingen gestructureerd in kaart te brengen en de impact af te stemmen met alle belanghebbenden, zoals de eigenaar en de beheerders van de webapplicatie.

toegangsvoorziening
Het toegangsvoorzieningsbeleid als onderdeel van het informatiebeveiligingsbeleid bepaalt welke medewerkers onder wat voor voorwaarden toegang hebben tot welke gegevens en de activiteiten die hiermee kunnen en mogen worden uitgevoerd. Hierbij kan het beleid voortbouwen op de wet- en regelgeving en de dataclassificatie. Naast zaken als authenticatie en algemene autorisatie van een gebruiker, kunnen hierin ook nadere autorisatie regels opgenomen worden, zoals locatie en tijdstip.

toekennen van de rechten
Alle personen met toegang tot zakelijke toepassingen, informatie systemen, netwerken en computerapparatuur moet worden geautoriseerd, op basis van hun rollen en autorisatieprofielen, voordat toegangsrechten worden toegekend.

uitvoer
Uitvoer refereert aan informatie aan gebruiker en/of informatie over de inrichting van de applicatie zelf. Dit laatste houdt in dat bijvoorbeeld een webapplicatie zo is geconfigureerd dat hiervan informatie over de inrichting kan worden verstrekt. Om misbruik te voorkomen moeten webapplicatie zo zijn geconfigureerd dat de webapplicatie geen informatie geeft over de interne werking of configuratie van de webapplicatie zelf of een van de systemen waarmee de webapplicatie samenwerkt.

valideren
Valideren van de inhoud zorgt ervoor dat alleen geldige gegevens verwerkt worden. Validatie vindt zowel op protocol-niveau (meestal http) als op applicatie-niveau plaats. Het doel is te voorkomen dat de software op het betreffende niveau in misbruikt wordt of faalt door de door de gebruiker aangeleverde gegevens.

vaststellen van de identiteit
Gebruikers doorlopen een aanvraagproces voordat ze worden voorzien van toegang tot zakelijke toepassingen, informatie systemen, netwerken en computerapparatuur. Bij het inloggen zal het identiteit- en toegangsmanagementsysteem de identiteit moeten vaststellen. Hiervoor zullen moeten voldoen aan bepaalde wachtwoord- en toegangsvoorzieningsbeleid (B.02) die tevens door het toegangssysteem wordt afgedwongen.

veilige (communicatie)protocollen
Er kan onderscheid gemaakt worden tussen veilige en onveilige (communicatie)protocollen. Onveilige protocollen kunnen worden afgeluisterd, voorbeelden zijn Telnet en http. Door gebruik te maken van versleuteling (encryptie) via SSL of https wordt afluisteren voorkomen.

vertrouwelijkheid van transacties
Bij een deel van de transacties zal het noodzakelijk zijn de vertrouwelijkheid te waarborgen. Dit heeft betrekking op de communicatie die voor de transacties nodig is, maar ook op de opslag van authenticatiegegevens die nodig zijn om een transactie aan te (willen) gaan.

voorschriften
Regels bedoeld voor het beheersen of reguleren van het gedrag van personen en organisaties.

werkinstructies
Zie instructies.

wet- en regelgeving
Het informatiebeveiligingsbeleid vermeldt de relevante wet- en regelgeving die van toepassing is op de (geautomatiseerde) gegevensopslag en -verwerking binnen de organisatie. Van deze wet- en regelgeving worden de relevante eisen op een rijtje gezet.

BIJLAGE B
» AFKORTINGEN

A	**ACL**	Access Control List
	AD	Active Directory
	ADH	Anonymous Diffie-Hellman
	Ajax	Asynchronous JavaScript and XML
	API	Application Programming Interface
	APIDS	Application-based Intrusion Detection System
	ASVS	Application Security Verification Standard
B	**BGP**	Border Gateway Protocol
	BREIN	Bescherming Rechten Entertainment Industrie Nederland
	BSN	Burgerservicenummer
C	**CA**	Certification Authority
	CDP	Cisco Discovery Protocol
	CIS	Center for Internet Security
	CMDB	Configuration Management Database
	CMS	Content Management System
	CP	Certificate Policy
	CPS	Certification Practice Statement
	CPU	Central Processing Unit
	CSRF	Cross-Site Request Forgery
	CRL	Certificate Revocation List
	CSS	Cascading Style Sheet
D	**DAC**	Discretionary Access Control
	DBA	Database Administrator
	(D)DoS	(Distributed) Denial-of-Service
	DHCP	Dynamic Host Configuration Protocol
	DMZ	Demilitarised Zone
	DN	Distinguished Name
	DNO	Diensten Niveau Overeenkomst
	DNS	Domain Name Services
	DNSSEC	DNS Security Extensions
	DOM	Document Object Model
	(D)DoS	(distributed) Denial-of-Service
	DRP	Disaster Recovery Plan
E	**EPFW**	End-Point Firewall
	ESAPI	Enterprise Security Application Programming Interface

	EV SSL	Extended Validation SSL (Certificates)
F	**FTP**	File Transfer Protocol
	FTPS	FTP over SSL
G	**GIAC**	Global Information Assurance Certification
	GID	Group Identifier
	GPO	Group Policy Object
	GSLB	Global Server Load Balancing
H	**HIDS**	Host-based Intrusion Detection System
	HTML	Hypertext Markup Language
	HTTP	Hypertext Transfer Protocol
	HTTPS	Hypertext Transfer Protocol Secure
	HSM	hardware security module
I	**IAAS**	Infrastructure-as-a-service
	I&AM	Identity and Access Management
	IANA	Internet Assigned Numbers Authority
	IDMS	Intelligent DDoS Mitigation System
	IDS	Intrusion Detection System
	IIS	Internet Information Services/Server
	IM	Instant Messaging
	IP	Internet Protocol
	IPS	Intrusion Prevention System
	ISAPI	Internet Server Application Program Interface
	ISP	Internet Service Provider
	ISS	Internet Security Systems
	ISSA	Information Systems Security Association
J	**JSON**	JavaScript Object Notation
L	**LAN**	Local Area Network
	LDAP	Lightweight Directory Access Protocol
	LSLB	Local Server Load Balancing
M	**MAC**	Mandatory Access Control
	MAC	Media Access Control
	MTA	Mail Transfer Agent
	MTU	Maximum Transmission Unit
N	**NAT**	Network Address Translation
	NCSC	Nationaal Cyber Security Centrum
	NetBIOS	Network Basic Input Output System
	NetBT	NetBIOS over TCP/IP
	NIDS	Network-based Intrusion Detection System
	NORA	Nederlandse Overheid Referentie Architectuur
	NTP	Network Time Protocol
O	**OASIS**	Organization for the Advancement of Structured Information Standards
	OODA	Observe-Orient-Do-Act
	OS	Operating System
	OSI	Open System Interconnection
	OSPF	Open Shortest Path First
	OTAP	Ontwikkel, Test, Acceptatie en Productie
	OWA	Outlook Web Access
	OWASP	Open Web Application Security Project
P	**PAAS**	Platform-as-a-service
	PDCA	Plan-Do-Check-Act
	PFW	Perimeter Firewall
	PHP	PHP: Hypertext Preprocessor
	PKI	Public-Key Infrastructure
	PL/SQL	Procedural Language/Structured Query Language
	POP	Post Office Protocol
	PVIB	Platform voor Informatiebeveiliging
R	**RA**	Registration Authority
	RBAC	Role-based Access Control
	RBW	Raamwerk Beveiliging Webapplicaties
	RDP	Remote Desktop Protocol
	REST	Representational State Transfer
	RFC	Request For Comments
	RFC	Request for Change
	RFI	Remote File Inclusion
	RP	Reverse Proxy
	RSS	Really Simple Syndication (RSS 2.0)
	RSS	Rich Site Summary (RSS 0.91 en RSS 1.0)
	RSS	RDF Site Summary (RSS 0.9 en 1.0)
	RTBH	Remotely-Triggered Black Hole
S	**SAAS**	Software-as-a-service
	SAML	Security Assertion Markup Language
	SANS	SysAdmin, Audit, Network, Security
	SCP	Secure Copy
	SFTP	SSH File Transfer Protocol
	SIRT	Security Incident Response Team
	SIVA	Structuur, Inhoud, Vorm, Analysevolgorde (audit-methodiek)
	SLA	Service Level Agreement
	SMTP	Simple Mail Transfer Protocol
	SN	Serial Number
	SNMP	Simple Network Management Protocol
	SOAP	Simple Object Access Protocol
	SPoF	Single Point-of-Failure
	SQL	Structured Query Language
	SSD	Secure Software Development
	SSH	Secure Shell
	SSL	Secure Sockets Layer

	SSO	Single Sign-On/Single Sign-Out
	STP	Spanning Tree Protocol
T	**TCP**	Transport Control Protocol
	TFTP	Trivial File Transfer Protocol
	TLS	Transport Layer Security
	TTL	Time-To-Live
U	**UDP**	User Datagram Protocol
	UID	User Identifier
	URL	Uniform Resource Locator
	uRPF	Unicast Reverse-Path-Forwarding
V	**VA**	Vulnerability Assessment
	VLAN	Virtual LAN
	VoIP	Voice over IP
	VPN	Virtual Private Network
W	**WAF**	Web Application Firewall
	WAS	Web Application Scanner
	WASC	Web Application Security Consortium
	Wbp	Wet bescherming persoonsgegevens
	Wcc	Wet computercriminaliteit
	WebDAV	Web-based Distributed Authoring and Versioning
	WEH	Wet Elektronische Handtekeningen
	WSDL	Web Service Description Language
	WS-Trust	Web Services Trust
	WSUS	Windows Server Update Services
X	**XML**	eXtensible Markup Language
	XSRF	Zie CSRF
	XSS	Cross-Site Scripting

BIJLAGE C
» REFERENTIES

Nr.	Omschrijving
[1]	NCSC 'Raamwerk Beveiliging Webapplicaties', versie 2.0, de dato 4 november 2010 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/raamwerk-beveiliging-webapplicaties.html
[2]	OWASP Top 10 Application Security Risks – 2013 https://www.owasp.org/index.php/Top_10_2013
[3]	OWASP Testing Guide v3, de dato 2 november 2008 https://www.owasp.org/index.php/OWASP_Testing_Guide_v3_Table_of_Contents
[4]	OWASP Code Review Guide https://www.owasp.org/index.php/OWASP_Code_Review_Guide_Table_of_Contents
[5]	OWASP Application Security Verification Standard (ASVS) http://code.google.com/p/owasp-asvs/wiki/ASVS
[6]	NEN-ISO/IEC 27001:2013 'Managementsystemen voor informatiebeveiliging' http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270012013-en.htm
[7]	NEN-ISO/IEC 27002:2013 'Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging' http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270022013-en.htm
[8]	NEN-ISO/IEC 27005:2011 'Information security risk management' http://www.nen.nl/NEN-Shop/Norm/NENISOIEC-270052011-en.htm
[9]	Basisnormen Beveiliging en Beheer ICT-infrastructuur Deze norm is uitgegeven door het Platform voor InformatieBeveiliging (PVIB) in 2003, ISBN 90-5931-228-7.
[10]	NORA Dossier Informatiebeveiliging, versie 1.3 http://e-overheid.nl/onderwerpen/architectuur-en-nora/982-dossier-informatiebeveiliging
[11]	NCSC whitepaper 'Cloudcomputing', versie 1.0, de dato 19 december 2011 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-cloudcomputing.html
[12]	NCSC whitepaper 'Aanbevelingen ter bescherming tegen Denial-of-Service-aanvallen', versie 1.1, de dato 20 november 2006 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/bescherming-tegen-ddos-aanvallen.html
[13]	NCSC whitepaper "Patchmanagement", versie 1.1, de dato 30 juni 2008 https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/patchmanagement.html
[14]	CWE/SANS Top 25 Software Errors http://cwe.mitre.org/top25/

Overige referenties/bronnen/literatuur waar gebruik van is gemaakt zijn:

» Wikipedia – 'Gebruiker' , 'Gebruikersnaam' en 'Gebruikersgroep'
» Logius: Gebruiksvoorwaarden DigiD - https://www.digid.nl/voorwaarden/
» Ehow: Dynamic Separation of Duties - http://www.ehow.com/info_8671842_dynamic-separation-duties.html
» SANS: Role Based Access Control to Achieve Defense in Depth - http://www.sans.edu/research/security-laboratory/article/311
» NGI: Taken, Functies, Rollen en Competenties in de Informatica, Den Haag 2001 - https://www.ngi.nl/TakenEnFuncties/Takenfunctiesrollen_en_competenties.pdf
» Platform Informatiebeveiliging Studie Role Based Access Control, Versie 1.0, November 2005 - http://www.pvib.nl/download/?id=6391714&download=1
» Feisty Duck Limited – 'OpenSSL Cookbook', Version 1.1, de dato October 2013 - https://www.feistyduck.com/library/openssl-cookbook/
» Qualys SSL Labs – 'SSL/TLS Deployment Best Practices', version 1.3, de dato 17 September 2013 - https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf
» Qualys SSL Test - https://www.ssllabs.com/ssltest/

Deze beveiligingsrichtlijnen zijn tot stand gekomen in een publiek-private samenwerking mede door waardevolle inbreng van de volgende deskundigen:

Eric Nieuwland (Inspearit)
John van Huijgevoort (NCSC)
Michiel Oosterwijk (NCSC)
Koen Sandbrink (NCSC)
Wiekram Tewarie (UWV)

BIJLAGE D
» AANVALSMETHODEN

Aanvalsmethoden	Omschrijving
(Distributed) Denial-of-Service	Denial-of-Service-aanvallen (DoS) zijn elektronische aanvallen die een systeem, dienst of netwerk zo belasten dat ze niet meer beschikbaar zijn. Dit kan door de systemen uit te schakelen of een netwerk te overladen met dataverkeer. Een Denial of Service kan van een enkel systeem afkomstig zijn, maar ook van meerdere systemen tegelijkertijd. Een DoS-aanval vanaf meerdere systemen heet in jargon een Distributed-Denial-of-Service (DDoS).
Brute force	Brute force is het gebruik van rekenkracht om een 'probleem' op te lossen. De methode bestaat uit het botweg uitproberen van alle combinaties van toegestane tekens, net zolang tot diegene gevonden is die overeenkomt met de gewenste invoer.
Bufferoverflow	Bufferoverflows in het platform kunnen door kwaadwillenden worden misbruikt om willekeurige code uit te voeren op de webserver. In sommige gevallen biedt een bufferoverflow alleen mogelijkheden om de kwetsbare service te laten crashen. Het probleem bij een bufferoverflow is dat een kwetsbare applicatie data wil opslaan buiten de geheugenbuffer die voor deze applicatie is gereserveerd. Het gevolg hiervan is dat de applicatie geheugen in aanliggende geheugengebieden overschrijft. Een kwaadwillende kan het geheugen hierdoor mogelijk vullen met een eigen programma en dit programma vervolgens laten uitvoeren. Een bufferoverflow op het platform kan vooral tot grote problemen leiden wanneer deze zich bevindt in een centraal onderdeel van het platform dat bovendien moeilijk af te schermen is voor kwaadwillenden. Hierbij valt te denken aan een kwetsbaarheid in de implementatie van TCP/IP.
Clickjacking	Bij clickjacking wordt een webpagina geladen in een iframe binnen een website die de aanvaller heeft opgezet. Gebruikers worden naar die opgezette website gelokt via bijvoorbeeld phishing en worden daar verleid ogenschijnlijk eenvoudige handelingen met de muis te verrichten. De website bevat echter scripts die ervoor zorgen dat het frame met de aangevallen webpagina onzichtbaar is, maar wel op de voorgrond is geplaatst. Hierdoor zullen de muisklikken en -bewegingen niet op de opgezette site, maar op de aangevallen pagina worden uitgevoerd. Als de gebruiker gelijktijdig in de aangevallen webapplicatie is ingelogd terwijl de website van de aanvaller wordt geopend, zal de gebruiker ongemerkt handelingen verrichten die de aanvaller wenst te doen.
Cross-Site Scripting (XSS)	Cross-Site Scripting (XSS) is 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.
Guest-hopping	Guest-hopping maakt gebruik van kwetsbaarheden in de hypervisor, die het mogelijk

maken om de beveiliging, die strikte scheiding tussen verschillende virtuele machines moet garanderen, te compromitteren. Op deze manier wordt toegang verkregen tot andere virtuele machines of zelfs de hypervisor. Over het algemeen wordt gebruik gemaakt van de zwakste schakel, de minst beveiligde virtuele machine op het systeem. Die wordt gebruikt als vertrekpunt om aanvallen op andere virtuele machines uit te voeren. Op deze manier wordt van de ene naar de andere virtuele machine gesprongen.
Bijvoorbeeld: Een aanvaller is geïnteresseerd in de gegevens van virtuele machine A, maar is niet in staat om direct tot A door te dringen. Dan zal de aanvaller proberen om virtuele machine B aan te vallen en vanaf deze virtuele machine proberen om toegang te krijgen tot A.

Hyperjacking

Hyperjacking is een methode waarbij een 'rogue' hypervisor onder de bestaande legitieme infrastructuur (hypervisor of besturingssysteem) wordt geïnstalleerd, met controle over alle acties tussen het doelwit en de hardware. Voorbeelden van hyperjacking zijn Blue Pill[77] en Vitriol[78].

Man-in-the-middle (MitM)

Bij man-in-the-middle (MitM) bevindt de aanvaller zich tussen een klant en een dienst. Hierbij doet hij zich richting de klant voor als de dienst en andersom. De dienst kan hier bijvoorbeeld een internetwinkel zijn. Als tussenpersoon kan de aanvaller nu uitgewisselde gegevens afluisteren en/of manipuleren.

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.

Replay

Bij een 'replay'-aanval wordt een legitieme sessie van een doelwit opnieuw afgespeeld (meestal vastgelegd door het afluisteren van het netwerkverkeer).

Session fixation

Bij session fixation bepaalt een aanvaller van tevoren de sessie-id (meestal in een cookie) van een slachtoffer, voordat hij of zij inlogt. Nadat het slachtoffer inlogt, kan de aanvaller meeliften op de sessie met de door hem gekozen id.

Side channel

Een 'side channel'[79] - aanval maakt gebruik van een virtuele machine, die aanvallers hebben geïnstalleerd. Deze virtuele machine kan worden geïnstalleerd door gebruik te maken van kwaadaardige software of door zelf nieuwe virtuele machines af te nemen bij de cloudleverancier.
Deze 'kwaadaardige' virtuele machine kan vervolgens gedeelde resources monitoren van andere virtuele machines. Deze resources bestaan uit geheugen en processoren op de gedeelde fysieke machine. Door deze gegevens te verzamelen en te analyseren, wordt het 'makkelijker' om vast te stellen wanneer een andere virtuele machine aangevallen kan vallen. Het is zelfs mogelijk om via zogenaamde 'keystroke timing attacks'[80], wachtwoorden en andere gevoelige informatie van een virtuele machine te achterhalen.

Social engineering

Een aanvalstechniek waarbij misbruik wordt gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht met als doel vertrouwelijke informatie te verkrijgen of het slachtoffer een bepaalde handeling te laten verrichten.

77 http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html
78 http://www.blackhat.com/presentations/bh-usa-06/BH-US-06-Zovi.pdf
79 http://people.csail.mit.edu/tromer/papers/cloudsec.pdf
80 http://www.ece.cmu.edu/~dawnsong/papers/ssh-timing.pdf

Sniffing

Sniffing is het onderscheppen en lezen van informatie, zoals e-mailberichten of gebruikersnamen en wachtwoorden. Afluisteren wordt ook wel 'sniffing' genoemd.

Spoofing

Spoofing is jezelf voordoen als een ander. Iemand kan het e-mailadres van een ander gebruiken als zogenaamd afzendadres, zodat de geadresseerde in verwarring raakt. Deze methode kan handig zijn voor de verspreiding van virussen, omdat de ontvanger zou kunnen denken dat de afzender betrouwbaar is. Spoofing gebeurt ook op netwerkniveau, veelal met het doel internetverkeer in de war te schoppen.

SQL-injectie

Veel webapplicaties maken gebruik van een database om daarin allerlei informatie op te slaan. De informatie die een dergelijke database kan bevatten, is zeer gevarieerd. Denk bijvoorbeeld aan gebruikersnaam en wachtwoord voor besloten gedeelten van de website, nieuwsberichten, logging van bezochte pagina's, et cetera. Om de informatie uit de database beschikbaar te maken op de website, voert de code achter een website allerlei verzoeken naar de database uit, op het moment dat de gebruiker een pagina van de website opent. Dit soort verzoeken maakt in veel gevallen gebruik van de standaard databasetaal 'Structured Query Language', kortweg SQL. Vaak kan de gebruiker daarbij de inhoud van het SQL-verzoek direct of indirect beïnvloeden via een zoekterm of een ander invoerveld. Kwaadwillende hebben de mogelijkheid om een extra SQL-verzoek toe te voegen (injecteren), waardoor bijvoorbeeld de inhoud van de database wordt aangepast. We noemen dit verschijnsel dan ook 'SQL-injectie'. SQL-injectie kan plaats vinden als invoer van gebruikers op onvoldoende gecontroleerde wijze wordt verwerkt in een SQL-verzoek.
Deze bedreiging is niet nieuw maar wel relevant bij SaaS-diensten. De vraag is namelijk, hoe de cloudleverancier omgaat met de scheiding van data binnen databases van verschillende cloudgebruikers.

BIJLAGE E
» KWETSBAARHEDEN

E.1 Beleidsdomein

Kwetsbaarheden en bedreigingen
Deze paragraaf beschrijft kwetsbaarheden en bedreigingen die zich voor kunnen doen in het beleidsdomein.
Mogelijke kwetsbaarheden en bedreigingen zijn:

KB.01 Weerlegbaarheid

Toelichting
Er is sprake van weerlegbaarheid als de webapplicatie geen mogelijkheden biedt om belangrijke zaken rondom een transactie te bewijzen. De volgende zaken vallen onder de weerlegbaarheid van een transactie:
» De bron van een transactie.
Een zendende partij kan ontkennen dat een bepaald bericht van hem afkomstig is.
» Het tijdstip van een transactie.
Een zendende of ontvangende partij kan ontkennen dat een transactie op een bepaald tijdstip heeft plaatsgevonden.
» De ontvangst van een transactie.
Een ontvangende partij kan ontkennen dat deze een bepaalde transactie heeft ontvangen.
» De inhoud van een transactie (integriteit).
Een zendende of ontvangende partij kan ontkennen dat een transactie een bepaalde inhoud bevatte.

Misbruik van certificaten en de gevolgen daarvan zijn:

KB.02 Misbruik van een vals subcertificaat voor een specifiek domein

Toelichting
Misbruik van een vals subcertificaat voor een specifiek domein (bijvoorbeeld google.com). Dit kan bijvoorbeeld verkregen worden door toegang tot een filesysteem van een webdienst waarop dit certificaat wordt of door toegang tot een server die deze certificaten kan genereren.
Misbruik kan tot gevolg hebben dat de authenticiteit, vertrouwelijkheid en integriteit van de dragers van deze certificaten (websites, berichten, documenten, et cetera) niet meer gegarandeerd zijn en dat gevoelige informatie kan worden ontfutseld en schade kan worden geleden.

KB.03 Misbruik van een vals rootcertificaat

Toelichting
Misbruik van een vals rootcertificaat, waardoor alle sub certificaten van deze root niet meer vertrouwd zijn. Dit kan verkregen worden wanneer kwaadwillenden toegang hebben tot de servers van CA's die root certificaten genereren of opslaan.
Misbruik kan tot gevolg hebben dat de authenticiteit, vertrouwelijkheid en integriteit van de dragers van deze certificaten (websites, berichten, documenten, et cetera) niet meer gegarandeerd zijn en dat gevoelige informatie kan worden ontfutseld en schade kan worden geleden. Deze vorm is daarbij ernstiger omdat de reikwijdte groter is: kwaadwillenden kunnen in dat geval voor elk willekeurig domein certificaten genereren. Ook kunnen wellicht valse certificaten voor code signing of document signing gegenereerd worden.

E.2 Uitvoeringsdomein: toegangsvoorziening

Kwetsbaarheden en bedreigingen
Deze paragraaf beschrijft kwetsbaarheden en bedreigingen die zich voor kunnen doen op het gebied van identiteit- en toegangsbeheer.
Mogelijke kwetsbaarheden en bedreigingen zijn:

KU.01 Foutieve implementatie van authenticatie en sessiemanagement

Toelichting
Http kent geen mechanisme om de status van een sessie te behouden. Wanneer een gebruiker zich heeft geauthenticeerd tot een webapplicatie, is het wenselijk dat de webapplicatie onthoudt dat de gebruiker zich succesvol heeft geauthenticeerd. Anders zou de gebruiker zich bij elk volgend verzoek opnieuw moeten authenticeren en de historie van zijn acties binnen de webapplicatie verloren gaan.

Om de sessie tussen een gebruiker en een webapplicatie vast te stellen heeft de systeemontwikkelaar de volgende mechanismen ter beschikking:
» Sessie op basis van argumenten in de URL.
» Sessie op basis van verborgen velden.
» Sessie op basis van cookies.

Ongeacht de toegepaste manier van sessiemanagement kunnen problemen ontstaan. Hieronder worden twee van deze problemen beschreven:
» Een kwaadwillende ontdekt dat een webapplicatie gebruikmaakt van het verborgen veld genaamd 'userid'. Bij het initieel benaderen van de webapplicatie is dit verborgen veld leeg. Nadat de kwaadwillende probeert in te loggen met een standaard gebruikersnaam en wachtwoord mislukt dit en het veld 'userid' blijft leeg. De kwaadwillende probeert vervolgens om het inlogscherm te omzeilen en een verzoek aan de webapplicatie te richten waarin hij het verborgen veld 'userid' de waarde 'Blackhat' geeft. Hierna krijgt de kwaadwillende de melding 'Welkom Blackhat' en kan hij gebruik maken van de webapplicatie zonder zich geauthenticeerd te hebben. De webapplicatie vertrouwt in dit geval volledig op de waarde van het verborgen veld 'userid'.
» Een reguliere gebruiker logt in op de webapplicatie en ziet vervolgens dat in de URL continu de parameter 'sessieid=9001' terug te vinden is. De gebruiker vraagt zich af of hij deze parameter kan misbruiken door een andere waarde op te geven voor de sessieid. Nadat hij de waarde van de parameter verandert in 'sessieid=9000' is hij nog steeds geauthenticeerd en krijgt hij de gegevens te zien van een ander persoon die op dat moment ook is ingelogd. De webapplicatie blijkt gebruik te maken van oplopende sessieids die zeer eenvoudig te voorspellen zijn.

Authenticatie- en sessiemanagement zijn lastige onderdelen van een webapplicatie. Niet alleen het vaststellen van een sessie maar ook het uiteindelijk beëindigen van een sessie kan problemen met zich meebrengen. De volgende vraag doet zich in dit kader voor: hoe zorgen we ervoor dat de webapplicatie een sessie uiteindelijk ook weer afsluit? Sessies kunnen immers niet oneindig lang blijven bestaan. De aanwezigheid van een sessie zorgt aan de ene kant voor onnodig resourcegebruik op de server (de server moet alle sessies bijhouden en hiervoor geheugen reserveren) en daarnaast voor een beveiligingslek.

Hoe meer sessies een webserver op enig moment open heeft staan, hoe groter de kans dat een kwaadwillende erin slaagt één van deze sessies te kraken. En ook: hoe langer een sessie actief blijft, hoe langer eventueel onderschepte sessiegegevens bruikbaar blijven voor een kwaadwillende (denk bijvoorbeeld aan misbruik van een cookie in een internetcafé).

Referentie OWASP Top 10
» A2 - Broken Authentication and Session Management
https://www.owasp.org/index.php/Top_10_2013-A2

OWASP Application Security Verification Standard (ASVS)
» V2 - Authentication Verification Requirement
http://code.google.com/p/owasp-asvs/wiki/Verification_V2
» V3 - Session Management Verification Requirements
http://code.google.com/p/owasp-asvs/wiki/Verification_V3

KU.02 Foutieve implementatie van autorisatie

Toelichting
Vergelijkbare problemen als bij authenticatie- en sessiemanagement (zie vorige kwetsbaarheid) kunnen zich voordoen bij toegangsbeheer. Toegangsbeheer volgt op authenticatie en houdt in dat de webapplicatie controleert of een gebruiker gerechtigd is om bepaalde acties uit te voeren. Denk hierbij aan het mogen uitvoeren van een bepaalde transactie of het mogen bekijken van een specifieke webpagina.

De volgende voorbeelden illustreren implementatiefouten die ertoe kunnen leiden dat de webapplicatie deze autorisaties niet goed afhandelt:
» De webapplicatie voert geen normalisatie van het verzoek vanaf de gebruiker uit.
» De webapplicatie baseert de toegang tot de beveiligde directory op basis van de waarde van een cookie.
» Een kwetsbaar script binnen de webapplicatie voert geen goede invoervalidatie uit.

Referentie OWASP Top 10
» A7 - Missing Function Level Access Control
https://www.owasp.org/index.php/Top_10_2013-A7

OWASP Application Security Verification Standard (ASVS)
» V4 - Access Control Verification Requirements
http://code.google.com/p/owasp-asvs/wiki/Verification_V4

KU.03 Ongeautoriseerde directe objectreferenties

Toelichting
Zodra een gebruiker zich via een authenticatiemechanisme heeft geauthenticeerd op een webapplicatie, krijgt deze vervolgens de beschikking over de toegang tot verschillende typen objecten. Denk aan databaserecords, bestanden en directories. Een webapplicatie gaat goed om met de objecten die het de gebruiker aanbiedt, maar 'faalt' in het autoriseren wanneer de gebruiker de referenties naar objecten handmatig wijzigt.

Referentie OWASP Top 10
» A4 - Insecure Direct Object References
https://www.owasp.org/index.php/Top_10_2013-A4

KU.04 Onveilige authenticatiemechanismen

Toelichting

Niet alle authenticatiemechanismen die een webapplicatie kan gebruiken, zijn even veilig. Een belangrijk gevaar dat verbonden is aan het gebruik van authenticatiemechanismen, is de mogelijkheid tot het achterhalen casu quo onderscheppen hiervan. Als een kwaadwillende erin slaagt om authenticatiegegevens te achterhalen, kan deze zich voordoen als iemand anders.
Voor het onderscheppen van authenticatiegegevens heeft de kwaadwillende een aantal mogelijkheden:

» Phishing
» Social engineering
» Sniffing
» Cross-Site Scripting (XSS)

Ook standaard - en veel gebruikte -authenticatiemechanismen zijn niet per definitie veilig. Denk aan gebruikersauthenticatie op basis van het basic authentication mechanisme binnen http. Dit authenticatiemechanisme maakt gebruik van base64 encoding. Strings die op basis van base64 zijn gecodeerd, zijn ook eenvoudig weer te decoderen. Het is eenvoudig om via een simpele tool (base64 decoder) een gebruikersnaam en een wachtwoord uit deze string te 'toveren'. Als een kwaadwillende deze gegevens weet te sniffen, dan is het voor deze kwaadwillende zeer eenvoudig om de inhoud ervan te misbruiken.

Referentie OWASP Top 10

» A2 - Broken Authentication and Session Management
https://www.owasp.org/index.php/Top_10_2013-A2

KU.05 Discrepantie tussen authenticatiemechanisme en beveiligingsbeleid

Toelichting

Bij veel projecten besteedt men, als gevolg van bijvoorbeeld tijdsdruk, onvoldoende aandacht aan het projecteren van het beveiligingsbeleid van de organisatie op de webapplicatie en de bijbehorende data. Gevolg: de authenticatie is veel te 'zwaar' voor de data die de webapplicatie gebruikt, of de authenticatie is veel te 'zwak'. In geen van de gevallen is er sprake van een ideale situatie. In het tweede geval is er zelfs sprake van een beveiligingsrisico, omdat data onvoldoende beschermd bereikbaar is via internet. Discrepantie tussen het authenticatiemechanisme en het beveiligingsbeleid kan ook gedurende de levenscyclus van een webapplicatie ontstaan. Op het moment dat een nieuwe webapplicatie het levenslicht ziet, voert de organisatie bijvoorbeeld een risicoanalyse uit, waaruit voortvloeit dat de webapplicatie voldoende beschermd is op basis van gebruikersnaam/wachtwoord authenticatie. De webapplicatie groeit vervolgens een aantal jaren door waarbij de organisatie steeds meer functionaliteiten en data aan de webapplicatie toevoegt. Wat een organisatie vaak nalaat is, om regelmatig een risicoanalyse uit te voeren op de webapplicatie. Op een gegeven moment voldoet het gebruikte authenticatiemechanisme niet meer voor de gestaag doorgegroeide webapplicatie.

KU.06 Het wiel opnieuw uitvinden

Toelichting

De implementatie van authenticatie- en toegangsmechanismen is niet altijd triviaal. De implementatie ervan kan veel tijd en moeite in beslag nemen als het gaat om complexe authenticatiemechanismen (digitale certificaten, tokens) en complexe toegangsmatrices (veel rollen, veel resources). Bij iedere implementatie bestaat de kans op (beveiligings-) fouten, moeten beheermechanismen worden ingeregeld, moeten diepgaande testen worden uitgevoerd, et cetera.
Het is reëel dat een authenticatiemechanisme meerdere malen wordt uitgevonden, zeker als verschillende webapplicaties op verschillende manieren worden ontsloten en daarbij verschillende protocollen en technologieën worden gebruikt. Stel dat een organisatie start met een webapplicatie die gebruikers benaderen via hun webbrowser (op basis van HTML).
De webapplicatie is beschermd met een gebruikersnaam en een wachtwoord. Vervolgens besluit de organisatie om delen van de webapplicatie ook beschikbaar te stellen via een webservice (op basis van XML). Ook deze webservice wil men beschermen op basis van een gebruikersnaam en een wachtwoord. In veel gevallen moet je voor deze webservice een nieuw authenticatieproces inrichten. Dit terwijl het grootste gedeelte van het bestaande authenticatiemechanisme (in veel gevallen) herbruikt kan worden.

KU.07 Incompatibele authenticatiemechanismen

Toelichting

Wanneer je het wiel voor elke webapplicatie opnieuw uitvindt (§8.2.6), bestaat de kans dat webapplicaties een groot aantal verschillende authenticatiemechanismen implementeren om deze te beschermen. Deze incompatibiliteit kan tot verschillende problemen leiden.
Enkele van de meest voorkomende zijn:

» Bij het 'in elkaar schuiven' van verschillende webapplicaties (bijvoorbeeld verschillende bestaande webapplicaties achter een nieuw te ontwikkelen portaal) ontstaan problemen, omdat de verschillende authenticatiemechanismen ervoor zorgen dat gebruikers op elke afzonderlijke webapplicatie opnieuw moeten inloggen. Het is, met andere woorden, niet mogelijk om via één account toegang te verkrijgen tot de afzonderlijke webapplicaties (Single Sign-On).
» De beheertooling voor het ene authenticatiemechanisme is niet bruikbaar voor het andere. Gevolg hiervan is dat voor elk authenticatiemechanisme een apart beheerproces (inclusief achterliggende techniek) ingericht moet worden voor gebruikersbeheer, rollenbeheer, et cetera.
» Het is niet mogelijk een goed profiel op te bouwen van een gebruiker. Wanneer persoon A account A1 in webapplicatie 1 krijgt en account A2 in webapplicatie 2, zijn deze twee identiteiten veelal niet met elkaar te combineren of moeten hiervoor onevenredig veel activiteiten worden ondernomen. Hierdoor kun je geen geheel omvattend profiel van deze persoon maken en moeten webapplicaties overlappende gegevens ieder apart bijhouden (denk hierbij bijvoorbeeld aan een adreswijziging die elke webapplicatie afzonderlijk moet doorvoeren).

E.3 Uitvoeringsdomein: webapplicaties

Kwetsbaarheden en bedreigingen

Deze paragraaf beschrijft de meest voorkomende kwetsbaarheden in webapplicaties. De meest bekende kwetsbaarheden in webapplicaties zijn ongetwijfeld XSS en SQL-injectie. Ondanks deze bekendheid komen beide kwetsbaarheden nog steeds veelvuldig voor in webapplicaties. Deze twee kwetsbaarheden staan dan ook op nummer 1 en 3 in de OWASP Top 10 2013.
Mogelijke kwetsbaarheden en bedreigingen zijn:

KU.08 SQL-injectie

Toelichting

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.

Databases lijken tegenwoordig kleine besturingssystemen, aangezien de acties die men via queries (of stored procedures) kan uitvoeren steeds krachtiger en uitgebreider worden.
Hieronder volgt een kleine opsomming de mogelijkheden die SQL biedt:

» 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.
» Databases bieden vaak de mogelijkheid om DNS-verzoeken uit te voeren (bijvoorbeeld utl_inaddr.get_host_address in Oracle) waardoor men vanuit de database hostnamen kan omzetten naar ip-adressen.
» Vaak is het mogelijk om via de aanroep van een stored procedure (bijvoorbeeld xp_sendmail in Microsoft SQL Server), mail te versturen. Daarbij biedt de database vaak de mogelijkheid om de inhoud van de mail te baseren op de uitvoer van een query.
» Het inlezen van een webpagina behoort ook vaak tot de mogelijkheden van een database (bijvoorbeeld utl_http.request in Oracle).
» Sommige databases bieden zelfs de mogelijkheid om commando's op OS-niveau aan te roepen (bijvoorbeeld xp_cmdshell in Microsoft SQL Server).

Deze functionaliteiten kunnen zeer nuttig zijn voor ontwikkelaars en de mogelijkheid bieden om in korte tijd een complexe webapplicatie te implementeren. Nadeel is dat de schade door kwetsbaarheden in de webapplicatie erg groot kan worden. Daarom is SQL injectie een belangrijke bedreiging.

Een SQL-injectiekwetsbaarheid ontstaat door onvoldoende controles op de invoer van gebruikersdata en door onveilige programmeergewoonten. De aanwezigheid van een SQL-injectiekwetsbaarheid betekent dat iedereen vanaf internet in staat is om de SQL-verzoeken die de webapplicatie verstuurt naar de database, te manipuleren. Daarbij heeft de aanvaller vaak toegang tot alle functionaliteiten die de database biedt. De gevolgen van deze kwetsbaarheid zijn in grote mate afhankelijk van de programmalogica.
Een kwaadwillende kan:

» het authenticatiemechanisme van de webapplicatie omzeilen en op deze manier ongeautoriseerd 'inloggen' op de webapplicatie.
» gegevens in de database wijzigen.
» de volledige database verwijderen ('droppen') waardoor alle informatie uit de database verloren gaat.
» een eigen gebruikersaccount aanmaken en dit account gebruiken om toegang tot de webapplicatie te verkrijgen en te behouden.
» informatie aan de database of het onderliggende besturingssysteem onttrekken.
» malafide links in de database injecteren waardoor bezoekers van de website geïnfecteerd raken met malware.

Referentie OWASP Top 10

» A1-Injection
https://www.owasp.org/index.php/Top_10_2013-A1

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

» Data Validation Testing
  › Testing for SQL Injection (OWASP-DV-005)
  https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)
  Oracle Testing
  MySQL Testing
  SQL Server Testing
  MS Access Testing
  Testing PostgreSQL (from OWASP BSP)

OWASP Code Review Guide:

» Reviewing Code for SQL Injection
https://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection

KU.09 Cross-Site Scripting (XSS)

Toelichting

Een kwaadwillende kan via een kwaadaardige website veelal willekeurige JavaScript (en andere scripts) uitvoeren op het systeem van een gebruiker. De kwaadwillende heeft via deze scripts echter geen toegang tot mogelijk gevoelige informatie op het systeem van deze gebruiker, vanwege beperkingen die browsers opleggen aan de scripts die het uitvoert. Zo kan een kwaadwillende bijvoorbeeld nooit toegang krijgen tot de inhoud van cookies die gekoppeld zijn

aan een ander domein dan het domein van de kwaadwillende (same origin policy), omdat de browser toegang tot deze gegevens niet toestaat.
Via Cross-Site Scripting (XSS) is het echter mogelijk om deze beperkingen te omzeilen. Bij XSS slaagt een kwaadwillende erin om kwaadaardige JavaScript terug te laten komen in het antwoord van een vertrouwde website. Het antwoord van de website wordt hierbij met andere woorden deels bepaald door de invoer van de kwaadwillende. De kwaadwillenden slaagt hierin als bij een website alle onderstaande zaken van toepassing zijn:

» De website maakt gebruik van de invoer vanaf de client: om de uitvoer van de website te kunnen manipuleren moet een kwaadwillende malafide JavaScript kunnen injecteren via invoer naar de website.
» De website voert geen of onvoldoende controles uit op deze invoer.
» De website voert geen of onvoldoende controles uit op het antwoord dat deze terugstuurt aan de client.

De kwaadwillende kan XSS-kwetsbaarheden misbruiken om gevoelige informatie, zoals een sessie-ID, van een gebruiker te achterhalen.
Grofweg bestaan er drie soorten XSS: reflected XSS, stored XSS en DOM-based XSS.

Referentie OWASP Top 10

» A3-Cross Site Scripting (XSS)
https://www.owasp.org/index.php/Top_10_2013-A3

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

» Data Validation Testing
› Testing for Reflected Cross Site Scripting (OWASP-DV-001)
https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OWASPDV-001)
› Testing for Stored Cross Site Scripting (OWASP-DV-002)
https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OWASPDV-002)
› Testing for DOM based Cross Site Scripting (OWASP-DV-003)
https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OWASP-DV-003)

OWASP Code Review Guide:

» Reviewing Code for Cross-Site Scripting
https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting

KU.10 Cross-Site Request Forgery (CSRF)

Toelichting

Cross-Site Request Forgery (CSRF of XSRF-) kwetsbaarheden ontstaan wanneer een website onvoldoende autorisatiecontroles uitvoert op een bepaalde transactie. Hierdoor kan het gebeuren dat een gebruiker onbedoeld een transactie uitvoert op een website waarmee deze gebruiker een sessie heeft. Misbruik vindt als volgt plaats: de gebruiker bezoekt een malafide of geïnfecteerde website en krijgt via deze website een link aangeboden naar een andere website waarmee de gebruiker een sessie heeft en die de kwaadwillende wil aanvallen. De gebruiker merkt hier vaak niets van, maar onder water vindt een transactie plaats vanuit de browser van de gebruiker naar een website waar de gebruiker zich mogelijk eerder heeft geauthenticeerd.

Referentie OWASP Top 10

» A8-Cross Site Request Forgery (CSRF)
https://www.owasp.org/index.php/Top_10_2013-A8

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

» Session Management
› Testing for Cross Site Request Forgery (CSRF) (OWASP-SM-005)
https://www.owasp.org/index.php/Testing_for_CSRF_(OWASP-SM-005)

OWASP Code Review Guide:

» Reviewing Code for Cross-Site Request Forgery
https://www.owasp.org/index.php/Reviewing_Code_for_Cross-Site_Request_Forgery

KU.11 Lekken van informatie (Onbedoeld vrijgeven van 'teveel' informatie)

Toelichting

Webservers en webapplicaties kunnen op allerlei manieren technische informatie over zichzelf 'lekken'[81]. Deze informatie kan een kwaadwillende helpen om een beeld te krijgen van de omgeving waarin de webapplicatie zich bevindt. De kwaadwillende kan bijvoorbeeld bepalen of de webapplicatie gebruik maakt van kwetsbare software.

Uitgebreide foutmeldingen

Sommige webapplicaties leveren bij het optreden van een foutsituatie allerlei informatie aan over de achtergrond(en) van de fout. Een uitgebreide foutmelding kan een kwaadwillende helpen om meer inzicht te krijgen in de programmalogica van een webapplicatie. Een foutmelding vertelt vaak iets over de gebruikte database, het uitgevoerde SQL-verzoek of het aangeroepen bestand. Al deze informatie draagt bij aan kennisvorming van de kwaadwillende over de infrastructuur.

Header-informatie

Http-headers kunnen veel informatie bevatten over de webapplicatie en de software waarvan de webapplicatie gebruik maakt. Eén van de bekendste http-headers die informatie vrijgeeft, is de 'Server'-header. In veel gevallen zal de webserver via deze header informatie geven over het type webserver waar de pagina van afkomstig is. In sommige gevallen bevat deze header echter nog veel meer informatie.

Commentaarregels in scripts

Commentaarregels in code kunnen ongewild informatie vrijgeven. Vooral HTML-code en 'client-side scripts' (zoals JavaScript) bevatten vaak commentaar. Commentaarregels zijn niet altijd problematisch. In sommige gevallen bevat commentaar echter 'een geheugensteuntje' voor programmeurs en vergeten zij deze informatie te verwijderen zodra een webapplicatie in productie gaat.

Referentie OWASP Top 10

» A5 - Security Misconfiguration
https://www.owasp.org/index.php/Top_10_2013-A5
» A6 - Information Leakage and Improper Error Handling (Top 10 2007, vervallen sinds Top 10 2010)
https://www.owasp.org/index.php/Top_10_2007-A6

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

» Configuration Management
https://www.owasp.org/index.php/Testing_for_configuration_management
» Information Gathering
› Spiders, Robots and Crawlers (OWASP-IG-001)
https://www.owasp.org/index.php/Testing:_Spiders,_Robots,_and_Crawlers_(OWASPIG-001)
» Search Engine Discovery/Reconnaissance (OWASP-IG-002)
https://www.owasp.org/index.php/Testing:_Search_engine_discovery/reconnaissance_(OWASP-IG-002)
» Identify application entry points (OWASP-IG-003)
https://www.owasp.org/index.php/Testing:_Identify_application_entry_points_(OWASPIG-003)
» Testing for Web Application Fingerprint (OWASP-IG-004)
https://www.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASPIG-004)
» Application Discovery (OWASP-IG-005)
https://www.owasp.org/index.php/Testing_for_Application_Discovery_(OWASP-IG-005)
» Analysis of Error Codes (OWASP-IG-006)
https://www.owasp.org/index.php/Testing_for_Error_Code_%28OWASP-IG-006%29

OWASP Code Review Guide:

» Chapter on Error Handling
https://www.owasp.org/index.php/Error_Handling

OWASP Application Security Verification Standard (ASVS)

» V8 - Error Handling and Logging Verification Requirements
http://code.google.com/p/owasp-asvs/wiki/Verification_V8

KU.12 Http response splitting

Toelichting

Http werkt met vraag- en antwoordberichten. Bij het bezoeken van een website stuurt een browser diverse vragen (http-requests) aan een webserver die de webserver vervolgens beantwoordt. Eén vraag leidt daarbij normaal gesproken tot maximaal één antwoord. Bij http-response splitting aanvallen is dit niet het geval. Doordat de webapplicatie onvoldoende validatie van gebruikersinvoer uitvoert, geeft deze webapplicatie niet alleen het eigen antwoord terug, maar ook het antwoord dat in de gebruikersinvoer werd meegegeven. Zo is het mogelijk dat één http-request leidt tot meerdere logische http-responses. Dit is mogelijk op het moment dat de webapplicatie ongevalideerde gebruikersinvoer rechtstreeks gebruikt in een http-responseheader.

Referentie OWASP Top 10

» A1 - Injection
https://www.owasp.org/index.php/Top_10_2013-A1

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)

OWASP Testing Guide:

» Data Validation Testing
› Testing for HTTP Splitting/Smuggling - HTTP Splitting, Smuggling (OWASP-DV-016)
https://www.owasp.org/index.php/Testing_for_HTTP_Splitting/Smuggling_(OWASPDV-016)

KU.13 Remote File Inclusion (RFI)

Toelichting

Remote File Inclusion (RFI) is een kwetsbaarheid die zich voordoet op webservers die gebruik maken van dynamische file includes in script- en programmeertalen. Wanneer een dergelijke website kwetsbaar is voor RFI, kan een kwaadwillende zijn eigen code door de server laten uitvoeren. RFI is mogelijk op het moment dat een pagina op een webserver de volgende kenmerken heeft:

» De pagina is geschreven in PHP.
» De pagina maakt gebruik van andere PHP-scripts via een include (of een andere vergelijkbare functie).
» Gebruikersinvoer bepaalt de naam van de scripts waarvan de

81 Het gaat hier dus niet om mogelijk vertrouwelijke informatie uit een database maar over informatie over de gebruikte tech-nieken/technologieën op de server. Het lekken van vertrouwelijke informatie uit de database is een kwetsbaarheid op de laag 'Vertrouwelijkheid en onweerlegbaarheid' van het RBW.

pagina gebruik maakt.
» PHP staat URL includes toe (allow_url_include = 'On').

Of een aanval succesvol is, hangt ook af van de configuratie van de webserver. Als de PHP-optie allow_url_include bijvoorbeeld is ingesteld op de waarde 'Off', zal PHP het importeren van een PHP-script vanaf een externe locatie niet toestaan en zal het moeilijker zijn om deze RFI-kwetsbaarheid uit te buiten. Wel is het in dat geval nog steeds mogelijk om willekeurige lokale bestanden op de server (bijvoorbeeld /etc/passwd) te laten importeren door het script.

Ook als de webserver zelf geen verbinding met internet kan opzetten, is het nog steeds mogelijk een RFI-kwetsbaarheid uit te buiten. Hiervoor kan een kwaadwillende bijvoorbeeld gebruik maken van een base64 data include.

Referentie OWASP Top 10
» A5 - Security Misconfiguration
https://www.owasp.org/index.php/Top_10_2013-A5
» A3 - Malicious File Execution (Top 10 2007, vervallen sinds Top 10 2010)
https://www.owasp.org/index.php/Top_10_2007-A3

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
» Configuration Management
https://www.owasp.org/index.php/Testing_for_configuration_management

OWASP Application Security Verification Standard (ASVS)
V12 - Security Configuration Verification Requirements
http://code.google.com/p/owasp-asvs/wiki/Verification_V12

KU.14 Path traversal

Toelichting
Een webserver kent altijd een webroot waarvandaan de webserver alle bestanden voor een bepaalde webapplicatie 'serveert'. Het idee is dat gebruikers alleen toegang hebben tot bestanden onder de webroot en niet tot bestanden die zich in andere directories van het systeem bevinden. In sommige gevallen is het voor kwaadwillenden echter mogelijk om bestanden buiten de webroot te benaderen. We spreken in dit geval van een path traversal kwetsbaarheid. Path traversal kwetsbaarheden kunnen zich op twee niveaus voordoen: op het niveau van de webserver en op het niveau van de webapplicatie.

Referentie OWASP Top 10
» A4 - Insecure Direct Object References
https://www.owasp.org/index.php/Top_10_2013-A4

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
» Authorization Testing
› Testing for path traversal (OWASP-AZ-001)
https://www.owasp.org/index.php/Testing_for_Path_Traversal_(OWASP-AZ-001)

KU.15 Command-injectie

Toelichting
Command-injectie houdt in dat een kwaadwillende in staat is om commando's uit te voeren op het niveau van het besturingssysteem. Dit kan gebeuren op het moment dat de webapplicatie OS-commando's aanroept en daarbij gebruik maakt van ongevalideerde invoer van de gebruiker.
De mogelijkheden die een kwaadwillende heeft bij een command-injectiekwetsbaarheid zijn groot. In principe kan een kwaadwillende in dit geval alle ondersteunde OS-commando's aanroepen en wordt hij alleen beperkt door de rechten waaronder de webserver draait.

Referentie OWASP Top 10
» A1 - Injection
https://www.owasp.org/index.php/Top_10_2013-A1

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
» Data Validation Testing
› Testing for Command Injection (OWASP-DV-013)
https://www.owasp.org/index.php/Testing_for_Command_Injection_(OWASP-DV-013)

OWASP Code Review Guide:
» Reviewing Code for OS Injection
https://www.owasp.org/index.php/Reviewing_Code_for_OS_Injection

KU.16 Buffer overflows

Toelichting
Een buffer overflow doet zich voor op het moment dat een webapplicatie meer data naar een geheugenbuffer schrijft dan dat daar initieel voor was gereserveerd. Hierdoor komt data op plekken in het geheugen terecht waar dit eigenlijk niet had gemogen. Misbruik van een buffer overflow kan leiden tot het uitvoeren van code op het systeem; hierdoor kan een kwaadwillende in het ernstigste geval volledige controle over een systeem krijgen. Buffer overflows in webapplicaties zijn niet altijd eenvoudig te ontdekken en vaak moeilijk te misbruiken.

Referentie OWASP Top 10
» A1 - Injection
https://www.owasp.org/index.php/Top_10_2013-A1

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
» Data Validation Testing
› Testing for Buffer overflow (OWASP-DV-014)
https://www.owasp.org/index.php/Testing_for_Buffer_Overflow_(OWASP-DV-014)
Testing for Heap overflow
Testing for Stack overflow
Testing for Format string

Denial of Service Testing:
» OWASP-DS-003 Testing for DoS Buffer Overflows - Buffer Overflows
https://www.owasp.org/index.php/Testing_for_DoS_Buffer_Overflows_(OWASP-DS-003)
» OWASP Code Review Guide:
› Reviewing Code for Buffer Overruns and Overflows
https://www.owasp.org/index.php/Reviewing_Code_for_Buffer_Overruns_and_Overflows

KU.17 Fouten in applicatielogica

Toelichting
Fouten in de applicatielogica kunnen ertoe leiden dat kwaadwillenden ongewenste activiteiten uitvoeren via de webapplicatie met compleet legitieme verzoeken. Kortom een kwetsbare webapplicatie waar geen technische fouten aan ten grondslag liggen. Fouten in de applicatielogica kunnen zich op elke plek in de webapplicatie voordoen.

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
› Business Logic Testing (OWASP-BL-001)
https://www.owasp.org/index.php/Testing_for_business_logic_(OWASP-BL-001)

KU.18 Configuratiefouten

Toelichting
De configuratie van de webapplicatie en het applicatieplatform spelen een belangrijke rol in de beveiliging van het geheel. Door een webapplicatie en/of applicatieplatform te installeren zonder daarbij aandacht te besteden aan de configuratie ervan kunnen zich verschillende beveiligingsproblemen voordoen. Enkele voorbeelden hiervan zijn:
» Gebruik van standaardpaden voor de webroot.
» Gebruik van standaard gebruikersnamen en wachtwoorden.
» Aanwezigheid van standaard plug-ins.
» Ontbreken van patches.
» Ingeschakelde 'debugging'-opties.

Referentie OWASP Top 10
» A5 - Security Misconfiguration
https://www.owasp.org/index.php/Top_10_2013-A5

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
» Configuration Management Testing
› SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) (OWASPCM-001)
https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)
› DB Listener Testing (OWASP-CM-002)
https://www.owasp.org/index.php/Testing_for_DB_Listener_(OWASP-CM-002)
› Infrastructure Configuration Management Testing (OWASP-CM-003)
https://www.owasp.org/index.php/Testing_for_infrastructure_configuration_management_(OWASP-CM-003)
› Application Configuration Management Testing (OWASP-CM-004)
https://www.owasp.org/index.php/Testing_for_application_configuration_management_(OWASP-CM-004)
› Testing for File Extensions Handling (OWASP-CM-005)
https://www.owasp.org/index.php/Testing_for_file_extensions_handling_(OWASPCM-005)
› Old, Back-up and Unreferenced Files (OWASP-CM-006)
https://www.owasp.org/index.php/Testing_for_Old,_Back-up_and_Unreferenced_Files_(OWASP-CM-006)
› Infrastructure and Application Admin Interfaces (OWASP-CM-007)
https://www.owasp.org/index.php/Testing_for_Admin_Interfaces_(OWASP-CM-007)
› Testing for HTTP Methods and Cross Site Tracing (XST) (OWASP-CM-008)
https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASPCM-008)

KU.19 Geen invoervalidatie

Toelichting
Ongecontroleerde (ongevalideerde) invoer van gebruikers is de belangrijkste dreiging voor een webapplicatie. Als invoer van gebruikers rechtstreeks wordt gebruikt in HTML-uitvoer, cookiewaarden, SQL-queries, et cetera, bestaat er een grote kans dat een kwaadwillende de webapplicatie compromitteert. Een gebrek aan invoervalidatie leidt vaak tot XSS en SQL-injectiekwetsbaarheden.

Referentie OWASP Top 10
» A1 - Injection
https://www.owasp.org/index.php/Top_10_2013-A1
» A3 - Cross Site Scripting (XSS)
https://www.owasp.org/index.php/Top_10_2013-A3

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
» Data Validation Testing
› Testing for Reflected Cross Site Scripting (OWASP-DV-001)
https://www.owasp.org/index.php/Testing_for_Reflected_Cross_site_scripting_(OWASPDV-001)
› Testing for Stored Cross Site Scripting (OWASP-DV-002)
https://www.owasp.org/index.php/Testing_for_Stored_Cross_site_scripting_(OWASPDV-002)
› Testing for DOM based Cross Site Scripting (OWASP-DV-003)
https://www.owasp.org/index.php/Testing_for_DOM-based_Cross_site_scripting_(OWASP-DV-003)
› Testing for SQL Injection (OWASP-DV-005)
https://www.owasp.org/index.php/Testing_for_SQL_Injection_(OWASP-DV-005)
Oracle Testing
MySQL Testing
SQL Server Testing
MS Access Testing
› Testing PostgreSQL (from OWASP BSP)
› Testing for Command Injection (OWASP-DV-013)
https://www.owasp.org/index.php/Testing_for_Command_Injection_(OWASP-DV-013)

OWASP Code Review Guide:
» Reviewing Code for OS Injection
https://www.owasp.org/index.php/Reviewing_Code_for_OS_Injection
» Reviewing Code for SQL Injection
https://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection
» Reviewing Code for Data Validation
https://www.owasp.org/index.php/Reviewing_Code_for_Data_Validation
» Reviewing Code for Cross-Site Scripting
https://www.owasp.org/index.php/Reviewing_Code_for_Cross-site_scripting

OWASP Application Security Verification Standard (ASVS)
» V5 - Input Validation Verification Requirements
http://code.google.com/p/owasp-asvs/wiki/Verification_V5

KU.20 Geen uitvoervalidatie

Toelichting
Naast het ontbreken van validatie van invoer ontbreekt het bij sommige webapplicaties ook aan de validatie van uitvoer. Als een webapplicatie onvoldoende controles uitvoert op de uitvoer die het terugstuurt naar de gebruiker, kan het gebeuren dat er zich onbedoelde of ongewenste inhoud in de uitvoer bevindt. Denk hierbij aan scriptingcode die een aanvaller gebruikt in XSS-aanvallen, informatie over gebruikte technologieën op de server en uitgebreide foutmeldingen.

Referentie OWASP Top 10
» A1 - Injection
https://www.owasp.org/index.php/Top_10_2013-A1
» A3 - Cross Site Scripting (XSS)
https://www.owasp.org/index.php/Top_10_2013-A3
» A5 - Security Misconfiguration
https://www.owasp.org/index.php/Top_10_2013-A5

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
» Configuration Management
› SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) (OWASPCM-001)
https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)
› DB Listener Testing (OWASP-CM-002)
https://www.owasp.org/index.php/Testing_for_DB_Listener_(OWASP-CM-002)
› Infrastructure Configuration Management Testing (OWASP-CM-003)
https://www.owasp.org/index.php/Testing_for_infrastructure_configuration_management_(OWASP-CM-003)
› Application Configuration Management Testing (OWASP-CM-004)
https://www.owasp.org/index.php/Testing_for_application_configuration_management_(OWASP-CM-004)
› Testing for File Extensions Handling (OWASP-CM-005)
https://www.owasp.org/index.php/Testing_for_file_extensions_handling_(OWASPCM-005)
› Old, Back-up and Unreferenced Files (OWASP-CM-006)
https://www.owasp.org/index.php/Testing_for_Old,_Back-up_and_Unreferenced_Files_(OWASP-CM-006)
› Infrastructure and Application Admin Interfaces (OWASP-CM-007)
https://www.owasp.org/index.php/Testing_for_Admin_Interfaces_(OWASP-CM-007)
› Testing for HTTP Methods and Cross Site Tracing (XST) (OWASP-CM-008)
https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASPCM-008)
Information Gathering
› Spiders, Robots and Crawlers (OWASP-IG-001)
https://www.owasp.org/index.php/Testing:_Spiders,_Robots,_and_Crawlers_(OWASPIG-001)
› Search Engine Discovery/Reconnaissance (OWASP-IG-002)
https://www.owasp.org/index.php/Testing:_Search_engine_discovery/reconnaissance_(OWASP-IG-002)
› Identify application entry points (OWASP-IG-003)
https://www.owasp.org/index.php/Testing:_Identify_application_entry_points_(OWASPIG-003)
› Testing for Web Application Fingerprint (OWASP-IG-004)

https://www.owasp.org/index.php/Testing_for_Web_Application_Fingerprint_(OWASPIG-004)
› Application Discovery (OWASP-IG-005)
https://www.owasp.org/index.php/Testing_for_Application_Discovery_(OWASP-IG-005)
› Analysis of Error Codes (OWASP-IG-006)
https://www.owasp.org/index.php/Testing_for_Error_Code_%28OWASP-IG-006%29

OWASP Application Security Verification Standard (ASVS)
» V6 - Output Encoding/Escaping Verification Requirements
http://code.google.com/p/owasp-asvs/wiki/Verification_V6

KU.21 Ineffectieve filters

Toelichting
In veel gevallen voert een webapplicatie wel invoervalidatie en filtering uit, maar blijkt deze filtering niet voldoende effectief genoeg om alle mogelijke aanvallen op de webapplicatie te blokkeren. Dit is voornamelijk het geval op het moment dat de webapplicatie gebruik maakt van blacklisting om mogelijk gevaarlijke strings uit de invoer te verwijderen.

Referentie OWASP Top 10
Zie kwetsbaarheid 'Geen invoervalidatie'.

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
Zie kwetsbaarheid 'Geen invoervalidatie'.

KU.22 Onveilige opslag van informatie

Toelichting
Onveilige opslag van informatie verhoogt niet zozeer de kans op een kwetsbaarheid, maar verhoogt wel de schade die een kwetsbaarheid teweeg kan brengen. Informatie die niet versleuteld opgeslagen is, kan bijvoorbeeld een probleem vormen op het moment dat de webapplicatie een path traversal of command-injectie kwetsbaarheid bevat. Het niet versleuteld opslaan van gevoelige informatie in een database is ook een probleem op het moment dat de webapplicatie kwetsbaar is voor SQL-injectie.

Referentie OWASP Top 10
» A6 - Sensitive Data Exposure
https://www.owasp.org/index.php/Top_10_2013-A6

KU.23 Extern ontwikkelde (kwetsbare) webapplicaties

Toelichting
Bij het nemen van maatregelen voor webapplicaties bestaat de kans dat de focus voornamelijk gericht is op intern ontwikkelde webapplicaties. 'Extern ontwikkelde aangekochte webapplicaties zijn veilig', wordt vaak gedacht. Niets is minder waar. Ook extern ontwikkelde webapplicaties kunnen kwetsbaarheden bevatten. En juist omdat deze in gebruik zijn bij meer organisaties, is de kans groter dat kwaadwillenden hun pijlen op deze webapplicaties richten en bijvoorbeeld exploits voor deze producten publiceren.

KU.24 Gebruik van voorbeeldscripts van internet

Toelichting
Op internet zijn veel voorbeeldscripts beschikbaar die beschrijven op welke manier ontwikkelaars bepaalde functionaliteiten in hun webapplicatie kunnen implementeren. Vaak is in deze voorbeeldscripts onvoldoende aandacht besteed aan het aspect beveiliging. Het gevaar bestaat dat ontwikkelaars deze voorbeeldscripts één-op-één verwerken in hun eigen webapplicatie, waardoor automatisch een kwetsbaarheid in hun webapplicatie introduceren.

KU.25 Onvoldoende hardening en patching

Toelichting
Het ontbreken van hardeningsmaatregelen en patches leidt tot veel van de hiervoor beschreven kwetsbaarheden. Het ontbreken van patches kan er bijvoorbeeld toe leiden dat allerhande kwetsbaarheden aanwezig blijven in extern ontwikkelde webapplicaties en in web- en applicatieservers.
Verder kan het ontbreken van hardeningsmaatregelen ertoe leiden dat succesvol misbruik van kwetsbaarheden leidt tot grote schade. Zo zijn de mogelijkheden van een command injectie kwetsbaarheid vaak beperkt tot de rechten van het account waaronder de webserver draait. Maakt de webserver gebruik van een account dat zeer hoge rechten heeft, dan kan de kwaadwillende nog meer schade aanrichten.

Referentie OWASP Top 10
» A5 - Security Misconfiguration
https://www.owasp.org/index.php/Top_10_2013-A5

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
» Configuration Management Testing
› SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) (OWASPCM-001)
https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001)
› DB Listener Testing (OWASP-CM-002)
https://www.owasp.org/index.php/Testing_for_DB_Listener_(OWASP-CM-002)
› Infrastructure Configuration Management Testing (OWASP-CM-003)
https://www.owasp.org/index.php/Testing_for_infrastructure_configuration_management_

(OWASP-CM-003)
  - Application Configuration Management Testing (OWASP-CM-004)
    https://www.owasp.org/index.php/Testing_for_application_configuration_management_(OWASP-CM-004)
  - Testing for File Extensions Handling (OWASP-CM-005)
    https://www.owasp.org/index.php/Testing_for_file_extensions_handling_(OWASPCM-005)
  - Old, Back-up and Unreferenced Files (OWASP-CM-006)
    https://www.owasp.org/index.php/Testing_for_Old,_Back-up_and_Unreferenced_Files_(OWASP-CM-006)
  - Infrastructure and Application Admin Interfaces (OWASP-CM-007)
    https://www.owasp.org/index.php/Testing_for_Admin_Interfaces_(OWASP-CM-007)
  - Testing for HTTP Methods and Cross Site Tracing (XST) (OWASP-CM-008)
    https://www.owasp.org/index.php/Testing_for_HTTP_Methods_and_XST_(OWASPCM-008)
- Information Gathering
  - Analysis of Error Codes (OWASP-IG-006)
    https://www.owasp.org/index.php/Testing_for_Error_Code_%28OWASP-IG-006%29

OWASP Code Review Guide:
- Chapter on Error Handling
  https://www.owasp.org/index.php/Error_Handling

E.4 Uitvoeringsdomein: platformen en webservers

Kwetsbaarheden en bedreigingen
Het platform bevindt zich tussen het netwerk en de webapplicatie. In sommige gevallen zijn de services die het platform aanbiedt rechtstreeks via internet te benaderen, waardoor kwetsbaarheden in het platform direct de beveiliging van de webapplicatie in gevaar brengen.
Mogelijke kwetsbaarheden en bedreigingen zijn:

KU.26 Kwetsbaarheden in het besturingssysteem

Toelichting
Niet alle kwetsbaarheden met betrekking tot besturingssystemen hebben direct gevolgen voor servers die in gebruik zijn door webapplicaties. Dit komt voornamelijk doordat webservers in de regel slechts bereikbaar zijn op een beperkt aantal poorten. Wanneer een kwetsbaarheid in het besturingssysteem aanwezig is die kwaadwillenden via de webserver kunnen misbruiken (bijvoorbeeld met de mogelijkheid om willekeurige code uit te voeren), dan kan dit ernstige gevolgen hebben voor alle webapplicaties die van deze server gebruik maken.

Trend: Kwaadwillenden zijn steeds sneller in staat om exploits voor deze kwetsbaarheden te schrijven en als een kwetsbaarheid op veel servers aanwezig is zullen kwaadwillenden veel moeite doen om deze uit te kunnen buiten. Dit heeft tot gevolg dat leveranciers steeds minder tijd hebben om bekende kwetsbaarheden te patchen.

KU.27 Onveilige beheermechanismen

Toelichting
Het beheer van servers kan op verschillende manieren plaatsvinden. Enkele van de meest gebruikte beheermechanismen zijn:
- Consoleverbindingen.
  Een consoleverbinding kan normaal gesproken alleen worden gemaakt via fysieke toegang tot de server. Tegenwoordig bestaan er echter ook apparaten waarmee deze consoleverbinding via het netwerk (op basis van bijvoorbeeld Telnet of SSH) kan worden benaderd.
- Telnet.
  Via telnet kan een command-line sessie worden geopend met een server. Telnet is een verouderd mechanisme dat vanwege het ontbreken van goede beveiligingsmechanismen steeds minder vaak wordt toegepast.
- Secure Shell (SSH).
  Via een SSH-verbinding kan een veilige (versleutelde) verbinding opgezet worden tussen een client en een server. Optioneel kan SSH gebruik maken van certificaten om wederzijdse authenticatie te laten plaatsvinden. Via SSH kan een command-line sessie worden geopend met een server. Het is echter ook mogelijk om andere functionaliteiten (zoals het kopiëren van bestanden via Secure Copy) via een SSH-verbinding te tunnelen.
- File Transfer Protocol (FTP).
  Via FTP kunnen bestanden worden uitgewisseld tussen een client en een server. FTP maakt gebruik van authenticatie op basis van een gebruikersnaam en wachtwoord. Deze gegevens verstuurt de FTP-client in clear-text (in onversleutelde vorm) over het netwerk. Dit laatste is één van de belangrijkste redenen dat het gebruik van FTP onveilig is.
- Webinterface.
  Veel systemen bieden tegenwoordig een webinterface waarmee beheerders de belangrijkste beheeractiviteiten kunnen uitvoeren. Een dergelijke webinterface kan gebruik maken van bestaande beveiligingsmechanismen zoals versleuteling via SSL, authenticatie op basis van X.509-certificaten, et cetera.

Beheermechanismen op basis van een onversleutelde verbinding brengen altijd een beveiligingsrisico met zich mee. Wanneer een organisatie dergelijke beheermechanismen ook toestaat over het internet, vergroot dit de kans dat kwaadwillenden deze authenticatiegegevens onderscheppen (zie richtlijn U/NW.05).

KU.28 Onjuiste autorisaties

Toelichting
Het is van belang om de rechten die worden toegekend aan processen, het bestandssysteem, het register, et cetera zoveel mogelijk in te perken. Het principe dat iets of iemand voor een taak niet meer rechten krijgt toegekend dan strikt noodzakelijk, wordt in het Engels ook wel het 'least privilege'-principe genoemd. Het is één van de basisuitgangspunten voor goede informatiebeveiliging, dat niet alleen wordt toegepast op mensen, maar ook op programma's en processen. De argumenten voor dit uitgangspunt zijn kortweg dat (1) iemand zijn werk moet kunnen doen en dat (2) in het geval van een incident, de schade zoveel mogelijk beperkt moet blijven. Op het moment dat dit 'least privilege'-principe niet wordt gevolgd, kunnen onveilige situaties ontstaan. Het foutief inrichten van rechten kan in de praktijk tot een grote verscheidenheid aan beveiligingsproblemen leiden.
Koppel altijd rechten aan processen, bestanden, directories, et cetera. Als een webserver niet op een juiste manier is ingericht, kunnen kwaadwillenden dit uitbuiten.

KU.29 Onnodige services

Toelichting
Niet alle geactiveerde services na de installatie van een besturingssysteem zullen nodig zijn. Elke service op een platform kan kwetsbaarheden bevatten en vormt daarmee een potentieel lek.

KU.30 Lekken van informatie

Toelichting
Van lekken van informatie is sprake wanneer vertrouwelijke informatie onbedoeld terecht komt bij ongeautoriseerde personen of als informatie onnodig wordt verstrekt. Dit hoeft dus niet noodzakelijk vertrouwelijke informatie te zijn.
De volgende voorbeelden beschrijven situaties waarin de webapplicatie onnodig(e) informatie verstrekt:
- Een webserver toont de gebruikte versies van software en plug-ins.
- Een script bevat commentaar waarin details over de werking van het script zijn opgenomen.
- Een foutmelding bevat informatie over de gebruikte database met bijbehorende gebruikersnamen en wachtwoorden.

De volgende voorbeelden beschrijven situaties waarin gevoelige informatie wordt gelekt richting ongeautoriseerde personen:
- Een kwaadwillende slaagt erin vertrouwelijke gegevens uit de database van de webapplicatie op te halen.
- Een kwaadwillende slaagt erin bestanden met vertrouwelijke informatie (bijvoorbeeld Word-documenten en tekstbestanden) op de webserver te benaderen.
- Een kwaadwillende slaagt erin om vertrouwelijke gegevens te onderscheppen, die vrij leesbaar over het internet worden uitgewisseld.
- Een kwaadwillende slaagt erin bestanden met vertrouwelijke informatie uit het interne netwerk te benaderen, terwijl deze bestanden niet bedoeld zijn voor ontsluiting via de webapplicatie.

Referentie OWASP Top 10
- A5 - Security Misconfiguration
  https://www.owasp.org/index.php/Top_10_2013-A5
- A6 - Information Leakage and Improper Error Handling (Top 10 2007, vervallen sinds Top 10 2010)
  https://www.owasp.org/index.php/Top_10_2007-A6

E.5 Uitvoeringsdomein: netwerken

Kwetsbaarheden en bedreigingen
Deze paragraaf beschrijft kwetsbaarheden en bedreigingen die op het gebied van het netwerk bestaan.
Mogelijke kwetsbaarheden en bedreigingen zijn:

KU.31 (distributed) Denial of Service ((D)DoS)

Toelichting
Over het algemeen gelden de volgende eigenschappen voor een (D)DoS aanval.
Het is bedoeld om:
- een netwerk te overspoelen met dataverkeer, waardoor legitiem dataverkeer niet meer kan doorkomen.
- connecties tussen twee systemen te verbreken.
- een gebruiker geen toegang te geven tot een systeem.
- een service op een systeem te onderbreken.

Voorbeelden van (D)DoS aanvallen om een webapplicatie onbereikbaar te maken zijn via flooding (bijvoorbeeld via een SYN-aanval), Smurf-aanval, et cetera.

Testmethodiek (OWASP Testing Guide/OWASP Code Review Guide)
OWASP Testing Guide:
In paragraaf 4.9 'Denial of Service Testing' van de OWASP Testing Guide v3.0 worden de volgende tests beschreven:
- OWASP-DS-001 Testing for SQL Wildcard Attacks - SQL Wildcard vulnerability.
- OWASP-DS-002 Locking Customer Accounts - Locking Customer Accounts.
- OWASP-DS-003 Testing for DoS Buffer Overflows - Buffer Overflows.
- OWASP-DS-004 User Specified Object Allocation - User Specified Object Allocation.
- OWASP-DS-005 User Input as a Loop Counter - User Input as a Loop Counter.
- OWASP-DS-006 Writing User Provided Data to Disk - Writing User

Provided Data to Disk.
» OWASP-DS-007 Failure to Release Resources - Failure to Release Resources.
» OWASP-DS-008 Storing too Much Data in Session - Storing too Much Data in Session.

KU.32 Pivoting (server hopping)

Toelichting
Toegang tot servers in het netwerk door via een gecompromitteerde machine andere machines in het netwerk te benaderen.

KU.33 Domain Name System (DNS)

Toelichting
Misbruik van DNS-services voor DoS-aanvallen en cache poisoning (ten behoeve van bijvoorbeeld phishing).
De belangrijkste bedreigingen zijn:
» Toestaan van 'zone transfers';
» Denial-of-Service;
» DNS cache poisoning;
» Kwetsbaarheden in DNS-software.

KU.34 Firewall

Toelichting
Firewall als kwetsbaar element vanwege de essentiële rol die de firewall in een netwerk vervult.
De belangrijkste bedreigingen zijn:
» De organisatie redeneert: 'we hebben een firewall, dus we zijn veilig'.
» De firewall is geconfigureerd als router.
» Misconfiguratie van firewalls door wildgroei in de firewall regels (bijvoorbeeld te ruime toegang of aanwezigheid van oude regels)
» Kwetsbaarheden in firewall software.
» Onduidelijke wensen.

E.6 Beheersingsdomein (control)

Kwetsbaarheden en bedreigingen
Deze paragraaf beschrijft kwetsbaarheden en bedreigingen die op het gebied van monitoring, auditing en alerting te onderscheiden zijn. Mogelijke kwetsbaarheden en bedreigingen zijn:

KC.01 Ontbreken van toezicht

Toelichting
Als een kwaadwillende een webapplicatie - of de infrastructuur hieromheen - aanvalt, kan dit kwalijke gevolgen hebben. Een organisatie kan alleen passende maatregelen nemen en de schade tot een minimum beperken, als de juiste mechanismen zijn ingezet voor het detecteren van aanvallen en deze mechanismen bovendien correct zijn geconfigureerd.
Het kan hieraan ontbreken om de volgende redenen:
» Er is überhaupt geen monitoring van netwerkverkeer.
» De monitoringcomponenten leveren zoveel informatie dat de belangrijke aanvallen niet meer te onderscheiden zijn van de vele 'script kiddie'-aanvallen; men ziet met andere woorden door de bomen het bos niet meer.
» De monitoringcomponenten verzamelen wel continu data, maar er is geen medewerker beschikbaar om deze te analyseren.
» De monitoringcomponenten verzamelen wel continu data, maar de gebeurtenissen van deze componenten zijn op geen enkele manier aan elkaar te koppelen doordat de tijdstippen op de componenten uit elkaar lopen.

Het ontbreken van dit toezicht kan ertoe leiden dat kwaadwillenden misbruik maken van webapplicaties zonder dat dit wordt gedetecteerd.

KC.02 Impact: onbekend

Toelichting
Wanneer een component een losstaande gebeurtenis rapporteert, helpt dit in het bepalen van de technische impact: de component is bijvoorbeeld tijdelijk niet meer beschikbaar of de performance is tijdelijk verminderd. Maar wat betekent dit nu voor de gehele keten? Merkt een gebruiker niets van deze storing of leidt de storing tot een zeer ernstige onderbreking van de service aan de gebruiker? Om de impact van een gebeurtenis te kunnen bepalen, is het belangrijk om de gebeurtenis in een groter geheel (de keten) te bekijken. De beschouwing van de omgeving als een keten van nauw samenwerkende componenten is in dit geval de enige juiste. Op basis van dit inzicht kan worden ingeschat wat de risico's zijn en welke maatregelen moeten worden genomen.

KC.03 Gebrek aan coördinatie en samenwerking

Toelichting
De componenten die logging genereren vallen vaak onder verschillende teams binnen en organisatie. Een netwerkbeheerteam beheert de netwerkcomponenten, een applicatiebeheerteam de webapplicaties en een autorisatiebeheerteam de autorisaties. Het analyseren van complexe gebeurtenissen vereist dat deze verschillende teams nauw met elkaar samenwerken. Gebrek aan samenwerking en coördinatie leidt ertoe dat een complexe gebeurtenis niet volledig geanalyseerd wordt.

BIJLAGE F
» RELATIE VERSIE 2012 EN 2015

Beveiligingslaag 2012	Richtlijn 2012	Richtlijn 2015	Maatregelen
Algemeen	B0-1	B.01	01 02
	B0-2	B.03	01 02 03 04
	B0-3	B.06	04 05
	B0-4	C.11	01 03
	B0-5[82]	C.08	01 02 05 06 07 08 09 10 11 12
	B0-6[82]	U/PW.07	01 02 03 04 05
		U/NW.06	01 02 03 04
	B0-7	C.09	01 02 03 04
	B0-8	C.04	01 02 03 04 05 06 07
	B0-9	C.03	01 03 05
	B0-10	C.02	01 02 03 04 05
	B0-11	C.10	02 05
	B0-12	B.02	01 02 04 05 06 07 08 09 10
		U/TV.01	01 02 03 04 05 06 08 11
	B0-13	C.11	02 03
	B0-14	B.05	01 02
Netwerk	B1-1	U/NW.03	06 07
	B1-2	U/NW.03	06
		U/NW.05	03 04 05
	B1-3	U/NW.07	01
	B1-4	U/NW.03	03 04 06
	B1-5	U/NW.04	02 03 05 06
	B1-6	U/NW.02	02
Platform	B2-1	U/PW.05	01 02
	B2-2	U/PW.01	01
	B2-3	U/PW.04	01 02
	B2-4	U/PW.06	01 02
Applicatie	B3-1	U/WA.03	04
	B3-2	U/PW.02	02
	B3-3	U/WA.03	03
	B3-4	U/WA.04	01
	B3-5	U/WA.07	01 02
	B3-6	U/WA.03	01
	B3-7	U/WA.03	02
	B3-8	U/PW.02	04
	B3-9	U/PW.02	05
	B3-10	U/PW.02	06
	B3-11	U/WA.06	01
	B3-12	U/PW.02	03
	B3-13	U/PW.03	02
	B3-14	C.05	01
	B3-15	C.05	02
	B3-16	U/PW.03	03
Identiteit	B4-1	U/TV.01	11
	B4-2	U/WA.08	02 03 04 05
Vertrouwelijkheid	B5-1	B.04	01 02 03 04
	B5-2	U/WA.05	05
	B5-3	U/WA.05	03
	B5-4	U/WA.05	04
	B5-5	U/WA.05	06
	B5-6	-	
	B5-7	B.04	01
Integratie	B6-1	B.06	04 05 09
Monitoring	B7-1	U/NW.04	07 08 09
		C.06	02
	B7-2	C.06	03
	B7-3	C.07	01 05
	B7-4	C.06	04
	B7-5	C.06	05
	B7-6	C.06	06
	B7-7	C.06	07
	B7-8	C.07	02 03 04
	B7-9	C.07	08 09 10 11

82 In de versie 2012 zijn richtlijnen B0-5 en B0-6 in deel 1 per abuis omgekeerd beschreven ten opzichte van deel 2. In deze tabel wordt uitgegaan van de volgorde zoals in deel 1.

Nationaal Cyber Security Centrum
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070-751 55 55
www.ncsc.nl | info@ncsc.nl

September 2015