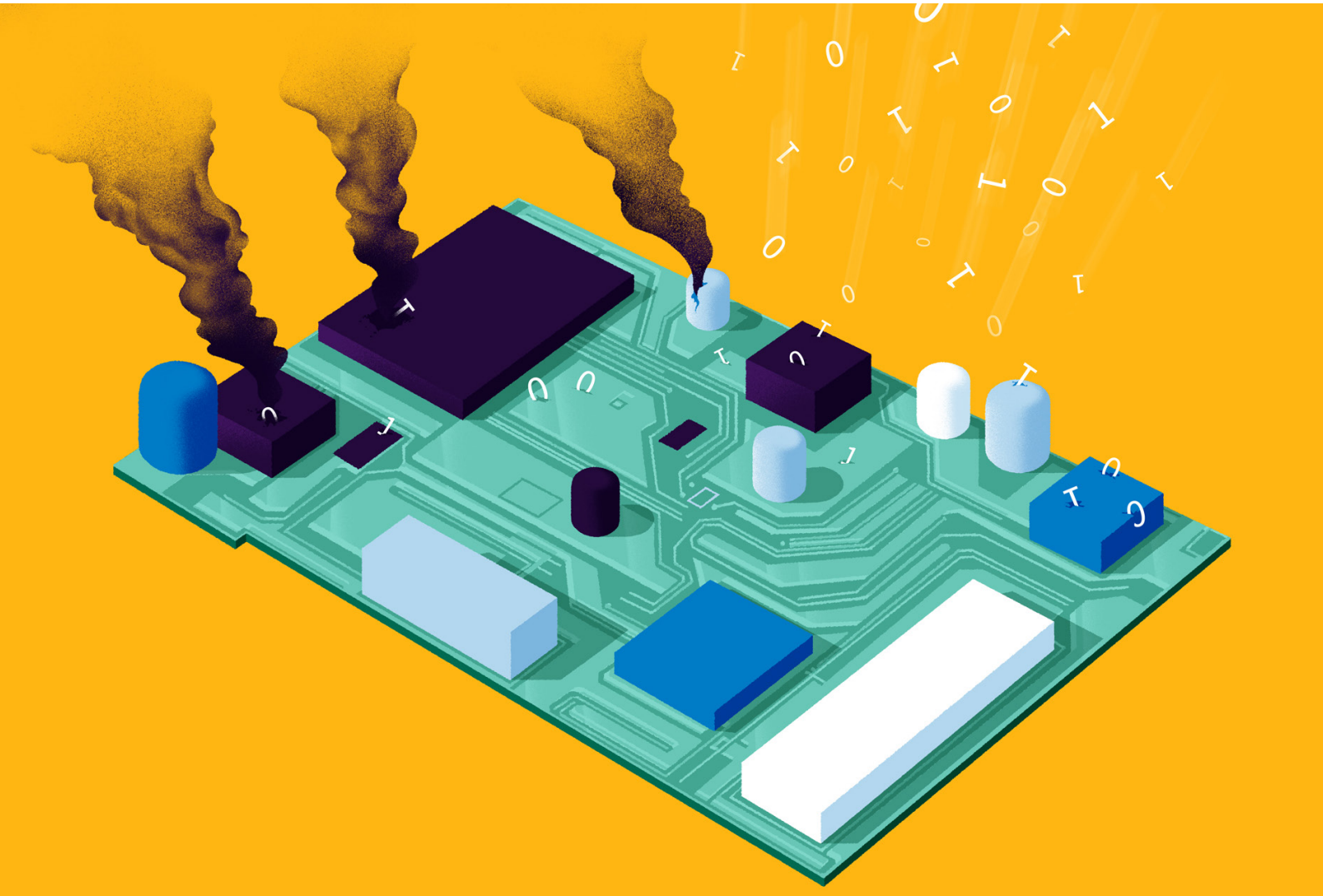
Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Vier cybersecuritylessen uit één jaar oorlog in Oekraïne



Deelnemende organisaties

Dit product wordt uitgebracht door het NCSC, het DTC en het CSIRT-DSP en is tot stand gekomen op basis van een kennisdelingssessie met cybersecurityexperts van verschillende overheidsorganisaties.

Cybersecurityexperts vanuit het NCSC, het DTC, het CSIRT-DSP, het ministerie van Buitenlandse Zaken, de Nederlandse Defensie Academie (NLDA), de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), de Nationale Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Defensie Cyber Commando (DCC) hebben deelgenomen aan de kennisdelingssessie.

Inhoud

Voorwoord	2
Voornaamste lessen	3
1. Opleving hacktivisme	4
2. Private organisaties	7
3. De basis op orde	10
4. Keteneffecten	13
Referenties	16

Voorwoord

Beste lezer,

Een jaar geleden vielen Russische troepen de landsgrenzen van Oekraïne binnen, waarmee oorlog weer terugkeerde op Europees grondgebied. Het verloop van de invasie is bekend. De snelle verovering die Rusland in gedachten had, mondde uit in een bloedige strijd die tienduizenden levens eiste en die nog altijd voortduurt. Als gevolg van de oorlog wordt, onzichtbaar voor het blote oog, ook in de digitale wereld gevochten door pro-Russische en pro-Oekraïense actoren.

Sinds het begin van de oorlog volgt het NCSC deze digitale strijd nauwlettend en met de grootst mogelijke alertheid. Samen met onze nationale en internationale partners detecteren en analyseren we 24/7 cyberdreigingen die mogelijkerwijs verband houden met de strijd in Oekraïne en bieden we handelingsperspectief aan bedrijven en organisaties in Nederland. Gelukkig is de impact van cyberaanvallen in ons land tot nu toe beperkt gebleven. Maar wat niet is, kan nog komen. Waakzaamheid blijft geboden.

Wat kunnen we leren van het afgelopen jaar? Zoals bij alle grote gebeurtenissen is het belangrijk om af en toe terug te blikken. Daar kunnen we van leren, zodat we weer vooruit kunnen kijken. Daarom heeft het NCSC in december het initiatief genomen om de ervaringen van het afgelopen jaar te evalueren met de betrokken partners. Wat voor cyberaanvallen hebben we gezien, hoe werkten deze, wat voor actoren zaten erachter? En ook belangrijk: welke maatregelen kunnen we hiertegen nemen? In dit rapport hebben we de vier belangrijkste cyberlessen van een jaar oorlog in Oekraïne kernachtig beschreven. We hebben waardevolle inzichten verkregen met deze terugblik. Ze helpen ons om optimaal voorbereid te zijn op toekomstige cyberaanvallen. Hoe meer kennis we vergaren over ons eigen handelen en (kwaadwillende) actoren in de digitale wereld, des te meer we de digitale weerbaarheid van Nederland kunnen vergroten.

Als het gaat om bewustwording van de impact van cyberdreigingen, heeft de oorlog in Oekraïne wel degelijk grote invloed gehad in Nederland. We zien een groeiend besef bij organisaties en bedrijven over onze economische afhankelijkheid en kwetsbaarheid van digitale diensten. Hierdoor weten private en publieke sectoren elkaar nog beter te vinden. Ze zoeken elkaar op en wisselen informatie uit. Nieuwe strengere Europese cyberwetgeving zal deze ontwikkeling verder stimuleren.
Terwijl de oorlog in Oekraïne een nieuwe fase ingaat, is het belangrijk dat organisaties en bedrijven onverminderd blijven samenwerken op het gebied van cybersecurity. Dat begint met meer robuuste en beter beveiligde IT-omgevingen. Het NCSC zal zich blijven inzetten om partijen nog beter met elkaar te verbinden en dreigingsinformatie en handelingsperspectief tijdig te delen.

Samen moeten we alert blijven op cyberaanvallen, voor dat ene moment dat komt als je het niet verwacht. Alleen samen kunnen we de impact van zo'n aanval op Nederland en de wereld zo klein mogelijk houden.

Hans de Vries
Directeur NCSC

Voornaamste lessen

In dit rapport blikt het NCSC met het DTC en CSIRT-DSP terug op een jaar oorlog in Oekraïne en cybersecuritylessen die daaruit getrokken kunnen worden. We kijken daarbij niet alleen naar digitale dreigingen, maar ook naar maatregelen die de digitale weerbaarheid verhogen. Dit hebben we gedaan met cybersecuritypartners vanuit de Nederlandse overheid. Dit hoofdstuk is een introductie waarin we de context en aanloop van het gehele rapport schetsen.

Aan de oorlog gerelateerde digitale aanvallen hebben vooralsnog niet gezorgd voor grote verstoringen in Nederland. Aanvallen die zijn uitgevoerd hebben een tijdelijk en lokaal effect gehad, daardoor was de impact beperkt.[1] Dit dreigingsbeeld lijkt stabiel, maar kan abrupt veranderen.[2]

Toch kunnen we veel cybersecuritylessen trekken uit de Russische invasie van Oekraïne.[3] Alhoewel in Nederland grote verstoringen zijn uitgebleven zijn Nederlandse bondgenoten wel getroffen door aanzienlijke aan de oorlog te relateren digitale aanvallen.[4][5] In veel gevallen zijn deze digitale aanvallen uitgevoerd door niet-statelijke actoren zoals hacktivisten.

Maatschappelijke onrust

Het bericht dat de Russische invasie van Oekraïne ook effect kon hebben op de Nederlandse digitale veiligheid bereikte via verschillende media ook de Nederlandse huiskamers.[39] Nederlanders zagen in deze periode een mogelijke cyberaanval als tweede meest bedreigende ontwikkeling voor de veiligheid en brede welvaart in Europa.[4]

Ook het NCSC, CSIRT-DSP en het DTC ontvingen in deze periode veel vragen over de effecten van de oorlog op de Nederlandse digitale veiligheid, zowel op een druk bezochte gezamenlijke webinar[5] als via de gebruikelijke communicatiekanalen.

Cybersecuritylessen

Omdat er al zoveel is gebeurd rondom de oorlog, in de vorm van digitale aanvallen en de genomen maatregelen om de digitale weerbaarheid te verhogen, vinden we het belangrijk hierop terug te blikken en er lessen uit te trekken. We doen dat in dit rapport.

De vier belangrijkste lessen zijn:

1. **Opleving hacktivisme:** Hacktivisten zijn nadrukkelijk aanwezig in de context van de Russische invasie van Oekraïne en voeren verstorende digitale aanvallen uit.
2. **Rol private organisaties:** Private organisaties spelen een belangrijke rol in de digitale oorlog om de digitale weerbaarheid van (Oekraïense) organisaties te verhogen en vitale diensten toegankelijk te houden.
3. **De basis op orde:** De snelle escalatie van de oorlog laat zien hoe belangrijk het is voorbereid te zijn op een toekomstige en snel escalerende cybercrisis.
4. **Keteneffecten:** Cyberaanvallen beperken zich niet tot landsgrenzen en kunnen internationaal effect hebben.

In dit rapport gaan we verder op deze vier cybersecuritylessen in en geven we per les ook handelingsperspectief. Zo kunnen organisaties hun digitale weerbaarheid verder verhogen.

1. Opleving hacktivisme

Les 1: Hacktivisten zijn nadrukkelijk aanwezig in de context van de Russische invasie van Oekraïne en voeren verstorende digitale aanvallen uit.

Sinds de start van de Russische invasie van Oekraïne zijn er veel digitale aanvallen uitgevoerd door hacktivisten[6]. Deze hacktivisten voeren digitale aanvallen uit tegen zowel Russische en Oekraïense belangen. Zo riepen Oekraïense autoriteiten, vlak na de Russische invasie, cyberspecialisten wereldwijd op tot aansluiting bij een nieuw gevormd Oekraïens IT-leger.[7]

- **Organisaties die ogenschijnlijk buiten de strijd stonden werden soms toch doelwit van hacktivisten.** Hacktivisten hebben niet alleen digitale aanvallen uitgevoerd op partijen die direct betrokken zijn in de oorlog. Pro-Russische hacktivisten hebben ook organisaties als doelwit aangemerkt, alleen omdat zij gevestigd zijn in een land dat Oekraïne steunt.[8] Zo zijn in Nederland ziekenhuizen het doelwit geweest van digitale aanvallen door hacktivisten.[1]

  Pro-Oekraïense hacktivisten hebben organisaties aangevallen, omdat die in hun ogen juist te weinig steun lieten blijken.[9] Het aanmerken van een organisatie als doelwit gebeurt vaak als reactie op een politieke ontwikkeling[10] en is vaak ook opportuun.

- **Hacktivisten voeren digitale aanvallen vaak reactief uit.** Zo zijn er hacktivistische digitale aanvallen uitgevoerd na de aankondiging van nieuwe wapenleveranties aan Oekraïne[11], het verwijderen van Sovjet-monumenten[12] of politieke besluitvorming die werd opgevat als anti-Russisch[13]. Daarbij kenmerken hacktivistische aanvallen zich niet door een financieel, maar ideologisch oogmerk.

- **Hacktivisten proberen aandacht te genereren voor de door hen uitgevoerde digitale aanvallen.** Daarbij maken ze in publieke communicatie gebruik van stevige retoriek om daden extra kracht bij te zetten. Zo kiezen hacktivisten voor doelwitten met symbolische waarde voor digitale aanvallen, zoals het Eurovisie Songfestival in 2022.[14]

- **Veel hacktivistische groepen zijn ad hoc samengesteld en hebben wisselende deelnemers.** Zo werkt de hacktivistische groepering Killnet via Telegramkanalen om daarmee contact te houden met hun achterban. De Telegramkanalen van Killnet hebben tienduizenden deelnemers. Dit hoeven niet allemaal hacktivisten zijn: ook cybersecurityonderzoekers of journalisten volgen zo deze groep.

Mogelijke impact op Nederlandse organisaties

- **Hacktivistische aanvallen hebben een wisselende impact.** Dit komt door de ad-hoc samenstelling van hacktivistische groepen. Dit maakt, in tegenstelling tot bijvoorbeeld geavanceerde statelijke actoren, onderlinge coördinatie en samenwerking lastiger voor hacktivisten. Ook veranderen hiermee de inzetbare capaciteiten en het expertiseniveau.

- **Een politieke opstelling van een organisatie is een risicofactor.** Een politieke opstelling van een organisatie maakt een organisatie een mogelijk doelwit van hacktivisten. Het is verstandig dit mee te nemen in een risicoanalyse.

- **Nederlandse digitale infrastructuur is misbruikt voor DDoS-aanvallen op Oekraïense websites.**[15] Veel internetverkeer loopt via Nederland vanwege de hoge kwaliteit van de Nederlandse digitale infrastructuur en de centrale ligging van Nederland bij veel internationale internetknooppunten. Kwaadwillenden kunnen ook van deze hoogwaardige infrastructuur gebruik maken om digitale aanvallen uit te voeren.

- **Hacktivisme vanuit Nederland kan leiden tot een ongewenste reactie.** Aanvallen door hacktivisten vanuit Nederland kunnen negatieve gevolgen hebben. Zo kan Nederland het doelwit worden van politiek gemotiveerde tegenacties. Ook is misbruik van de Nederlandse infrastructuur slecht voor de internationale reputatie van Nederland.[16]

- **De inmenging van hacktivisten maakt het dreigingsbeeld complexer.** Statelijke actoren kunnen bijvoorbeeld eigen activiteiten verhullen door aanvallen toe te dichten aan hacktivisten.[17]

- **Het uitvoeren van digitale aanvallen is strafbaar.** Of het nu gaat om het binnendringen van computers of servers, of het uitvoeren van een DDoS-aanval op een website. Deze regels gelden voor iedereen die vanuit Nederland zulke feiten pleegt.[18]

- **Betrokkenheid van werknemers bij hacktivisme kan ook voor problemen zorgen bij het uitvoeren van een vertrouwelijke functie binnen de overheid.** Denk hierbij aan het verkrijgen van een verklaring van geen bezwaar.[19]

Handelingsperspectief

Neem DDoS-aanvallen mee in een dreigingsanalyse

Door DDoS-aanvallen proberen hacktivisten de beschikbaarheid van digitale systemen en processen te verstoren. Dit is bij hacktivisten een veelvoorkomende aanvalstechniek.

Neem een DDoS-scenario mee in een dreigings- en risicoanalyse. In de factsheet "Continuïteit van online diensten" gaat het NCSC verder in op hoe u uw organisatie kunt beschermen tegen een DDoS-aanval.

Doorloop uw crisiscommunicatieplan

Hacktivisten kunnen ook door een hack-en-lek-aanval vertrouwelijke gegevens stelen en lekken om een organisatie of overheid reputatieschade te bezorgen. Door een defacement-aanval proberen hacktivisten toegang te krijgen tot communicatiekanalen van het doelwit en deze te bekladden met opruiende, verontrustende en provocerende teksten.

Hacktivisten zijn erop gericht om veel aandacht voor hun acties te genereren. Ze treden bij een uitgevoerde digitale aanval actief naar buiten en daarmee kunnen er vragen vanuit uw achterban of bijvoorbeeld media ontstaan.

Een goed crisiscommunicatieplan kan u helpen effectief te reageren op een digitale aanval, ook als deze veel publiciteit aantrekt.

In de publicatie "Aandachtspunten crisismanagement en crisiscommunicatie bij digitale incidenten" geeft het NCSC aanknopingspunten hoe om te gaan met een digitaal incident.

2. Private organisaties

Les 2: Private organisaties spelen een belangrijke rol in de digitale oorlog om de digitale weerbaarheid van (Oekraïense) organisaties te verhogen en vitale diensten toegankelijk te houden.

Private organisaties spelen een belangrijke rol in het beveiligen en beschikbaar houden van de Oekraïense digitale infrastructuur. Dit heeft op verschillende manieren een groot effect gehad op betrokken partijen in de oorlog.

- **Private organisaties zijn cruciaal geweest in het toegankelijk houden van Oekraïense digitale dienstverlening.** Oekraïense overheidsorganisaties zijn vaak getroffen geweest door digitale aanvallen. Door private organisaties, zoals internetdienstverleners, cybersecurityorganisaties, clouddienstverleners[20] en hosting-partijen, heeft de Oekraïense bevolking toegang kunnen houden tot digitale dienstverlening. Dit kon onder andere, omdat Oekraïense autoriteiten data en servers hebben verplaatst naar locaties buiten Oekraïne om ze buiten de handen van de Russische bezetter te houden.[21]

- **Dreigingsinformatie van private organisaties heeft ervoor gezorgd dat digitale aanvallen vroeg gestopt konden worden.** Zo berichtte Microsoft op 15 januari 2022 over destructieve malware die gericht was op verschillende organisaties in Oekraïne. Deze malware was ontdekt door Microsoft op 13 januari 2022.[22] Op basis van deze informatie is door veel organisaties adequaat gehandeld om schade in Oekraïne en daarbuiten te voorkomen.[23]

  Ook andere organisaties zoals ESET[24], SentinelLabs[25], Mandiant[26] en Unit42 van Palo Alto[27] hebben met dreigingsinformatie bijgedragen aan de digitale veiligheid van veel organisaties.[28]

- **Internetservice dienstverleners (ISPs) zijn in staat geweest het internet toegankelijk te houden in Oekraïne.** De internetinfrastructuur van Oekraïne is door Russische fysieke[29] en digitale[30] aanvallen zwaar beschadigd geraakt. Daarnaast leidt Rusland het internetverkeer in bezette gebieden om via Russische servers voor surveillance en censuurdoeleinden.[31] Dit heeft invloed op de beschikbaarheid, vertrouwelijkheid en integriteit van het internet voor organisaties en personen in Oekraïne.

  Doordat Oekraïne veel verschillende ISPs heeft bleek het lastig voor Rusland om een grote verstoring te veroorzaken. Wanneer een afzonderlijk netwerk uitviel had dit een relatief klein effect op het geheel.[32]
  Daarnaast speelde satellietcommunicatie een belangrijke rol in het beschikbaar houden van het internet in Oekraïne. Op verzoek van Oekraïense autoriteiten[33] heeft SpaceX haar satellietnetwerk Starlink geactiveerd boven Oekraïne op 27 februari 2022.[34] Hierdoor werd het internet weer toegankelijk in door de oorlog zwaar getroffen gebieden en konden Oekraïense troepen, burgers en organisaties contact houden met de buitenwereld.

- **Private organisaties leveren een waardevolle bijdrage door sancties en wetgeving te volgen.** Dit geldt voor overheidsorganisaties in Oekraïne, maar ook daarbuiten. Samenwerking en kennisdeling met de cybersecuritygemeenschap is cruciaal voor het veilig houden van digitale systemen.[35]

Mogelijke impact op Nederlandse organisaties

- **Door intensieve samenwerking met private partijen zijn veel organisaties in staat geweest hun digitale weerbaarheid te verhogen.** Dit geldt voor overheidsorganisaties in Oekraïne, maar ook daarbuiten. Samenwerking en kennisdeling met de cybersecuritygemeenschap is cruciaal voor het veilig houden van digitale systemen.

- **Private organisaties kunnen een doelwit worden van digitale aanvallen als ze steun verlenen aan een strijdende partij.** Betrokken partijen in een conflict zijn niet alleen maar staten, ook technologiebedrijven hebben door de digitale diensten en producten die ze aanbieden een aanzienlijke geopolitieke invloed. Deze invloed kan ze ook een mogelijk doelwit van digitale aanvallen maken.[36]

Handelingsperspectief

Steun aan Oekraïense organisaties kan voor ongewenste reacties zorgen, neem dit mee in een risicoanalyse

Nederlandse publieke[37] en private organisaties bieden steun aan Oekraïne in de strijd tegen de Russische bezetter. Deze steun kan om allerlei verschillende redenen wenselijk zijn, maar kan ook leiden tot ongewenste reacties.

Neem de dreiging van digitale aanvallen vanuit hacktivisten en statelijke actoren mee in een risicoanalyse. De dreiging kan toenemen wanneer uw organisatie steun verleent aan Oekraïense organisaties of zich uitspreekt tegen de invasie.

Werk samen met andere organisaties

Samen weten organisaties meer dan alleen. Zo kunnen organisaties in een samenwerkingsverband dreigingsinformatie of kennis en ervaringen uitwisselen. Actieve deelname aan verschillende samenwerkingsverbanden en overleggremia – ook in een periode van een lagere dreiging – kunnen ervoor zorgen dat er een stevige fundering voor samenwerking ligt in tijden van crisis.

Actieve deelname in samenwerkingsverbanden zoals een ISAC of een OKTT draagt bij aan de digitale weerbaarheid van alle deelnemers. Op de websites van het NCSC en het DTC staat meer informatie over het starten en door ontwikkelen van samenwerkingen.

3. De basis op orde

Les 3: De snelle escalatie van de oorlog laat zien hoe belangrijk het is voorbereid te zijn op een toekomstige en snel escalerende cybercrisis.

De digitale oorlog heeft laten zien hoe belangrijk het is om de basis van cyberveiligheid als organisatie op orde te hebben.

- **Het was in het begin onduidelijk welke invloed de Russische invasie van Oekraïne had op de Nederlandse digitale veiligheid.**[38] De mogelijke effecten van aan de invasie gerelateerde digitale aanvallen stonden eind februari ook op de agenda van verschillende media.[39] Ook onder de Nederlandse bevolking ontstond in deze periode veel onzekerheid over een mogelijke digitale aanval.[4]

  Het NCSC, DTC en het CSIRT-DSP beschikten op dat moment niet over aanwijzingen over digitale aanvallen die, voortvloeiend uit de oorlog in Oekraïne, impact zouden hebben op Nederland. Tegelijkertijd konden toekomstige digitale aanvallen op Nederlandse organisaties ook toen niet uitgesloten worden.[40]

- **Oekraïense organisaties wisten door een goede cyberverdediging veel schade te beperken.** De impact van de vele digitale aanvallen die Oekraïne te verwerken kreeg, is verhoudingsgewijs beperkt.[41] Oekraïense organisaties bleken sterk in **het monitoren van, en reageren op,** binnenkomende digitale aanvallen. Zo reageerden deze organisaties snel op malware en het patchen van kwetsbaarheden, waardoor schade door digitale aanvallen flink werd beperkt.[42]

  Ook hebben veel organisaties in Oekraïne meteen vanaf het begin van de oorlog **back-ups** gemaakt in, en diensten verhuisd naar, de cloud. Hierdoor waren data en digitale processen niet alleen afhankelijk van lokale systemen. Daarnaast biedt het gefragmenteerde Oekraïense communicatienetwerk bescherming voor diverse vitale diensten, doordat deze **redundantie** hebben.[43]

- **Gedurende de oorlog richtten digitale aanvallen zich vaak op kwetsbare randapparatuur.** Aanvallers hebben veel gebruik gemaakt van kwetsbare randapparatuur om het tempo in digitale aanvallen te verhogen. In tegenstelling tot tijdrovende phishing aanvallen is misbruik van kwetsbare randapparatuur beter schaalbaar. Hierbij gaat het om misbruik van bijvoorbeeld kwetsbare firewalls, routers en email servers.[44]

Mogelijke impact op Nederlandse organisaties

- **Er zijn veel verschillende digitale aanvallen uitgevoerd die te relateren zijn aan de oorlog.** Het NCSC heeft in 2022 deze digitale aanvallen bijgehouden in een tijdlijn.[45] Deze digitale aanvallen verschillen in aanvalsmethode en beoogd effect. Dit vormt een uitdaging bij het verhogen van de weerbaarheid van organisaties.

- **Niet alle digitale aanvallen zijn direct zichtbaar.** Dat we digitale aanvallen niet waarnemen betekent niet dat ze er niet zijn. Zo kunnen aanvallers ook posities op systemen innemen om pas later over te gaan tot het uitvoeren van verstorende effecten. Sommige basismaatregelen, zoals netwerksegmentatie en het verzamelen van loginformatie, zijn ook effectief als een aanvaller al toegang heeft tot een systeem.

Handelingsperspectief

Maak gebruik van scenario's in uw risicoanalyse

Een digitale aanval is vooraf lastig te voorspellen. Ook de gebruikte aanvalsmethode en het beoogde effect van een digitale aanval kan verschillen. Door gebruik te maken van specifieke scenario's voor uw organisatie kan u verschillende digitale aanvallen identificeren waardoor u getroffen kan worden. Scenario's kunnen u handvatten geven om de impact van, en de weerbaarheid van uw organisatie tegen, digitale aanvallen in kaart te brengen.

Het Cybersecuritybeeld Nederland (CSBN) van de NCTV en het NCSC biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en tot slot de risico's. De focus ligt daarbij op de nationale veiligheid. Deze publicatie is van waarde bij het ontwerpen van dreigingsscenario's of het uitvoeren van een risicoanalyse.

Het Dreigingsbeeld Statelijke Actoren (DBSA) van de AIVD, MIVD en NCTV geeft waardevolle inzichten in de dreiging vanuit statelijke actoren. Deze publicatie vormt een waardevolle basis voor scenario's en dreigingen vanuit statelijke actoren.

Tref tenminste de basismaatregelen cybersecurity

De onduidelijkheid over hoe en of de digitale dreiging zich zal manifesteren laat de noodzaak zien om uw digitale veiligheid op orde te hebben. Zowel het NCSC als het DTC hebben twee handreikingen uitgewerkt die, afhankelijk van het volwassenheidsniveau van de organisatie, van waarde zijn voor het verhogen van de digitale weerbaarheid.

In de handreiking "5 basisprincipes van veilig digitaal ondernemen" gaat het DTC verder in op beveiligingsprincipes die ondernemers helpen de digitale weerbaarheid te verhogen.

In de "Handreiking Cybersecuritymaatregelen" gaat het NCSC verder in op 8 basismaatregelen die noodzakelijk zijn om uw organisatie te beschermen tegen digitale dreigingen

4. Keteneffecten

Les 4: Cyberaanvallen beperken zich niet tot landsgrenzen en kunnen internationaal effect hebben.

Digitale aanvallen die zijn uitgevoerd in de context van de Russische invasie van Oekraïne hebben voornamelijk organisaties getroffen in Oekraïne, aangrenzende landen die in het verleden onderdeel waren van de Sovjet-Unie en Rusland zelf. Sommige van deze digitale aanvallen hebben een breder keteneffect gehad.

- **Uitval van een product of dienst kan leiden tot grote verstoringen of zelfs algehele uitval van een of meer producten of diensten.**[46] Wanneer een Nederlandse organisatie afhankelijk is van een digitaal product of dienst en deze uitvalt door een digitale aanval bij een leverancier elders spreken we van een keteneffect.

- **Veel organisaties hebben beperkt inzicht van welke digitale producten en diensten ze afhankelijk zijn.** Dit bleek onder andere uit de Log4J-crisis in december 2021.[47] Door deze complexe digitale dienstverlening is het vooraf moeilijk te overzien hoe keteneffecten zich kunnen manifesteren.

- **Keteneffecten kunnen opzettelijk of onopzettelijk plaatsvinden.** Een aanvaller kan doelbewust een digitaal product of dienst aanvallen om zo opzettelijk grootschalige verstoring te veroorzaken. Een keteneffect kan ook onopzettelijk plaatsvinden, in dit geval leidt een digitale aanval tot onvoorziene neveneffecten.

- **Deze keteneffecten waren het duidelijkst te zien bij de digitale aanval op Viasat.** Viasat is een aanbieder van satellietcommunicatiediensten.[48] Tienduizenden Viasat-modems werden op 24 februari 2022 getroffen door een digitale aanval. Op deze dag begon ook de Russische invasie van Oekraïne. Omdat Viasat diensten levert aan zowel militaire als civiele partijen[49] was de verstoring door deze digitale aanval tot ver buiten Oekraïne merkbaar. Zo waren duizenden windmolens in Europa tijdelijk onbereikbaar[50] en was het internet in sommige afgelegen gebieden tijdelijk niet toegankelijk.[51]

  Ook werd in Oekraïne desinformatie verspreid door een digitale aanval op een toeleverancier. Zo werden zeventig Oekraïense overheidswebsites in de nacht van 13 op 14 januari 2022 beklad met verontrustende teksten. Dit kwam doordat een gezamenlijke toeleverancier was getroffen door een digitale aanval.[52]

Impact op Nederlandse organisaties

Als klein en open handelsland is Nederland sterk vervlochten met het buitenland. Nederland is afhankelijk van internationale handels- en productieketens.[53] Dit geldt ook voor digitale producten en diensten; veel Nederlandse organisaties zijn afhankelijk van buitenlandse leveranciers.

- **De Nederlandse internationale oriëntatie en integratie komt ook met risico's.** Het kan lastig zijn zicht te houden op alle toeleveranciers van digitale diensten en producten. Een compromittatie bij een internationale toeleverancier kan zorgen voor effecten in Nederland. Daarnaast kan malware, indien systemen niet goed gesegmenteerd zijn, ook overslaan vanuit een systeem in het buitenland naar Nederlandse systemen.

- **Keteneffecten zijn vaak niet te voorspellen of vooraf te overzien.** Uitval kan tot een ketenreactie leiden die, vanwege de complexiteit van veel informatiesystemen, vooraf moeilijk in kaart te brengen is.

Handelingsperspectief

Segmenteer netwerken

Door het segmenteren van uw netwerk beperkt u de gevolgen van een digitale aanval. Segmenteren betekent dat een netwerk in meerdere zones wordt verdeeld. Hierdoor kan een aanval op een onderdeel of toeleverancier van uw organisatie in het buitenland moeilijker overslaan op uw netwerk.

In de basismaatregelen van het NCSC staat het belang van netwerksegmentatie beschreven. KPN zet in een blog op hoofdlijnen uiteen hoe netwerksegmentatie uit te voeren. Het Amerikaanse National Institute of Standards and Technology beschrijft in "SP 800-215" in detail hoe een gesegmenteerd netwerk is opgebouwd.

Gebruik Zero Trust-principes in uw IT-infrastructuur

Door toepassing van Zero Trust-principes worden er binnen uw netwerksegmenten verschillende verdedigingslagen aangebracht. Het Zero Trust-model gaat ervan uit dat netwerkverkeer in de basis niet te vertrouwen is en daardoor altijd geverifieerd moet worden. Dit maakt het lastiger voor aanvallers zich lateraal te verplaatsen over een netwerk.

Zie voor meer informatie over Zero Trust en hoe deze principes toe te passen zijn op uw systemen het factsheet "Bereid u voor op Zero Trust" en de expertblog "What about zero trust?" van het NCSC.

Breng uw toeleveringsketen in kaart

Een softwaretoeleveringsketen betreft alle codes, mensen, systemen en processen die bijdragen aan het ontwikkelen en uitvoeren van uw software. Ongewenste afhankelijkheden hierin kunnen ervoor zorgen dat uw organisatie extra kwetsbaar is voor dreiging die voortvloeit uit een politiek conflict. Denk hierbij ook aan leveranciers in het buitenland die, bijvoorbeeld door een boycot of digitale aanval, niet meer bereikbaar kunnen zijn. Ook kunnen toeleveranciers vatbaar blijken voor ongewenste politieke inmenging. Neem ook dit mee in een risicoanalyse.

Inzicht in de gebruikte systemen en software in uw organisatie, en de toegang daartoe beperken tot wat minimaal nodig is, beschermt onder andere tegen het overslaan van cyberincidenten binnen een keten. Dit is onderdeel van de "Handreiking Cybersecuritymaatregelen". Incidenten binnen uw toeleveringsketen kunnen ook problemen voor uw organisatie opleveren zonder dat het incident op u overslaat. Het Digital Trust Center biedt handvatten voor het maken van afspraken met een IT-leverancier.

Installeer software updates tijdig

Digitale aanvallen kunnen, door het gebruik van ongepatchte kwetsbaarheden, grootschalig worden uitgevoerd. Door tijdig patchbeleid zorgt u ervoor dat aanvallers beperkt de tijd hebben misbruik te maken van kwetsbaarheden. Dit verkleint de kans dat een eerder uitgevoerde digitale aanval overslaat op uw systemen.

Het installeren van software updates is een van de "basismaatregelen cybersecurity". Zie voor meer informatie de websites van het NCSC en het DTC.

Referenties

Meer informatie?

Vanuit de Universiteit van Amsterdam en de Nederlandse Defensie Academie is eind 2022 een publicatie uitgebracht waarin verder wordt ingegaan op digitale oorlogsvoering gedurende de oorlog in Oekraïne.

> Zie hiervoor de publicatie "The 'Next' War Should Have Been Fought in Cyberspace, Right?" van Paul Ducheine, Peter Pijpers en Kraesten Arnold.[3]

Het NCSC brengt daarnaast ook een nieuwe serie van de podcast "Enter" uit. In deze podcast gaat het NCSC met NCSC'ers, cyberexperts en andere betrokkenen verder in op hoe Nederland om is gegaan met de oorlog in Oekraïne en daaraan verbonden cybersecurityvraagstukken.

> Podcast "Enter" van het NCSC is te beluisteren op Spotify en Apple podcasts.

[1] "DDoS-aanvallen treffen aantal ziekenhuizen", Z-CERT, bezocht op 31 januari 2023.

[2] "Digitale aanvallen oorlog Oekraïne", NCSC, 31 maart 2022.

[3] Ducheine, Pijpers en Arnold, "The 'Next' War Should Have Been Fought in Cyberspace, Right?", Amsterdam Law School Legal Studies Research Paper No. 2022-47, 2022.

[4] Dit blijkt uit onderzoek van het Instituut Clingendael dat is uitgevoerd na de Russische inval van Oekraïne.

Monika Sie Dhian Ho, Mark Elchardus, Christopher Houtkamp en Teun van der Laan, "Tussen hoop en vrees", Clingendael, 30 december 2022.

[5] "Webinar: Huidig beeld en digitale impact oorlog Oekraïne", NCSC en DTC, 9 maart 2022.

[6] Het woord hacktivisme is een samentrekking van hacker en activisme. Hacktivisten zijn niet statelijke actoren die uit ideologische motieven digitale aanvallen met een activistisch oogmerk uitvoeren.

[7] James Pearson, "Ukraine launches 'IT army,' takes aim at Russian cyberspace", Reuters, 27 februari 2022.

[8] "Pro-Russian Hacktivist Groups Target Ukraine Supporters", Intel471, 14 september 2022.

[9] Pierluigi Paganini, "Anonymous targets western companies still active in Russia", SecurityAffairs.co, 24 maart 2022.

[10] Sergiu Gatlan, "Pro-Russian hacktivists take down EU Parliament site in DDoS attack", BleepingComputer, 23 november 2022.

[11] Een website van een luchthaven in de VS is het doelwit van een DDoS-aanval. Later wordt deze aanval opgeëist door de pro-Russische hacktivistische actor Killnet die deze aanval heeft uitgevoerd in reactie op Amerikaanse wapenleveranties aan Oekraïne.

[12] Estland heeft een grote DDoS-aanval afgeslagen nadat het land een aantal Sovjet-monumenten heeft verwijderd. Deze aanvallen zouden zijn uitgevoerd door de hacktivistische groepering Killnet.

Andrius Sytas, "Estonia says it repelled major cyber attack after removing Soviet monuments", Reuters, 18 juli 2022.

[13] Verschillende landen zoals Italië, Litouwen, Finland en Letland. Bij al deze landen werden digitale aanvallen uitgevoerd in reactie op een ontwikkeling die als anti-Russisch wordt opgevat.

[14] Mike Moore, "Eurovision 2022 was targeted by Russian hackers", TechRadar, 16 mei 2022.

[15] 360Netlab, Twitter, 16 februari 2022. https://twitter.com/360Netlab/status/1493797519725367302

[16] "De oorlog in Oekraïne en onze nationale veiligheid", NCTV, 30 maart 2022.

[17] Kamerstuk 3891936, "Stand van zaken cyber security in relatie tot het conflict in Oekraïne", 11 maart 2022.

[18] "Oorlog Oekraïne", Het Openbaar Ministerie, bezocht op 30 januari 2023.

[19] "Wanneer vindt er een veiligheidsonderzoek plaats?", Rijksoverheid.

[20] "#Cloud4Ukraine", Dutch Cloud Community, bezocht op 31 januari 2023.

[21] Eric Geller,"Ukraine prepares to remove data from Russia's reach", Politico, 22 februari 2022.

[22] Deze malware was WisperGate. Deze destructieve malware is erop gericht de Master Boot Records (MBR) van getroffen systemen te beschadigen. Daardoor raakt een getroffen systeem permanent onbruikbaar.

"Destructive malware targeting Ukrainian organizations", Microsoft, 15 januari 2022.

[23] Joyce Hakmeh en Esther Naylor, "How the tech community has rallied to Ukraine's cyber-defence", The Guardian, 7 maart 2022.

[24] "UA Crisis", ESET

[25] "Ukraine response", SentinalOne.

[26] "Ukraine crisis resource center", Mandiant.

[27] Unit42. https://unit42.paloaltonetworks.com/

[28] Deze lijst is niet exclusief. Veel andere organisaties en onderzoeksinstituten die hier niet genoemd zijn hebben waardevolle dreigingsinformatie gedeeld en daarmee bijgedragen aan een gezamenlijk dreigingsbeeld.

[29] Thomas Brewster, "Ukraine's engineers battle to keep the internet running while Russian bombs fall around them", Forbes, 22 maart 2022.

[30] Chris Vallance, "Ukraine war: Major internet provider suffers cyber-attack", BBC, 28 maart 2022.

[31] Matt Burgess, "Russia is taking over Ukraine's internet", WIRED, 15 juni 2022.

[32] Emile Aben, "The resilience of the internet in Ukraine", RIPE Labs, 10 maart 2022.

[33] Op 26 februari 2022 verzocht de Oekraïense vicepremier Mykhailo Fedorov SpaceX CEO Elon Musk om Starlink te activeren boven Oekraïne en Oekraïne terminals te verstrekken.

Callie Patteson, "Ukrainian vice prime ministers asks Elon Musk for Starlink satellites as Russia invades", New York Post, 26 februari 2022.

[34] Sam Raskin, "Elon Musk activates Starlink in Ukraine after vice prime minister's plea", New York Post, 27 februari 2022.

[35] "Nederlandse uitvoering sancties tegen Rusland en Belarus", Rijksoverheid.

[36] Maciej Góra, Ewelina Kasprzyk, Eliza Kotowska en Michał Krawczyk, "The twilight of the neutrality of digital technology", The Kosciuszko Institute, 2023.

[37] "Nederlandse hulp voor Oekraïne", Rijksoverheid.

[38] Zie het concept Fog of War dat gaat over de onzekerheid in situationeel overzicht bij militaire operaties; "War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth." Carl von Clausewitz, "On War", 1832, (ed. Peter Paret, 1989), 101.

[39] Talkshow Op1 besteedde op 25 februari 2022 bijvoorbeeld uitgebreid aandacht aan de onzekere effecten van een mogelijke "cyberoorlog".

"Ronald Prins over de onzichtbare cyberoorlog", Op1, 25 februari 2022.

[40] "Digitale aanvallen oorlog Oekraïne", NCSC, 26 februari 2022.

[41] John Bateman, "Russia's wartime cyber operations in Ukraine: Military impacts, influences and implications". Carnegie Endowment, 16 december 2022,

[42] James Lewis, "Cyber War and Ukraine", Center for Strategic and International Studies, 16 juni 2022.

[43] Nick Huber, "What Ukraine's cyber defence tactics can teach other nations", Financial Times, 9 november 2022.

[44] Andy Greenberg, "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless", WIRED, 10 november 2022.

[45] "Digitale aanvallen Oekraïne: een tijdlijn", NCSC.

[46] Eric Luiiff en Marieke Klaver, "Afhankelijkheden en keteneffecten", Magazine Nationale Veiligheid en Crisisbeheersing, 2015.

[47] "Log4J", NCSC.

[48] Matt Burgess, "A Mysterious Satellite Hack Has Victims Far Beyond Ukraine", WIRED, 23 maart 2022.

[49] Ellen Nakashima, "Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say", The Washington Post, 24 maart 2022.

[50] Maria Sheahan, Christoph Steitz en Andreas Rinke, "Satellite outage knocks out thousands of Enercon's wind turbines", Reuters, 28 februari 2022.

[51] "KA-SAT Network cyber attack overview", Viasat, 30 maart 2022.

[52] "Фрагмент дослідження кібератак 14.01.2022", CERT-UA, 26 januari 2022.

[53] "Nederland handelsland 2021", CBS, 14 september 2021.

Uitgave
Nationaal Cyber Security Centrum
(NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

februari 2023