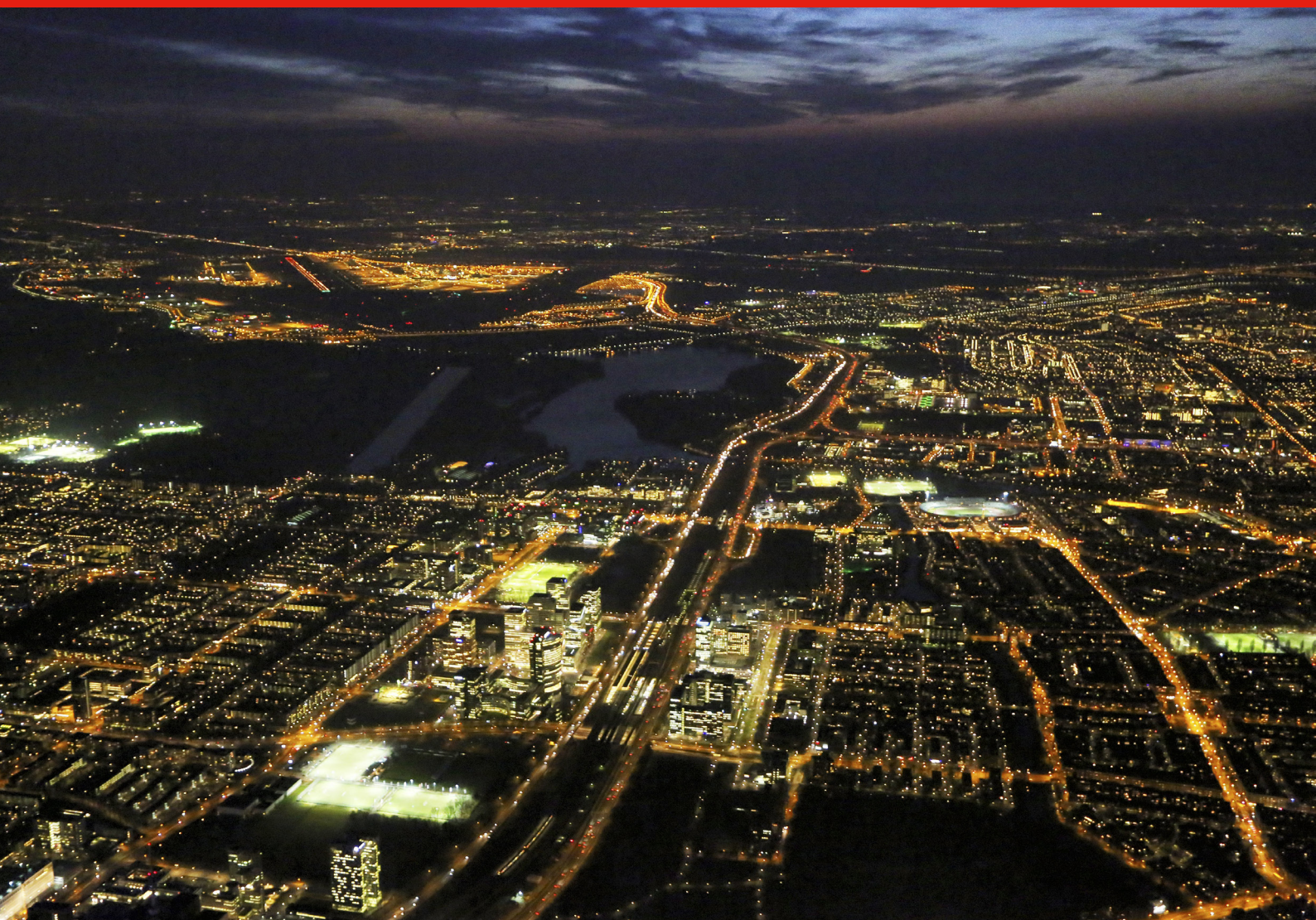
Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland 2023

De ontwikkeling van 'Generatieve AI', een vorm van AI die op basis van door de gebruiker gegeven opdrachten of vragen nieuwe content kan creëren uit bestaande data, gaat razendsnel. De impact op de samenleving kent nog vele onduidelijkheden. Hier wordt ook in dit CSBN aandacht aan besteed (p.41). Om de mogelijkheden te illustreren is het coverbeeld van dit CSBN met behulp van Midjourney gegenereerd. Midjourney genereert afbeeldingen uit natuurlijke taalbeschrijvingen, "prompts" genoemd. Voor dit coverbeeld is het volgende prompt gebruikt: ***Skyline of Zuidas from above, digital ecosystem with technology and connections. Daylight, Photorealistic photography, real life.*** *Ter vergelijking is hieronder een echte foto van de ZuidAs geplaatst.*



Inhoudsopgave

Verwacht het onverwachte

Als er één terrein is waarvoor geldt dat ervaringen uit het verleden geen garanties geven voor de toekomst, is dat digitale veiligheid. Digitale veiligheid vraagt een voortdurende en complexe evenwichtsoefening om uiteenlopende belangen, digitale dreigingen en digitale weerbaarheid in balans te krijgen of te houden. Vele partijen leveren inspanningen om de digitale weerbaarheid te verhogen en gevrijwaard te blijven van cyberincidenten. Voor organisaties geldt nog altijd dat het implementeren van basismaatregelen op het gebied van cybersecurity al veel effect kan hebben. Toch zijn cyberincidenten niet altijd te voorkomen. Die kunnen zich onverwacht voordoen en zij kunnen een onverwachte oorzaak, aard en impact hebben.

Dit hoofdstuk bevat de hoofdboodschappen van dit CSBN. Verdere onderbouwing vindt plaats in de hoofdstukken twee tot en met vijf.

Hoofdbevindingen CSBN 2023

1. De veiligheid van digitale processen is en blijft essentieel in onze sterk gedigitaliseerde maatschappij en is dus onlosmakelijk verbonden met de nationale veiligheid.
2. De digitale dreiging voor Nederland is onverminderd groot. Wel is die dreiging voortdurend aan verandering onderhevig. Zo is er sprake van geopolitieke verharding, met de Russische oorlog tegen Oekraïne als prominent voorbeeld. Die oorlog heeft daarnaast (mede) geleid tot een opleving van hacktivisme: het uit ideologische overwegingen uitvoeren van cyberaanvallen. Bij verdere escalatie van de oorlog kan de digitale dreiging abrupt veranderen en kunnen Nederlandse belangen worden geraakt.
3. De in het CSBN 2022 benoemde strategische thema's leiden nog onverkort tot complicaties voor risicobeheersing. Enkele veranderingen ten opzichte van vorig jaar zijn opgevallen:
   - de extra eisen voor digitale veiligheid die onder andere voortkomen uit nieuwe Europese wet- en regelgeving;
   - het onder druk staan van de verzekerbaarheid van digitale risico's;
   - de steeds verder toenemende onderlinge verwevenheid binnen een breder – niet alleen digitaal - ecosysteem;
   - de gelegenheidsstructuur die het digitale ecosysteem vormt voor cyberaanvallen.
4. Het verkleinen van de in het CSBN 2022 benoemde scheefgroei tussen de digitale dreiging en de weerbaarheid blijft een grote opgave. De aard van de digitale risico's voor de nationale veiligheid is niet fundamenteel gewijzigd.
5. Operationele technologie (OT) is een kwetsbare bouwsteen voor vitale processen. OT speelt een centrale rol in het aansturen, monitoren en beheren van fysieke processen binnen (vitale) organisaties. De veiligheid van OT is van vitaal belang, maar kent belangrijke uitdagingen. Ondanks groeiende aandacht voor de weerbaarheid van OT, is er ruimte voor verbetering.
6. Bijzondere kenmerken van digitale risico's vragen een bredere manier van beheersing dan andere risico's. Zo maken digitale risico's onderdeel uit van een breder, dynamisch én complex risicopalet en is de digitale ruimte een uiterst complex systeem dat zich lastig laat doorgronden. Bij een bredere manier van beheersing valt te denken aan een benadering waarin digitale risico's worden beschouwd als een integraal onderdeel van de risico's voor de nationale veiligheid. Verder kan de invalshoek van 'assume breach' (ga ervan uit dat er een cyberincident is) behulpzaam zijn.

Digitale dreiging onverminderd groot

De digitale dreiging voor Nederland is onverminderd groot, vooral als gevolg van:

1. De wisselwerking met andere, deels niet digitale, dreigingen en ontwikkelingen. Cyberincidenten kunnen het gevolg zijn van bijvoorbeeld een verstoring van de energievoorziening. Zij kunnen op hun beurt de oorzaak worden van een verstoring van de energievoorziening. Bovendien geldt dat een hele kluwen van ontwikkelingen van invloed is op digitale dreigingen. Een voorbeeld daarvan zijn technologische ontwikkelingen in zogeheten 'Generatieve AI', waaronder ChatGPT, Quantum computing en 'de metaverse'. Ook kunnen dreigingen zich gestaag onder de radar opbouwen totdat een kantelpunt optreedt. Daarna is het heel moeilijk om die dreigingen te keren. Zo'n gestage opbouw kan bijvoorbeeld voorkomen bij afhankelijkheden van bedrijven met een dominante positie in dienstverlenings- en/of digitale markten.

2. De complexiteit en verwevenheid van digitale processen, systemen en netwerken en het grote (groeiende) aanvalsoppervlak in combinatie met veelvoorkomende verouderde informatiesystemen. Als gevolg hiervan ontstaan kwetsbaarheden die cyberactoren kunnen uitbuiten. De kans op grootschalige uitval neemt eveneens toe.

3. Geopolitieke spanningen waardoor statelijke actoren grijpen naar cyberaanvallen als middel om hun belangen te behartigen, met bijvoorbeeld keteneffecten als gevolg. De Russische oorlog tegen Oekraïne is een prominent voorbeeld van die verharding (zie verder in dit hoofdstuk).

4. Het aantrekkelijke verdienmodel voor cybercriminelen. Criminelen verdienen bijvoorbeeld niet alleen aan losgeldbetalingen en illegale dienstverlening als Cybercrime-as-a-Service (CaaS). Veredeling van buitgemaakte informatie met andere informatie én de verkoop daarvan, zijn eveneens lucratief voor criminelen.

5. Internationale conflicten en maatschappelijk controversiële onderwerpen als mogelijke aanleiding voor hacktivisme.

6. De concentratie van informatie en digitale processen, bij uitstek aantrekkelijk voor misbruik door kwaadwillenden en met grote gevolgen bij uitval. Dat geldt bijvoorbeeld voor cloud-dienstverleners.

7. De beperkte kans voor kwaadwillenden om opgepakt en/of uitgeleverd te worden voor het uitvoeren van een cyberaanval.

Cyberincidenten in 2022/2023 passen in beeld van digitale dreiging

De cyberincidenten in de periode maart 2022 tot en met februari 2023 passen in het beeld van de digitale dreiging van de afgelopen jaren. Maatschappij ontwrichtende cyberincidenten in Nederland of andere EU-landen hebben zich niet voorgedaan. De aard van de cyberincidenten bleef divers. Ransomware maakte opnieuw een prominent aandeel uit van cyberaanvallen. Dat ging soms gepaard met publicatie van buitgemaakte informatie. Uitval van digitale processen deed zich eveneens relatief vaak voor. Opvallend ten opzichte van vorige jaren waren cyberaanvallen door hacktivisten, voornamelijk in het buitenland, maar ook enkele in Nederland. Tevens maakten enkele cyberincidenten extra duidelijk dat organisaties onderdeel zijn van een breder ecosysteem en daarbinnen te maken kunnen krijgen met cyberincidenten.

Russische oorlog tegen Oekraïne: omvangrijke cybercampagne, minder impact dan gedacht

In februari 2022 viel Rusland Oekraïne binnen. Russische cyberaanvallen zijn vooral gericht geweest op Oekraïne en de regio. Het betrof spionage en (voorbereidingshandelingen voor) sabotage. Ook verspreidde Rusland desinformatie. De Oekraïense en westerse digitale verdediging hebben de impact van de voortdurende Russische aanvalspogingen kunnen beperken.

De focus van Russische cyberoperaties ligt op spionage om militaire, diplomatieke en economische informatie van zowel Oekraïne als NAVO-lidstaten te bemachtigen. Ten aanzien van de NAVO richt de Russische inlichtingenbehoefte zich onder meer op militaire steun die via NAVO-lidstaten aan Oekraïne geleverd wordt. De Russische cybersabotagecampagne tegen Oekraïne is de meest grootschalige en intensieve uit de geschiedenis, aldus de AIVD en MIVD.

Opvallend is de betrokkenheid van criminele en hacktivistische actoren in de context van de oorlog. Een verder kenmerkend element in het verloop van de oorlog is dat private bedrijven steun aan Oekraïne verlenen. Dat gebeurt vaak in samenwerking met landen die steun bieden aan Oekraïne. Verder houdt Rusland zich bezig met beïnvloeding van de publieke opinie in westerse landen door onder andere desinformatie te verspreiden.

Ontwrichtende cyberaanvallen die de nationale veiligheid van Nederland schaden, hebben zich (nog) niet voorgedaan. Bij verdere escalatie van de oorlog kan de digitale dreiging abrupt veranderen. Cyberaanvallen kunnen dan de nationale veiligheid gaan aantasten. Ook kan Nederland worden geraakt door keteneffecten die doorwerken naar vitale processen en te maken (blijven) krijgen met aanvallen van bijvoorbeeld pro-Russische criminelen.

Strategische thema's leiden nog onverkort tot complicaties voor risicobeheersing

In het CSBN 2022 heeft de NCTV in samenwerking met partners zes strategische thema's geïdentificeerd die de komende jaren relevant zijn voor de digitale veiligheid van Nederland. Deze zijn nog onverkort van toepassing. Bij de reflectie op deze thema's zijn enkele veranderingen opgevallen. Deze komen hieronder aan bod.

Strategische thema's genoemd in het CSBN 2022

- Risico's vormen de keerzijde van een gedigitaliseerde samenleving.
- Digitale ruimte is speelveld voor regionale en mondiale dominantie.
- Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet.
- Marktdynamiek compliceert beheersing digitale risico's.
- Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen.
- Beperkingen in digitale autonomie beperken ook digitale weerbaarheid.

Extra eisen voor digitale veiligheid, maar kost tijd voordat deze effect sorteren

Een belangrijke verandering die de digitale weerbaarheid de komende jaren kan vergroten, zijn de extra eisen voor digitale veiligheid. Deze vloeien voort uit nieuwe Europese wet- en regelgeving, de Nederlandse Cybersecurity Strategie 2022-2028 en het daarvan afgeleide actieplan. De bewustwording over en verdere uitwerking en implementatie van dat alles, vergt wel de nodige doorlooptijd.

Verharding geopolitieke spanningen

Het afgelopen jaar zijn de geopolitieke spanningen verder opgelopen. Sectoren en organisaties kunnen de gevolgen ondervinden van deze verharding, maar daar weinig aan veranderen. Het vormt wel een factor waar bij de bepaling van het gewenste niveau van digitale weerbaarheid rekening mee moet worden gehouden. Zo zou een statelijke actor een ICT-dienstverlener van een vitale organisatie kunnen aanvallen als springplank naar die digitale organisatie.

Verzekerbaarheid digitale risico's onder druk

Hoewel organisaties veel kunnen doen aan digitale weerbaarheid, kunnen cyberincidenten zich toch voordoen en/of is schade niet altijd te voorkomen. De verzekerbaarheid van digitale risico's staat onder druk om uiteenlopende redenen. Een eerste reden die verzekeraars noemen is de toename van digitale risico's. Een tweede reden is dat cyberincidenten kunnen uitgroeien tot een zogeheten systemische crisis en daardoor onverzekerbaar zijn. Verder geldt dat de markt voor cybersecurityverzekeringen in Nederland in omvang beperkt is en in de kinderschoenen staat. Het resultaat van die druk is, of kan zijn: uitsluiting van organisaties met een verhoogd risicoprofiel, voor organisaties te hoge premies of uitsluiting van de schade van vele typen cyberincidenten. Dit alles kan er uiteindelijk toe leiden dat financieel gezonde organisaties ten onder gaan aan de schade die zij lijden door cyberincidenten.

Onderdeel zijn van breder ecosysteem compliceert risicobeheersing

Of het nu gaat om landen, sectoren of organisaties, weinigen zullen onafhankelijk kunnen functioneren van een breder ecosysteem. Denk daarbij aan outsourcing van onderdelen van de bedrijfsvoering, zoals de salarisadministratie, toegangspasbeheer of marktonderzoek. Onderdeel zijn van een breder ecosysteem heeft voordelen, zoals het profiteren van schaalvoordelen en specialistische kennis, waaronder op het terrein van cybersecurity.

Onderdeel zijn van een breder ecosysteem compliceert tegelijkertijd ook risicobeheersing. Zo bestaat lang niet altijd inzicht in afhankelijkheden én kwetsbaarheden in het bredere ecosysteem. Het is bovendien lastig daar grip op te krijgen. Die afhankelijkheden en kwetsbaarheden kunnen wel een substantieel onderdeel zijn van de digitale risico's. Een prominent voorbeeld hiervan deed zich voor in 2023. Grote organisaties huurden onderzoeksbureaus in voor klantonderzoek. Meerdere onderzoekbureaus maakten op hun beurt gebruik van dezelfde softwareleverancier. Toen zich bij die softwareleverancier een datalek voordeed, kwamen de gegevens van naar schatting rond de twee miljoen Nederlanders in de openbaarheid. In dit voorbeeld werden dus klanten van een organisatie slachtoffer van een datalek bij de dienstverlener van de dienstverlener van de organisatie, oftewel in de derde lijn.

Digitale ecosysteem vormt gelegenheidsstructuur voor cyberaanvallen

Cybercriminelen zijn onderdeel van een breder malafide en bonafide digitaal ecosysteem en zijn daarvan afhankelijk. Dit ecosysteem vormt dus een gelegenheidsstructuur voor hen. Door toenemende specialisatie onder cybercriminelen worden ook zij steeds afhankelijker van elkaars (online) diensten in het kader van cybercrime-as-a-service. Ook andere actoren, bijvoorbeeld statelijke, maken daar soms gebruik van. Deze afhankelijkheid geldt ook voor het afnemen van legale diensten, zoals webhosting en communicatiediensten als VPN of domeinregistraties. Deze afhankelijkheid biedt daarentegen ook kansen voor het verhogen van de digitale weerbaarheid. Als het om internetdiensten in de brede zin gaat, zijn principes als aanvaardbaar gebruik, ken-je-klant, het zorgvuldigheidsbeginsel en antimisbruikbepalingen veelal nog vrijblijvend, met alle ruimte voor het wel of niet naleven

ervan als gevolg. Dit biedt cybercriminelen vele kansen om anoniem én schaalbaar te werk te gaan. Kansen die zij niet onbenut laten.

OT: kwetsbare bouwsteen voor vitale processen

Operationele technologie (OT) binnen industriële netwerken, ook wel aangeduid als 'Industrial Automation and Control Systems' (IACS), speelt een centrale rol in het aansturen, monitoren en beheren van fysieke processen binnen organisaties. Daarmee fungeert het ook als motor van vitale sectoren. OT raakt steeds meer vervlochten met informatietechnologie (IT). Daarnaast speelt het 'Industrial Internet of Things' (IIoT) een steeds belangrijker rol in industriële omgevingen. Dit heeft voordelen voor het optimaliseren van processen, maar het brengt ook risico's met zich mee. Zo vergroot deze ontwikkeling het aanvalsoppervlak en daarmee het risico dat OT-systemen gecompromitteerd raken. Ook brengt dit uitdagingen met zich mee voor het beveiligen van dergelijke systemen. Daarbij is onder andere een grotere rol weggelegd voor detectie en mitigatie van digitale aanvallen. Op deze en andere vlakken is er ruimte voor verbetering. Dit vereist specifieke kennis, competenties en samenwerking. Vanuit de overheid zijn er de afgelopen jaren meerdere initiatieven ontwikkeld om dit proces te ondersteunen. Daarbij weten organisaties elkaar onderling steeds beter te vinden. Hier liggen kansen om op voort te bouwen om de weerbaarheid van vitale processen te waarborgen.

Verkleining van scheefgroei tussen digitale dreiging en weerbaarheid nog steeds grote opgave

Het verkleinen van de in het CSBN 2022 benoemde scheefgroei tussen de digitale dreiging en de weerbaarheid blijft een grote opgave: de digitale dreiging blijft immers onverminderd groot en de complicaties voor risicobeheersing zijn onverkort van toepassing.

De aard van de digitale risico's is niet fundamenteel anders ten opzichte van CSBN 2022. Er zijn vier risico's voor de nationale veiligheid (zie kader hieronder). Deze gelden direct of indirect ook voor specifieke sectoren en organisaties en individuele burgers.

Vier risico's voor de nationale veiligheid

1. Ongeautoriseerde inzage in informatie (en eventueel publicatie daarvan), in het bijzonder door spionage. Denk aan spionage gericht op communicatie binnen de Rijksoverheid of spionage om de ontwikkeling van innovatieve technologieën te achterhalen. Denk ook aan inzage in informatie over medewerkers of bedrijfsprocessen als springplank voor cyberaanvallen of andere kwaadaardige doeleinden.
2. Ontoegankelijkheid van processen, zoals door (voorbereidingen voor) sabotage van processen die zorgdragen voor de energievoorziening en cybercriminaliteit, waaronder de inzet van ransomware en DDoS-aanvallen.
3. Schending van de (veiligheid van de) digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leverancierskketens, misbruik van internetprotocollen of sabotage van kabels.
4. Grootschalige uitval: een situatie waarin één of meer processen zijn verstoord als gevolg van natuurlijke of technische oorzaken of als gevolg van niet-moedwillig menselijk handelen.

Alle digitale processen, organisaties en sectoren kwetsbaar

Alle digitale processen, organisaties en sectoren zijn potentieel kwetsbaar voor cyberincidenten. Zij kunnen direct te maken krijgen met cyberaanvallen door kwaadwillenden. Dat geldt vooral voor ongeautoriseerde inzage in informatie (en eventueel publicatie daarvan). Het geldt ook voor ontoegankelijkheid van processen, als gevolg van (voorbereidingen voor) sabotage, de inzet van ransomware en DDoS-aanvallen. Ook kunnen alle landen, sectoren en organisaties indirect de gevolgen ondervinden van een cyberaanval op een andere organisatie of grootschalige uitval in het bredere ecosysteem, bijvoorbeeld wanneer een grote mondiale dienstverlener wordt getroffen.

Vaak gehoord is het argument "in mijn organisatie zijn staten niet geïnteresseerd", "bij mij valt niets te halen" of "in onze sector zijn weinig incidenten". Echter, daarbij wordt over het hoofd gezien dat bijvoorbeeld criminelen continu alle 'digitale deuren' proberen te openen ongeacht de organisatie, met alle gevolgen van dien voor de slachtoffers. Statelijke actoren gaan actief op zoek naar organisaties in ketens, als opstap naar interessante(re) doelwitten. Zo zag de AIVD in 2022 onder andere dat verschillende landen met een offensief cyberprogramma probeerden data te stelen in de (Europese) reis- en luchtvaartsector. Die informatie combineren ze met andere data om mensen die voor hen interessant zijn, te identificeren, op te sporen of te volgen. Organisaties die veel data verwerken, vormen dus een aantrekkelijk doelwit voor cyberactoren. Een ander voorbeeld zijn ICT-dienstverleners die voor vele organisaties werken. Ook kunnen organisaties worden aangevallen als systemen een kwetsbaarheid bevatten, zonder dat een kwaadwillende kijkt om wat voor organisatie het gaat. Symbolische Nederlandse doelwitten, zoals internationaal bekende Nederlandse multinationals of instanties, kunnen eveneens een doelwit vormen, met als onderliggend motief wraak op Nederland of de Nederlandse regering. Zo zou steun aan Oekraïne vanuit Nederland voor

bijvoorbeeld hacktivisten aanleiding kunnen zijn tot DDoS-aanvallen of digitale bekladdingen van websites (defacement).

Bijzondere kenmerken digitale risico's vragen om bredere manier van beheersing

Digitale risico's hebben enkele bijzondere kenmerken die een bredere manier van beheersing vragen dan andere risico's. Dat geldt op het niveau van organisaties, maar zeker ook op sectoraal en landelijk niveau. Ten eerste maken digitale risico's onderdeel uit van een breder, dynamisch én complex risicopalet. Zo is er een wisselwerking met andere, zeker ook niet digitale, dreigingen en ontwikkelingen. Ook is gewezen op risico's die voortkomen uit het bredere ecosysteem waar landen, sectoren en organisaties onderdeel van zijn. Verder geldt dat ten opzichte van andere risico's de digitale ruimte een uiterst complex systeem is. Informatie over cyberincidenten is weliswaar soms beschikbaar, maar lang niet voor iedereen. Het is onderling slechts in beperkte mate vergelijkbaar en lastig te interpreteren. Voor de beheersing van overstromingen is bijvoorbeeld veel meer informatie beschikbaar over een langere periode. Het simuleren van incidenten of het bouwen van modellen om het verloop van incidenten en gevolgen in kaart te brengen, is behulpzaam voor risicomanagement, maar uiterst complex voor digitale risico's. Wie overziet wat de impact is van een grootschalige en meerdaagse verstoring van internetdiensten in Nederland op digitale processen en de gevolgen daar weer van op de maatschappij, sectoren en organisaties? En, het internet laat zich uiteraard niet een dag uitzetten om te kijken wat er gebeurt.

Uit de aard van het belang van digitale veiligheid en de aard van de digitale dreiging vloeit voort dat beheersing van digitale risico's zeker niet alleen een vraagstuk is voor technische experts. Het is ook, of wellicht vooral, een vraagstuk van governance en/of risicomanagement voor politici en bestuurders op het niveau van organisaties, sectoren en landen. Digitale risico's zijn een integraal onderdeel van een breder risicopalet en vragen daarom om integraal risicomanagement. Als gevolg van nieuwe Europese wet- en regelgeving krijgen bestuurders van veel organisaties binnen de EU overigens een grotere wettelijk verankerde verantwoordelijkheid voor digitale veiligheid.

Als er één terrein is waarvoor geldt dat ervaringen uit het verleden geen garanties geven voor de toekomst, is dat wel digitale veiligheid. Vandaar de oproep om breder te kijken dan incidenten die zich hebben voorgedaan en breder te kijken dan eisen waaraan moet worden voldaan. Dat geldt bijvoorbeeld voor het anticiperen op mogelijke gevolgen voor digitale veiligheid van generatieve AI, dat zich snel aan het ontwikkelen is en Quantum computing. Een andere nuttige invalshoek is de aanname dat er al sprake is van een cyberincident. Dat leidt tot een bredere blik dan bijvoorbeeld een toets of er voldaan is aan de technische maatregelen om te voorkomen dat klanten- of personeelsinformatie door onbevoegden kan worden ingezien. Een focus op een situatie waarin klanten- of personeelsinformatie wél is gemanipuleerd of op het internet is geplaatst, kan behulpzaam zijn voor risicobeheersing. Wat is dan het handelingsperspectief? Hoe groot kunnen de gevolgen zijn en op welke wijze kunnen die gevolgen dan nog worden beperkt? En dan de ultieme vraag of de balans tussen dreiging, belang en weerbaarheid wel de gewenste is. Kortom: "verwacht het onverwachte" en wees daarop voorbereid.

Door een technische storing in een tunnel moet deze worden afgesloten. Daardoor loopt het verkeer op de snelweg vast. In de omliggende steden kan een verkeersinfarct ontstaan.

1 Inleiding

Doel en afbakening

Het Cybersecuritybeeld Nederland 2023 (CSBN 2023) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en tot slot digitale risico's. Daarnaast heeft het CSBN 2023 tot doel om inzicht te geven in mogelijke veranderingen in de strategische thema's die in CSBN 2022 zijn uitgewerkt. Deze thema's vormden een inhoudelijke basis voor de Nederlandse Cybersecurity Strategie 2022-2028. Dit CSBN vormt een inhoudelijke basis voor de evaluatie van het daarvan afgeleide actieplan.

Sleutelbegrippen

Vanwege de verwevenheid van de fysieke en digitale ruimte en omwille van de leesbaarheid, worden de termen 'cyber' en 'digitale' slechts beperkt gebruikt. In het CSBN zijn de belangrijkste begrippen als volgt gedefinieerd[1]:

- **Belang**: waarden, verworvenheden, materiële en immateriële zaken waaraan schade kan ontstaan als een cyberincident zich voordoet en het gewicht dat de maatschappij of een partij aan de verdediging ervan toekent. In het CSBN ligt de focus op nationale veiligheidsbelangen.
- **Cyberaanval**: moedwillige activiteit van een actor die is gericht op het met digitale middelen verstoren van één of meer digitale processen.
- **Cyberincident**: (samenhangende set van) gebeurtenissen of activiteiten die kunnen leiden tot verstoring van één of meer (digitale) processen.
- **Cybersecurity**: het geheel aan maatregelen om relevante risico's tot een aanvaardbaar niveau te reduceren. De maatregelen kunnen zijn gericht op het voorkomen van cyberincidenten en - wanneer cyberincidenten zich hebben voorgedaan - deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau is, is de uitkomst van een risico-afweging.
- **Digitaal proces (hierna: proces)**: een proces dat geheel of gedeeltelijk wordt uitgevoerd door de complexe en onderling samenhangende interactie tussen mensen en vele componenten van hardware, software en/of netwerken. Volledig geautomatiseerde processen, zoals procesbesturingssystemen, vallen ook onder het begrip.
- **Digitale ruimte**: de complexe omgeving die het resultaat is van onderling verweven digitale processen, ondersteund door wereldwijd gedistribueerde fysieke informatie- en communicatietechnologie (ICT-)apparaten en verbonden netwerken. De digitale ruimte wordt vanuit drie invalshoeken of lagen benaderd: 1) digitale processen uitgevoerd (of in gang gezet) door mensen; 2) de technische laag (van IT en OT) die de digitale processen mogelijk maakt; 3) de risicomanagement- en/of governance laag die de twee andere lagen bestuurt.
- **Dreiging**: een opzettelijk of niet-opzettelijk gevaar dat kan leiden tot een cyberincident of een combinatie van gelijktijdige of opeenvolgende cyberincidenten.
- **Risico**: de (combinatie van de) kans dat een dreiging leidt tot een cyberincident én de impact van het cyberincident op belangen, beide in relatie tot het actuele niveau van digitale weerbaarheid.
- **Uitval**: een situatie waarin één of meer digitale processen zijn verstoord als gevolg van natuurlijke of technische oorzaken, of als gevolg van menselijke fouten.
- **Verstoring**: een aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie(verwerking), dat wil zeggen, een verstoring in de technische laag van de digitale ruimte.
- **Weerbaarheid**: het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Wat een aanvaardbaar niveau van weerbaarheid is, is de uitkomst van een risico-afweging en daarop gebaseerde politieke en/of bestuurlijke keuzen als het gaat om (onder andere) de juiste technische, procedurele of organisatorische maatregelen te kiezen.

Het accent ligt op de nationale veiligheid. Digitalisering biedt vele kansen, maar leent zich ook voor allerlei vormen van misbruik en er kan sprake zijn van uitval. Het CSBN richt zich niet op de kansen van digitalisering, maar wél op verstoringen van (kritische) processen met een digitale component.

Het CSBN is primair bedoeld voor strategie- en beleidsvorming op nationaal niveau. Het beoogt het kabinet, de leden van de Eerste en Tweede Kamer, ambtenaren, beleidsmakers, overige bestuurders en directies en andere geïnteresseerden inzicht te geven in de digitale risico's voor Nederland. Cybersecuritybedrijven en –professionals gebruiken het CSBN als referentiekader richting de eigen bestuurders of klanten. Het CSBN is ook bedoeld als hulpmiddel voor risicomanagement, waarbij het zich specifiek richt op de identificatie en analyse van risico's, een van de stappen in een risicomanagementproces. Tot slot is het CSBN toegankelijk voor het brede publiek.

Leeswijzer

Dit CSBN bestaat uit het voorgaande hoofdstuk waarin de hoofdboodschappen zijn verwoord en uit vijf verdiepende hoofdstukken. Het hoofdstuk vòòr deze Inleiding bevat de hoofdboodschappen. Deze indeling beoogt dat lezers uit verschillende doelgroepen makkelijk door het CSBN kunnen navigeren en zich kunnen richten op de onderwerpen die aansluiten bij hun professionele rol of interesse. De verdiepende hoofdstukken hebben de volgende thema's:

- Hoofdstuk 2, het Jaarbeeld, geeft een overzicht van relevante incidenten in Nederland in de periode maart 2022 t/m februari 2023 en de duiding daarvan.
- Hoofdstuk 3 blikt terug op de cybercomponent in de Russische oorlog tegen Oekraïne en beoordeelt wat de gevolgen daarvan zijn geweest en kunnen zijn.
- Hoofdstuk 4 gaat nader in op het belang van Operationele technologie (OT) en risico's die daaraan kleven.
- Hoofdstuk 5 beschrijft nieuwe inzichten en/of veranderingen die zijn opgetreden in zes strategische thema's die complicaties vormen voor strategische risicobeheersing.
- Hoofdstuk 6 schetst drie scenario waarbij een cyberincident in een digitaal ecosysteem niet alleen leidt tot problemen in de bedrijfsvoering van de organisatie waar het incident zich voordoet, maar ook tot schade voor burgers of andere organisaties in het ecosysteem. Dit hoofdstuk is vooral bedoeld om de lezer te helpen anticiperen op mogelijke incidenten.

Bijlage 1 bevat een verantwoording van de totstandkoming van het CSBN. Bijlage 2 bevat de bronnen en referenties.

Een stroomstoring legt het leven (deels) stil. Straatverlichting valt uit en huishoudelijke apparaten zijn dan niet te gebruiken. In een ziekenhuis kan de patiëntenzorg niet altijd doorgaan.

2 Jaarbeeld

Cyberincidenten in de periode maart 2022 tot en met februari 2023 passen in het beeld over de digitale dreiging van de afgelopen jaren. Maatschappij ontwrichtende cyberincidenten in Nederland of andere EU-landen hebben zich niet voorgedaan. De aard van de cyberincidenten bleef divers. Cyberaanvallen waren voornamelijk afkomstig van statelijke en criminele actoren. Uitval van digitale processen deed zich relatief vaak voor. Opvallend ten opzichte van vorige jaren waren cyberaanvallen door hacktivisten, voornamelijk in het buitenland, maar ook enkele in Nederland. Ook maakten de cyberincidenten extra duidelijk dat organisaties onderdeel zijn van een breder ecosysteem en daarbinnen kwetsbaar kunnen zijn.

Incidenten in Nederland passen in beeld van digitale risico's en type doelwitten

Verstoorde digitale processen door voornamelijk ransomware-aanvallen

Tijdens de rapportageperiode hebben actoren doelbewust digitale processen ontoegankelijk gemaakt. Het ging daarbij vooral om ransomware-aanvallen. Deze richten zich al lang niet meer alleen op het versleutelen van data. Criminelen stelen nu ook vaak data om daarmee andere misdrijven te plegen, zoals het onder druk zetten van slachtoffers om losgeld te betalen door te dreigen met publicatie van deze gestolen data. Bij diverse ransomware-aanvallen werd informatie daadwerkelijk gepubliceerd en kwam gevoelige informatie beschikbaar voor derden.

Ook Nederland getroffen door DDoS-aanvallen van hacktivisten

Deze rapportageperiode kende de nodige berichten over DDoS-aanvallen die (kortstondig) digitale processen verstoorden. Het ging daarbij vooral om aanvallen buiten Nederland en van hacktivisten. Een voorbeeld hiervan is de DDoS-aanval op het Europees parlement in november 2022. Pro-Russische hacktivisten riepen daarnaast wel op tot DDoS-aanvallen op (onder andere) Nederlandse ziekenhuizen en enkele ziekenhuizen in Nederland werden daadwerkelijk voor kortere tijd slachtoffer van DDoS-aanvallen. Naast pro-Russische hacktivisten zouden religieuze hacktivisten DDoS-aanvallen op Nederlandse websites hebben uitgevoerd als vergelding voor een Koranverscheuring. Hierbij dient de kanttekening geplaatst te worden dat dergelijke groepen media-belust zijn en bewust claims opkloppen of zelfs zaken claimen die niet hebben plaatsgevonden. Ook is attributie van hacktivistische activiteiten lastig.

Datalekken door kwaadwillenden en niet-moedwillig menselijk handelen

Meer dan eens hebben we deze periode gezien dat er sprake was van ongeautoriseerde inzage in informatie en soms ook publicatie van buitgemaakte informatie, resulterend in datalekken. Hierbij ging het vaak om ransomware-actoren. Zo was er deze periode sprake van een incident waarbij een aanvaller erin slaagde toegang te krijgen tot een zorgplatform en gevoelige informatie in te zien. Ook niet-moedwillig menselijk handelen kan leiden tot het lekken van gevoelige informatie. Zo waren door een technische handeling van de ICT-leverancier van de gemeente Veenendaal vertrouwelijke documenten tijdelijk onbedoeld publiekelijk beschikbaar.

Uitval als gevolg van technische oorzaken

Grootschalige uitval van vitale processen door technische storingen is in deze rapportageperiode niet voorgekomen, maar wel diverse uitval-incidenten. Uitval kan verschillende oorzaken hebben waaronder technische problemen en niet-moedwillig menselijk handelen. Deze periode leidden met name technische oorzaken meer dan eens tot uitval. Prominent in het nieuws kwam een ICT-storing en falend back-up systeem die voor aanzienlijke treinuitval in de regio Rotterdam zorgde.[2]

Aanvallen op niet-vitale bedrijven kunnen toch vitale sector en Rijksoverheid raken

Incidenten illustreren dat er vanuit het bredere ecosysteem (zie hoofdstuk 5) risico's uitgaan voor veel organisaties doordat zij in sterke mate verbonden en verweven zijn met processen van andere organisaties. Een cyberincident bij een niet-vitale organisatie kan daardoor ook gevolgen hebben voor vitale sectoren en de rijksoverheid. De ransomware-aanval op ID-ware is illustratief voor hoe een cyberaanval op een niet-vitaal bedrijf toch kan doorwerken naar aanbieders van vitale diensten en de Rijksoverheid. Persoonsgegevens van onder andere medewerkers van de Eerste en Tweede Kamer lekten door de aanval op dit bedrijf.

Cyberaanvallen op gemeenten vormen risico voor gevoelige informatie

Een cyberaanval op publieke organisaties kan grote gevolgen hebben voor de dienstverlening en het functioneren van deze organisaties. Daarnaast kwam van diverse gemeenten gevoelige informatie op straat te liggen na cyberaanvallen. Datalekken bij publieke organisaties kunnen onder andere burgers raken. Veel gevoelige informatie is over hen immers bij gemeenten vastgelegd vanwege het uitvoeren van wettelijke taken. Dit maakt een cyberaanval waarbij informatie wordt gestolen en gelekt extra problematisch. Kwaadwillenden kunnen misbruik maken van die informatie voor bijvoorbeeld fraude of spionage.

Incidenten in het buitenland kunnen zich ook voordoen in Nederland

Geopolitieke situatie van invloed op dreigingslandschap Nederland

Het CSBN 2022 stelt dat cyberaanvallen door statelijke actoren het nieuwe normaal zijn en dat landen de digitale ruimte gebruiken om geopolitieke voordelen te behalen. Ook in deze rapportageperiode zijn cyberoperaties aan het licht gekomen die in verband worden gebracht met statelijke actoren, waaronder spionage, diefstal van intellectueel eigendom en het inzetten van destructieve malware. Deze cyberoperaties moeten zeker worden gezien in het licht van geopolitieke ontwikkelingen (zie verder hoofdstuk 5).

Misbruik spyware door buitenlandse actoren tegen journalisten, politici en/of dissidenten ook in Nederland denkbaar

Al jaren wordt bericht over spionagesoftware die wordt gebruikt om bijvoorbeeld journalisten, activisten, politici en dissidenten digitaal te volgen. In deze rapportageperiode was er veel aandacht voor de inzet (en het misbruik) van spyware in en door Europese landen. Uit een rapport van een Europese onderzoekscommissie blijkt dat ook binnen Europa spyware wordt ingekocht en gebruikt.[3] De zorg hierbij is vooral het misbruik van dergelijke software, waarbij het middel zonder wettelijke waarborgen wordt toegepast en ingezet tegen minderheden of tegenstanders van machthebbers. Zo werd bekend dat onder andere in Polen en Spanje spyware is ingezet tegen politici en activisten. Het is voorstelbaar dat buitenlandse mogendheden spyware inzetten tegen Nederlandse journalisten, activisten, dissidenten of zelfs politici. Denkbaar is ook dat criminelen spyware inzetten tegen bijvoorbeeld vermogensbeheerders om te kunnen profiteren van hun kennis over gevoelige transacties.

Vernietiging van data door wiperware kan zich ook voordoen in Nederland

In de eerste helft van 2022 zagen onderzoekers van cybersecuritybedrijven een toename in het gebruik van wiperware, parallel aan de Russische oorlog tegen Oekraïne.[4] Ook later in de rapportageperiode werden nieuwe wiperware-varianten ontdekt.[5][6] Inzet van wipers is echter niet beperkt tot de oorlog. Buiten de oorlog zijn ook verschillende wipers waargenomen. Zo werd bekend dat een geavanceerde cyberactor een nieuwe wiper heeft gebruikt bij aanvallen op de toeleveringsketen van organisaties in onder andere Israël.[7] Ook criminelen lijken wiperfunctionaliteiten toe te voegen aan hun operaties. Een voorbeeld hiervan is de LokiLocker-ransomware. Die heeft een ingebouwde wiperfunctionaliteit die kan worden ingezet om slachtoffers af te persen.[8]

Hoewel in het algemeen de omvang en impact vooralsnog beperkt lijkt, laten enkele uitzonderingen zien dat door de kenmerken van de malware deze categorie bijzonder gevaarlijk is. Deze malware maakt geïnfecteerde computers immers onklaar door alle bestanden te overschrijven en te wissen. Wipers kunnen computers van bedrijven of vitale organisaties platleggen en daarmee maatschappelijke ontwrichting veroorzaken. Doordat dit type malware vaker lijkt voor te komen kan het, mogelijk onbedoeld, op termijn ook in Nederland vaker opduiken.

Cyberaanvallen op energiesector ook in Nederland voorstelbaar

Hoewel bedrijven niet altijd open zijn over het type cyberaanval, laten incidenten zien dat zowel statelijke als criminele actoren aanvallen uitvoerden op de energiesector. Zo werden verschillende energiebedrijven in Europa getroffen door ransomware en kwam naar buiten dat statelijke actoren aanvallen uitvoerden op bedrijven in de olie- en gassector.[9] Ook in Nederland zou de

energiesector geraakt kunnen worden. Indirect is dit zelfs al voorgekomen toen door een ransomware-aanval op de Duitse windmolenfabrikant Nordex meerdere windmolens op Windpark Oude Maas niet konden proefdraaien.

Een geavanceerde statelijke actor die de AIVD attribueert aan een inlichtingen- en/of veiligheidsdienst, is sinds enkele jaren geïnteresseerd in Europese en westerse overheidsinformatie over de energiesector. De activiteiten van de actor betreffen in deze gevallen spionage activiteiten.

Nationale overheden doelwit van ontwrichtende cyberaanvallen

Deze periode hebben zich diverse (ontwrichtende) cyberaanvallen op publieke organisaties en (nationale) overheden voorgedaan. Wereldwijd werden verschillende overheidsinstellingen getroffen door cyberaanvallen. Naast ransomware-aanvallen in Latijns-Amerika, die tot grote verstoringen leidden in onder andere Costa Rica, waren er ook in Europa incidenten met vergaande gevolgen. Montenegro had bijvoorbeeld moeite om zijn overheidsdiensten te herstellen na een aanval met Cuba-ransomware. Albanië haalde een groot deel van zijn overheidswebsites en –diensten offline na een cyberaanval. Albanië en andere NAVO-lidstaten attribueren de aanval aan Iran. Deze en andere incidenten laten zien dat nationale overheden op de radar staan van kwaadwillenden en illustreren de risico's voor de Rijksoverheid.

2022

Maart

- Vertragingen op het spoor door bug in software Alstom
- Persoonsgegevens van klanten woningcorporaties gelekt na ransomware-aanval bij ICT-leverancier
- Duizenden bestanden versleuteld en gelekt na ransomware-aanval op energiebedrijf
- Nederlandse windmolens konden niet proefdraaien door ransomware-aanval
- Spionage op Nederlands defensiebedrijf door Lazarus APT

April

- Persoonsgegevens gelekt na ransomware-aanval op luchthavenbeveiligingsbedrijf
- Bestanden van Gelderse gemeenten Buren en Neder-Betuwe staan op darkweb na ransomware-aanval
- Fysieke sabotage van Franse glasvezelkabels leidde tot regionale internet uitval
- Pegasus-spyware ingezet tegen Catalaanse politici en activisten

September

- Zorg Maastricht UMC+ nagenoeg stilgelegd door ICT-storing
- DigiD urenlang beperkt bereikbaar wegens DDoS-aanvallen
- Gegevens medewerkers Eerste en Tweede Kamer gelekt na ransomware-aanval op leverancier van toegangspassen
- Productiefaciliteiten van Nederlands vaccinbedrijf deels verstoord door ransomware-aanval, gestolen data gelekt op darkweb
- Werking parlement Bosnië en Herzegovina verstoord na cyberaanval

Oktober

- Landelijk politienummer en tiplijnen moeilijk te bereiken door storing
- Tienduizenden medische dossiers en persoonsgegevens gestolen bij digitaal zorgplatform
- IT-systemen Duitse energieleverancier verstoord door cyberaanval

November

- Website Europees Parlement offline na DDoS-aanval pro-Russische hackersgroep Killnet

December

- Gegevens gestolen en kantoorsystemen beperkt toegankelijk na hack op leerwerkbedrijf
- Gegevens tienduizenden klanten van mobiele providers gelekt
- Operationele problemen bij groothandel Makro en moederbedrijf na ransomware-aanval
- Stadsdiensten en burgerzaken gemeente Antwerpen offline na ransomware-aanval bij ICT-partner van gemeente

- *Incident binnenland*
- *Incident buitenland*

Mei

- Door pro-Russische hacktivistische groep XakNet Team gelekte dataset bevat gegevens overheidspersoneel
- Spaanse premier doelwit van Pegasus-spyware
- Nationale noodtoestand in Costa Rica door stilvallen meerdere overheidssystemen na ransomware-aanval

Juni

- Vertrouwelijke documenten en persoonsgegevens gemeente Veenendaal gelekt door menselijke fout van softwareleverancier
- ICT-systemen ARTIS versleuteld door ransomware

Augustus

- Tandartszorg 120 Nederlandse tandartspraktijken enkele dagen stil gelegd door ransomware-aanval
- Vertrouwelijke data vijf Limburgse gemeenten ontoegankelijk door hack bij softwareleverancier
- Persoonsgegevens gelekt na cyberaanval op energie-dienstverlener
- Diensten overheid Montenegro verstoord door ransom-wareaanval

Juli

- Onderbreking van werkzaamheden sociaal domein van gemeente Noordenveld door ransomware-aanval
- Treinverkeer ontregeld door niet-werkend back-up-systeem ProRail
- Poolse officials aangevallen met Pegasus spyware
- Albanië sloot overheidswebsites en –diensten af wegens cyberaanval
- Griekse oppositieleider en Europarlementariër doelwit van Predator-spyware
- Data gestolen en systemen ontoegankelijk gemaakt bij ransomware-aanval op Luxemburgse energiebedrijven

2023

Januari

- Websites verschillende Nederlandse ziekenhuizen tijdelijk onbereikbaar door DDoS-aanvallen

Februari

- Verschillende websites van Nederlandse organisaties doelwit van hacktivistische DDoS-aanval na Koran-verscheuring

2022

Maart 2022

Vertragingen op het spoor door bug in software Alstom: Een bug in de software van het spoorsignaleringssysteem van de Franse leverancier Alstom heeft voor problemen gezorgd op het spoor. De bug leidde tot vertragingen en annuleringen van treinen in onder meer Nederland, Polen, Zweden, Italië, India, Thailand en Peru. De impact in Nederland bleef minimaal.[10]

Persoonsgegevens van klanten woningcorporaties gelekt na ransomware-aanval bij ICT-leverancier: Meerdere Nederlandse woningcorporaties zijn slachtoffer geworden van een datalek nadat hun ICT-leverancier The Sourcing Company (TSC) doelwit werd van een aanval met Conti-ransomware. De aanvallers hebben de servers van TSC versleuteld, data gestolen en deze online gepubliceerd. Onder andere persoonsgegevens van een deel van de huurders zijn hiermee geopenbaard.[11]

Duizenden bestanden versleuteld en gelekt na ransomware-aanval op energiebedrijf: Energiebedrijf NV GEBE Sint-Maarten is slachtoffer geworden van BlackByte-ransomware. Bij de aanval zijn duizenden bestanden versleuteld, gestolen en door de aanvallers op hun leksite gepubliceerd. De aanval heeft impact gehad op de computersystemen van GEBE, maar niet op de levering van stroom, water of andere vitale processen.[12]

Nederlandse windmolens konden niet proefdraaien door ransomware-aanval: Door een ransomware-aanval op de Duitse windmolenfabrikant Nordex konden meerdere windmolens op Windpark Oude Maas niet proefdraaien. Na de aanval heeft de fabrikant zijn ICT-systemen op meerdere locaties uit voorzorg stilgelegd. De aanval heeft geen impact gehad op de hardware die toegang heeft tot de besturing van de windmolens. De aanval is opgeëist door criminelen die achter de Conti-ransomware schuilen.[13]

Spionage op Nederlands defensiebedrijf door Lazarus APT: Onderzoekers van beveiligingsbedrijf ESET stellen dat Lazarus APT [I] een spionage-aanval heeft uitgevoerd op een Nederlands defensiebedrijf. Medewerkers van het bedrijf openden via LinkedIn malware van een persoon die zich voordeed als recruiter bij Amazon. De aanval zou onderdeel zijn van een campagne waarbij Lazarus ook luchtvaart-, ruimtevaart- en defensiebedrijven in andere landen heeft aangevallen.[14]

I Lazarus APT is een digitale actor die zich bezighoudt met digitale spionage, cybercrime, en sabotage. APT staat voor Advanced Persistent Threat. Vaak gebruikt in de betekenis dat een groep geavanceerde middelen kan inzetten om voor langere tijd ongezien te opereren. Vanwege deze reden wordt een APT vaak gelinkt aan (buitenlandse) overheden.

April 2022

Persoonsgegevens gelekt na ransomware-aanval op luchthavenbeveiligingsbedrijf: Luchthavenbeveiligingsbedrijf I-SEC, dat onder andere diensten verleent op Schiphol, is slachtoffer geworden van Conti-ransomware. De buitgemaakte gegevens zijn op de leksite van Conti gepubliceerd. De dataset bevat persoonsgegevens van onder andere (oud-)medewerkers van I-SEC.[15]

Bestanden van Gelderse gemeenten Buren en Neder-Betuwe staan op darkweb na ransomware-aanval: Twee Gelderse gemeenten zijn slachtoffer geworden van een datalek nadat aanvallers met SunCrypt-ransomware bestanden konden stelen. De aanvallers hebben 130GB aan data buitgemaakt en gepubliceerd op de leksite van SunCrypt. Onder andere identiteitsbewijzen behoorden tot de gelekte data. Volgens forensisch onderzoek zijn de aanvallers binnengedrongen door gestolen inloggegevens van een leverancier te misbruiken.[16]

Mei 2022

Door pro-Russische hacktivistische groep XakNet Team gelekte dataset bevat gegevens overheidspersoneel: De pro-Russische hacktivistische groep XakNet Team heeft een dataset bestaande uit duizenden bestanden gelekt via hun publiek toegankelijke Telegram-kanaal. Volgens de MIVD waren in deze dataset communicatie- en persoonsgegevens aanwezig van een groot aantal personen, waaronder enkele Nederlandse overheidsfunctionarissen.

Juni 2022

Vertrouwelijke documenten en persoonsgegevens gemeente Veenendaal gelekt door menselijke fout bij softwareleverancier: Door een technische handeling van een softwareleverancier van de gemeente Veenendaal stonden geheime documenten en documenten met persoonsgegevens per ongeluk tijdelijk online. Vanuit acht IP-adressen zijn documenten uit 2016 ingezien. Na een melding van een oplettende burger heeft de leverancier het lek snel gedicht.[17]

ICT-systemen ARTIS versleuteld door ransomware
Cybercriminelen zijn binnengedrongen op het netwerk van dierentuin ARTIS, waardoor ICT-systemen offline gingen en bezoekers geen online tickets konden aanschaffen. De dierentuin is niet ingegaan op de eis van de hackers om een miljoen euro aan cryptovaluta te betalen. In plaats daarvan heeft de dierentuin de systemen door middel van back-ups weten te herstellen. Volgens de ICT-partners van ARTIS zijn er geen (persoons)gegevens gestolen of ingezien.[18]

Juli 2022

Onderbreking van werkzaamheden sociaal domein van gemeente Noordenveld door ransomware-aanval

De gemeente Noordenveld is getroffen door een ransomware-aanval. Tijdens de aanval is een aantal servers en administratiesystemen versleuteld. De ICT-leverancier van het systeem was in staat om vanuit een back-up data te herstellen, met slechts enkele dagen verlies van productiedata als gevolg. De ransomware-aanval heeft niet geleid tot het verlies van persoonsgegevens of onderbreking van het betalen van uitkeringen.[19]

Treinverkeer ontregeld door niet-werkend back-upsysteem ProRail
Door een ICT-storing in de verkeersleidingspost van ProRail moest treinverkeer rond Rotterdam op 31 juli 2022 enkele uren worden stilgelegd. Door de storing kon de verkeersleiding niet zien waar treinen zich bevonden. In zo'n geval zou ProRail op een back-upsysteem moeten terugvallen, maar vanwege een softwarefout was dit niet mogelijk.[20]

Augustus 2022

Tandartszorg 120 Nederlandse tandartspraktijken enkele dagen stil gelegd door ransomware-aanval: Nederlandse tandartspraktijken van Colosseum Dental zijn meerdere dagen gesloten geweest nadat het bedrijf slachtoffer werd van een ransomware-aanval. Patiënten konden niet behandeld worden omdat hun dossiers door de aanval niet beschikbaar waren. Het bedrijf heeft afspraken met de aanvallers gemaakt over het herstel en het niet-openbaar maken van gegevens.[21]

Vertrouwelijke data vijf Limburgse gemeenten ontoegankelijk door hack bij softwareleverancier: De softwareleverancier van de gemeenten Eijsden-Margraten, Gulpen-Wittem, Kerkrade, Meerssen en Vaals is getroffen door een hack, waardoor data van de gemeenten ontoegankelijk werd. De hackers vielen een administratiesysteem aan waarbij data van onder andere bijstandsuitkeringen, jeugdzorg, de Wet maatschappelijke ondersteuning en energietoeslagen niet door gemeenteambtenaren geopend kon worden.[22]

Persoonsgegevens gelekt na cyberaanval op energiedienstverlener: Energiedienstverlener Ista is het slachtoffer geworden van een cyberaanval. Om schade aan ICT-infrastructuur te voorkomen, haalde het bedrijf alle mogelijk getroffen ICT-systemen offline. De aanvallers hebben de buitgemaakte gegevens van 146.000 mensen op internet gepubliceerd. Onder de gepubliceerde gegevens bevonden zich adresgegevens van klanten, namen en informatie over energie- en waterverbruik. Volgens het bedrijf zitten hier geen persoonsgegevens van Nederlanders tussen. Desalniettemin hebben verschillende woningcorporaties potentiële datalekken gemeld.[23]

September 2022

Zorg Maastricht UMC+ nagenoeg stilgelegd door ICT-storing: Een ICT-storing bij ziekenhuis Maastricht UMC+ heeft ervoor gezorgd dat nagenoeg alle zorg in het ziekenhuis stil is komen te vallen. Door de technische storing was het ziekenhuis onbereikbaar en was toegang tot het elektronisch patiëntendossier-systeem niet mogelijk. Sommige patiënten die ten tijde van de storing naar het ziekenhuis kwamen, werden weer naar huis gestuurd. Acute behandelingen gingen wel door.[24]

DigiD urenlang beperkt bereikbaar wegens DDoS-aanvallen: DigiD is op 12 september 2022 doelwit geworden van een DDoS-aanval. Hierdoor was de dienst urenlang slecht bereikbaar en konden burgers soms niet inloggen. Het is niet duidelijk wie er verantwoordelijk is voor de aanval.[25]

Gegevens medewerkers Eerste en Tweede Kamer gelekt na ransomware-aanval op leverancier van toegangspassen: ID-ware, een grote leverancier voor toepassingen rondom authenticatie en toegangspassen, is slachtoffer geworden van ALPHV/BlackCat-ransomware. De aanvallers hebben gegevens buitgemaakt van klanten van ID-ware en deze gepubliceerd op een leksite. In de dataset bevonden zich onder andere toegangspassen van leden en medewerkers van de Eerste en Tweede Kamer. Daarnaast zijn persoonsgegevens en toegangspassen gelekt van verschillende Nederlandse onderwijsinstellingen, overheidsorganisaties en bedrijven.[26]

Productiefaciliteiten van Nederlands vaccinbedrijf deels verstoord door ransomware-aanval, gestolen data gelekt op darkweb: Het Nederlandse vaccinbedrijf Bilthoven Biologicals is getroffen door ALPHV/BlackCat-ransomware. De aanvallers wisten productiefaciliteiten, zoals machines voor het produceren van vaccins, te raken. De machines hebben tijdens de aanval grotendeels door kunnen draaien. Daarnaast zouden de aanvallers e-mails en documenten met wetenschappelijke data, zoals informatie over vaccins, hebben gestolen. Deze gestolen data is (deels) gepubliceerd op het darkweb.[27]

Oktober 2022

Landelijk politienummer en tiplijnen moeilijk te bereiken door storing: Door een technische storing waren het politienummer 0900-8844, de opsporingstiplijn en Meldpunt 144 op 18 oktober 2022 enkele uren moeilijk tot niet bereikbaar. Het probleem speelde zich af in het hele land. Alarmnummer 112 werkte ten tijde van de storing wel naar behoren.[28]

Tienduizenden medische dossiers en persoonsgegevens gestolen bij digitaal zorgplatform
Via een kwetsbaarheid in het digitale zorgplatform Carenzorgt heeft een aanvaller ingebroken en privacygevoelige gegevens gestolen. Diverse Nederlandse zorginstellingen hebben daarom bij de Autoriteit Persoonsgegevens melding gemaakt van een datalek. Ongeveer negenduizend zorgaanbieders en bijna een half miljoen mensen maken gebruik van de digitale gezondheidsomgeving Carenzorgt.[29]

December 2022

Gegevens gestolen en kantoorsystemen beperkt toegankelijk na hack op leerwerkbedrijf
Door een hack op leerwerkbedrijf Pantar, het grootste sociaal ontwikkelbedrijf in de regio Amsterdam-Diemen, zijn kantoorsystemen niet of beperkt toegankelijk gemaakt. Uit voorzorg schakelde het bedrijf ook een groot aantal systemen uit. De aanvallers hebben volgens het bedrijf gegevens buitgemaakt, maar er zouden geen klantgegevens zijn gestolen.[30]

Gegevens tienduizenden klanten van mobiele providers gelekt
Enkele tienduizenden klanten van Caiway Mobiel en Delta Mobiel zijn slachtoffer geworden van een datalek. Een aanvaller wist toegang te krijgen tot de bestelomgeving voor mobiele abonnementen en kon daarop namen, adressen, e-mailadressen, geboortedata, telefoon- en bankrekeningnummers van klanten downloaden. Volgens de providers zijn inloggegevens zoals wachtwoorden en creditcardgegevens niet buitgemaakt.[31]

Operationele problemen bij groothandel Makro en moederbedrijf na ransomware-aanval
Metro, het moederbedrijf van groothandel Makro, heeft problemen ondervonden tijdens herstelwerkzaamheden na een ransomware-besmetting. Tijdens de herstelwerkzaamheden heeft Metro nieuwe kwaadaardige bestanden aangetroffen, waarna het bedrijf zijn ICT-systemen uitschakelde. Hierdoor vielen ook een aantal operaties van dochteronderneming Makro stil. De aanval zorgde onder andere voor problemen met de verspreiding van reclamefolders vanuit de zeventien vestigingen in Nederland. De criminelen hebben bij de aanval ook persoonsgegevens van medewerkers van Metro buitgemaakt.[32]

2023

Januari 2023

Websites verschillende Nederlandse ziekenhuizen tijdelijk onbereikbaar door DDoS-aanvallen: In het laatste weekend van januari kampten verschillende ziekenhuizen, waaronder het UMCG, LUMC en het MUMC+, met DDoS-aanvallen waardoor websites tijdelijk onbereikbaar waren.[33] [34] Hierbij viel de aanval op het UMCG het meest op omdat een aantal websites van het ziekenhuis meerdere dagen offline was. De bedrijfsvoering van het ziekenhuis ondervond geen hinder en het patiëntenportaal bleef beschikbaar. [35] De aanvallen werden geclaimd door de pro-Russische hacktivisten van Killnet, nadat zij eerder (onder andere) Nederlandse ziekenhuizen op een lijst hadden geplaatst met de oproep deze aan te vallen vanwege de Nederlandse steun aan Oekraïne.[36]

Februari 2023

Verschillende websites van Nederlandse organisaties doelwit van hacktivistische DDoS-aanval na Koran-verscheuring: Een aantal Nederlandse overheidsorganisaties en bedrijven is doelwit geworden van hacktivistische DDoS-aanvallen op hun websites. Onder andere de groepen 'Mysterious Team Bangladesh' en 'Turk Hack Team' claimden bij de aanvallen betrokken te zijn geweest. De aanvallen zouden een reactie zijn geweest op de Koran-verscheuring in Den Haag eind januari. De aanvallen zouden onderdeel zijn geweest van de campagnes #OpHolland en #OpSweden.[37]

Opvallende incidenten in buitenland

April 2022

Fysieke sabotage van Franse glasvezelkabels leidde tot regionale internet uitval[38]

Pegasus-spyware ingezet tegen Catalaanse politici en activisten[39]

Mei 2022

Spaanse premier doelwit van Pegasus-spyware[40]

Nationale noodtoestand in Costa Rica door stilvallen meerdere overheidssystemen na ransomware-aanval[41]

Juli 2022

Poolse officials aangevallen met Pegasus spyware[42]

Albanië sloot overheidswebsites en –diensten af wegens cyberaanval[43]

Griekse oppositieleider en Europarlementariër doelwit van Predator-spyware.[44]

Data gestolen en systemen ontoegankelijk gemaakt bij ransomware-aanval op Luxemburgse energiebedrijven[45]

Augustus 2022

Diensten overheid Montenegro verstoord door ransomware-aanval[46]

September 2022

Werking parlement Bosnië en Herzegovina verstoord na cyberaanval [47]

Oktober 2022

IT-systemen Duitse energieleverancier verstoord door cyberaanval[48]

November 2022

Website Europees Parlement offline na DDoS-aanval pro-Russische hackersgroep Killnet[49]

December 2022

Stadsdiensten en burgerzaken gemeente Antwerpen offline na ransomware-aanval bij ICT-partner van gemeente[50]

Ruim een jaar na de start van de oorlog in Oekraïne blijkt de impact van cyberaanvallen kleiner te zijn dan verwacht. Dat wil niet zeggen dat cyberaanvallen geen belangrijke rol spelen.

3 Russische oorlog tegen Oekraïne: omvangrijke cyber-campagne, minder impact dan verwacht

Ruim een jaar na de start van de oorlog van Rusland tegen Oekraïne zijn Russische cyberaanvallen vooral gericht geweest op Oekraïne en de nabije regio. Het betrof spionage en (voorbereidingshandelingen voor) sabotage. Ook verspreidt Rusland desinformatie. Ontwrichtende cyberaanvallen die de nationale veiligheid van Nederland schaden, hebben zich (nog) niet voorgedaan. Bij verdere escalatie van de oorlog kan de digitale dreiging abrupt veranderen. Cyberaanvallen kunnen dan de nationale veiligheid gaan aantasten. Ook kan Nederland worden geraakt door keteneffecten die doorwerken naar vitale processen en te maken (blijven) krijgen met aanvallen van pro-Russische criminelen en hacktivisten.

Niet de verwachte cyberoorlog, wel cyberaanvallen

Cyberaanvallen hebben (nog) niet het ontwrichtende en doorslaggevende effect gehad dat werd verwacht, maar hebben wel een ondersteunende rol gehad in bijvoorbeeld het verstoren van de communicatie aan Oekraïense zijde of het (proberen te) ontvreemden van informatie over (internationale) besluitvorming. Bij de start van de Russische oorlog tegen Oekraïne ging men ervan uit dat er voor het eerst een oorlog zou plaatsvinden met een beslissende rol voor cyberaanvallen. Een belangrijke reden hiervoor was dat een land met geavanceerde cybercapaciteiten een oorlog startte tegen een sterk gedigitaliseerd land.[51] Ook is in het verleden gebleken dat Rusland over zowel de capaciteiten als de intentie beschikt om ontwrichtende aanvallen uit te voeren tegen Oekraïne.[52] Daarnaast bestond de vrees dat aanvallen op Oekraïne ook over konden slaan naar andere landen, of dat landen die steun zouden betuigen aan Oekraïne als vergelding konden rekenen op cyberaanvallen door Rusland.

Omvangrijke offensieve campagne, maar beperkte impact mede dankzij hulp aan en hoge weerbaarheid van Oekraïne

Een jaar na de start van de oorlog blijkt de impact van cyberaanvallen kleiner te zijn dan verwacht. Dat wil niet zeggen dat cyberaanvallen geen belangrijke rol spelen.

De vele honderden aanvallen op beide zijden laten zien dat er sprake is van een zeer indrukwekkende en volhardende campagne.[53] Een volledig beeld over de omvang en impact van aanvallen ontbreekt echter. Dit komt bijvoorbeeld door oorlogsgeweld ter plaatse, wat een inschatting bemoeilijkt. Daarnaast kunnen slachtoffers bewust zaken onbenoemd laten. Binnen de context van de oorlog vallen de aanvallen eerder mee dan tegen, maar buiten die context is sprake van een omvangrijke offensieve campagne van cyberaanvallen. De Russische cybersabotagecampagne tegen Oekraïne is zelfs de meest grootschalige en intensieve uit de geschiedenis.[54]

In open bronnen zijn diverse voorbeelden bekend geworden van Russische cybersabotagepogingen tegen Oekraïense vitale infrastructuur, onder meer de stroomvoorziening. De MIVD heeft inlichtingen over nog veel meer van dergelijke aanvalspogingen tegen vitale infrastructuur die (nog) niet openbaar bekend zijn geworden. Russische statelijke actoren hebben een sterke intentie en ontplooien een hoog niveau van activiteiten op het gebied van cybersabotage.

Grootschalige en langdurige ontwrichting als gevolg van cyberaanvallen is tot nu toe echter uitgebleven, en de gevolgen van cybersabotage vallen in het niet bij de impact van fysieke militaire operaties.[55] De relatief beperkte impact van Russische cyberaanvallen in het algemeen is onder andere te danken aan de hoge weerbaarheid van Oekraïne.[56] Private bedrijven speelden een grote rol in het verhogen van die weerbaarheid, bijvoorbeeld door het aanbieden van diensten aan en het delen van dreigingsinformatie met Oekraïne. Ook krijgt Oekraïne significante hulp van westerse inlichtingendiensten.[57] Daarnaast is gedurende de oorlog gebleken dat Rusland moeite heeft om cyberoperaties te synchroniseren met andere militaire operaties, zoals luchtaanvallen.[58] Het succes van de Oekraïense digitale verdediging is echter niet gegarandeerd. Waarschijnlijk kan dit succes alleen volgehouden worden zolang de westerse steun net zo intensief en adaptief blijft als de cyberoperaties van de Russische inlichtingendiensten.[59]

Vele wiperware-aanvallen op Oekraïne, ook op vitale infrastructuur

Oekraïne en de nabije regio staan ontegenzeggelijk in de aandacht van Rusland. De Oekraïense digitale infrastructuur wordt vrijwel constant aangevallen.[60] Russische hackers hebben vele verschillende types wiperware ingezet tegen Oekraïense doelwitten, ook binnen vitale sectoren (zie ook hoofdstuk 2).[61] Een bekend voorbeeld is de aanval op het Amerikaanse satellietbedrijf Viasat. Deze aanval vond enkele uren voor de invasie plaats en verstoorde, dankzij het wissen van grote hoeveelheden data, tijdelijk de communicatie aan Oekraïense zijde.[62] Ook werd in maart 2022 een van de grootste internetproviders in Oekraïne gehackt. Dit leidde ongeveer een dag lang tot uitval van het internet in grote delen van het land.[63]

Andere actoren liften mee op thema oorlog

Naast Rusland hebben ook andere statelijke actoren cyberaanvallen ingezet in relatie tot de oorlog. Zo lijken statelijke actoren, die niet direct betrokken zijn (geweest) bij de oorlog, opportunistisch te hebben gehandeld en meegelift op het thema van de oorlog. Bijvoorbeeld door bij de verspreiding van malware gebruik te maken van phishing. Hierbij zijn vaak bewoordingen gebruikt in titels of beschrijvingen die met de oorlog te maken hebben. Op die manier worden slachtoffers makkelijker verleid om ergens op te klikken of bestanden te openen.[64] Statelijke actoren, anders dan Rusland, hebben voornamelijk geprobeerd om toegang te krijgen tot bepaalde systemen. Het is aannemelijk dat dit als doel (economische) spionage had.[65] Daarnaast is ook spionage door in ieder geval één ander land waargenomen op (pro-)Oekraïense doelwitten, om informatie over de oorlog te bemachtigen.[66]

In algemene zin wordt de digitale ruimte door statelijke actoren gebruikt om geopolitiek voordeel te behalen. Bredere geopolitieke ontwikkelingen worden vaker gebruikt om slachtoffers te verleiden kwaadaardige links of bestanden te openen. Het inspelen op geopolitieke ontwikkelingen zoals de oorlog is dan ook niet onverwacht.

Cybercriminelen kiezen partij

Kort nadat de invasie van Oekraïne begon, verschenen berichten van cybercriminele groepen waarin zij hun steun uitspraken voor Russische of Oekraïense zijde. Zo verklaarde de criminele Contigroep zijn steun aan Rusland, en gaf aan dat cyberaanvallen op Russische doelwitten zouden worden beantwoord met aanvallen op kritieke infrastructuur.[67] [68] Dat onderschrijft de notie dat criminelen bepaalde doelwitten bewust uitkiezen omdat die in lijn zijn met geopolitieke belangen van bepaalde staten, of dat er zelfs banden kunnen bestaan tussen overheden en cybercriminelen.[69] Statelijke actoren kunnen namelijk cybercriminelen inhuren, gedogen of onder druk zetten om cyberaanvallen op gewenste doelwitten uit te voeren.[70] Daarnaast kunnen andere partijen, zoals statelijke actoren, zich ook voordoen als criminele organisaties.[71] Hierdoor wordt de scheidslijn tussen financieel gemotiveerde cybercriminelen en statelijke actoren vager en lastiger te onderscheiden. Dat compliceert attributie. Specifiek voor cybercriminele groepen uit Rusland geldt dat zij opereren in een vrijer speelveld. Vanwege de vele sancties is het namelijk aannemelijk dat de Russische autoriteiten minder snel geneigd zullen zijn om cybercriminelen die westerse belangen aanvallen te hinderen.

Hacktivisme terug van weggeweest

Ook hacktivisten kwamen tijdens de oorlog in actie terwijl die de afgelopen jaren relatief weinig cyberaanvallen ondernamen.[72] Zo maakte Anonymous bekend zich tegen Rusland te keren. Daarna zijn verschillende cyberaanvallen door het collectief opgeëist, zoals DDoS-aanvallen op Russische overheidswebsites, het hacken van een Belarussische wapenleverancier, en het uitvoeren van defacements op Russische televisiekanalen. Een ander bekend voorbeeld van hacktivistische inspanningen is het pro-Oekraïense IT-Army. De Oekraïense minister van Digitale Transformatie deed een oproep aan hackers wereldwijd om het IT-Army te helpen met het uitvoeren van bijvoorbeeld DDoS-aanvallen op Russische doelwitten.[73] [74] En al tijdens de troepenopbouw in Belarus voorafgaand aan de invasie, claimden pro-Oekraïense hacktivisten dat zij het systeem van het Belarussische treinnetwerk hadden gecompromitteerd. Zij dreigden treinen te ontregelen die Russische troepen en materieel vervoerden.[75] Ook pro-Russische hacktivisten hebben van zich laten horen. Zo riep de hacktivistische groepering Killnet op tot het bestoken van Europese ziekenhuizen met DDoS-aanvallen, waaronder enkele in Nederland (zie Jaarbeeld).

Bij hacktivisme is wel een aantal kanttekeningen te plaatsen. De meetbare impact van hacktivistische activiteiten is veelal kortdurend en relatief beperkt. Wel kunnen psychologische effecten op de bevolking en de autoriteiten tot de gevolgen behoren. Ook moet worden opgemerkt dat hacktivistische groepen over het algemeen losjes georganiseerd zijn en dat duidelijk leiderschap veelal ontbreekt. Zo is deelname over het algemeen vrijwillig en volgen deelnemers geen gestructureerd plan, vindt de communicatie vaak plaats via kanalen als Telegram, en zijn de cybermiddelen die worden ingezet relatief eenvoudig en laagdrempelig.[76] Desalniettemin zijn er ook aanwijzingen dat statelijke actoren zich vermengen met hacktivisten, of onder de vlag van hacktivisme opereren.[77] [78] Dit maakt attributie van hacktivistische aanvallen lastig. Het gevaar is dat de activiteiten van hacktivisten verkeerd geïnterpreteerd worden door landen die het slachtoffer worden van hun aanvallen, wat tot tegenreacties kan leiden.[79]

Private bedrijven ondersteunen Oekraïne voor digitale weerbaarheid

Een kenmerkend element in het verloop van de oorlog is dat private bedrijven steun aan Oekraïne verlenen, vaak in samenwerking met landen die steun bieden aan Oekraïne. Dit wordt veelal gedaan door de weerbaarheid van (Oekraïense) organisaties te verhogen en vitale diensten toegankelijk te houden.[80] Zo bleek Microsoft maanden voor de invasie al actief patches te creëren voor malware die gericht was op Oekraïne, en dreigingsinformatie te delen met de Oekraïense autoriteiten. Verder boden Amazon en Microsoft de Oekraïense overheid de mogelijkheid om overheidsdata over te zetten naar de cloud en de veiligheid daarvan te waarborgen.[81] Daarnaast werd het satellietnetwerk Starlink van SpaceX geactiveerd boven Oekraïne.[82] Hierdoor was er weer toegang tot internet in gebieden waar de internetinfrastructuur beschadigd was geraakt door Russische fysieke en digitale aanvallen.[83] [84] Behalve private bedrijven bieden ook westerse inlichtingendiensten significante hulp bij het vergroten van de weerbaarheid, bijvoorbeeld door te assisteren in monitoring-, detectie- en responsmaatregelen.[85]

Rusland poogt publieke opinie te beïnvloeden met desinformatie

Informatieconfrontatie, waaronder beïnvloeding door misleiding, desinformatie, en cyberoperaties, speelt een centrale rol in de Russische wijze van optreden. Dit wordt voor een belangrijk deel uitgevoerd via digitale middelen om onder meer psychologische schade te veroorzaken.[86] Hierbij wordt gepoogd om de Oekraïense inspanningen te ondermijnen, de steun voor de oorlog binnen Rusland te vergroten, en de internationale publieke opinie te vormen.[87] De Russische inlichtingendiensten zijn er bijvoorbeeld enkele malen in geslaagd om de controle over uitzendingen van Oekraïense media tijdelijk over te nemen en Russische boodschappen uit te zenden. Aansluitend werden de systemen van deze media digitaal gesaboteerd.[88] Daarnaast hebben Russische staatsmedia consequent desinformatie naar buiten gebracht.[89] [90] Desinformatie wordt al lange tijd door Rusland ingezet, ook voor de oorlog. Hoewel Moskou zijn pijlen daarbij niet specifiek op Nederland richt, heeft Moskou sinds de invasie verregaande pogingen gedaan om het westerse publieke debat over de oorlog en het politiek-bestuurlijke bestel heimelijk te beïnvloeden.[91]

Russische focus ook op Nederland, tot dusver geen ontwrichtende impact

Russische spionagepogingen waargenomen in Nederland en vitale infrastructuur wordt heimelijk in kaart gebracht

Vooralsnog hebben aanvallen gerelateerd aan de oorlog niet geleid tot grote verstoringen of impact op de nationale veiligheid in Nederland. Echter zijn er in de context van de oorlog wel cyberaanvallen uitgevoerd waarbij Nederland, NAVO-lidstaten, en/of 'het westen' in het algemeen een doelwit zijn geweest van Rusland.

Veruit het grootste deel van Russische cyberoperaties is gericht op spionage om militaire, diplomatieke en economische informatie van zowel Oekraïne als NAVO-lidstaten te bemachtigen.[92] Het ligt voor de hand dat de inlichtingenbehoefte van Rusland is gegroeid tijdens en door de oorlog tegen Oekraïne. Enerzijds omdat het zeer waardevol kan zijn om informatie in te winnen over bijvoorbeeld mogelijke besluitvorming, militaire ondersteuning of aanwezigheid en/of transport van wapens. Anderzijds omdat 'reguliere' kanalen grotendeels wegvielen tijdens de oorlog door bijvoorbeeld sancties en het uitwijzen van diplomaten.[93] [94] Deze (pogingen tot)

spionage nemen verschillende vormen aan. Rusland probeert er door spionage onder meer achter te komen hoe de NAVO en de EU besluiten nemen, en vervolgens hoe het die besluitvorming kan ondermijnen.[95] Verder richt de Russische inlichtingenbehoefte zich onder meer op militaire steun die via NAVO-lidstaten aan Oekraïne geleverd wordt. Ook de Nederlandse krijgsmacht, ministeries en ambassades zijn afgelopen jaar doelwit geweest van (onsuccesvolle) cyberspionagepogingen. Daarnaast hebben Russische cyberspionnen routers gehackt van Nederlandse particulieren en het midden- en kleinbedrijf. Deze operatie is zorgelijk, omdat Rusland deze gehackte routers kan misbruiken om heimelijke cyberoperaties tegen Nederlandse belangen of die van bondgenoten uit te voeren.[96] Verder kan sprake zijn van economische spionage, bijvoorbeeld om de negatieve effecten van sancties te verminderen en/of om aan noodzakelijke kennis te komen.

De AIVD en MIVD zien verder dat Rusland delen van de Nederlandse vitale infrastructuur heimelijk in kaart brengt. Zo kunnen onder andere Nederlandse internetkabels doelwit zijn voor sabotage.[97] Hoewel het hier gaat om fysieke componenten zoals kabels, kan sabotage daarvan doorwerken in het digitale domein. Dat kan leiden tot verstoring of zelfs ontwrichting in Nederland. Ook valt niet uit te sluiten dat de fysieke handelingen onderdeel zijn of worden van een digitale sabotagecampagne.

Focus van Rusland waarschijnlijk op Oekraïne en omgeving

Het is aannemelijk dat geavanceerde Russische cyberaanvallen zich voornamelijk op Oekraïne en de nabije regio zullen blijven richten. Maatschappij ontwrichtende cyberaanvallen kosten doorgaans veel capaciteit; het creëren van malware, verkennen van systemen, innestelen, en vervolgens uitrollen van malware kan vele maanden in beslag nemen. Ook kan een actor als Rusland dergelijke capaciteit niet overal tegelijkertijd inzetten, en moet het keuzes maken omtrent doelwitselectie. Nederlandse organisaties kunnen wel door ketenafhankelijkheden geraakt worden als gevolg van aanvallen in relatie tot de Russische oorlog tegen Oekraïne. Eerdere aanvallen door Russische actoren hebben geleid tot nevenschade.

Nederlandse nationale veiligheid tot dusver niet geraakt als gevolg van cyberaanvallen, maar dat valt niet uit te sluiten

De kans op gerichte aanvallen op Nederlandse belangen schat het NCSC in als mogelijk.[98] Hoewel tot dusver niet geraakt, valt niet uit te sluiten dat cyberaanvallen als gevolg van de oorlog in Oekraïne de nationale veiligheid gaan raken. Zoals beschreven in eerdere CSBN's en de voorgaande paragraaf, hebben Russische actoren spionageactiviteiten ontplooid en worden delen van de Nederlandse vitale infrastructuur heimelijk in kaart gebracht. Rusland heeft al jaren een offensief cyberprogramma tegen onder andere Nederland. De almaar verslechterende relatie met Rusland en de geopolitieke isolatie waarin het land zich bevindt, kan er verder toe bijdragen dat cyberaanvallen tegen Nederland toenemen of dat meer geavanceerde aanvallen plaatsvinden.

Er moet rekening mee worden gehouden dat een cyberaanval in Oekraïne of de regio gevolgen kan hebben voor Nederland of andere westerse landen, bijvoorbeeld door keteneffecten binnen digitale ecosystemen (zie voor verder toelichting op keteneffecten en digitale ecosystemen hoofdstuk 5). Ook kan een cyberaanval die niet wordt uitgevoerd met een onderliggende intentie van ontwrichting, daar wel toe leiden. Op die manieren kan een cyberaanval toch significante impact hebben, of zelfs de nationale veiligheid raken.

Indien hackers cyberaanvallen vanuit of via Nederland uitvoeren op buitenlandse doelwitten, kan Nederland ook getroffen worden door een tegenreactie. Ook Nederlandse ingezetenen kunnen deelnemen aan acties van hacktivisten en zo betrokken raken bij de oorlog of andere conflicten. Die betrokkenheid kan onvoorziene consequenties hebben en is bovendien strafbaar.[99]

Al met al kan worden gesteld dat wat betreft cyberaanvallen in de context van de Russische oorlog tegen Oekraïne met het onverwachte rekening moet worden gehouden. Russische cyberaanvallen met een ontwrichtende impact mogen dan nog niet zijn voorgekomen, maar dat is niet uit te sluiten in de toekomst. Zo kan de dreiging abrupt veranderen als gevolg van een verdere escalatie van de oorlog.

In ons dagelijks leven betalen we voornamelijk met de betaalpas. We hebben minder vaak contant geld in onze portemonnee. Een landelijke pinstoring leidt daarom tot ongemak en onrust.

4 Operationele Technologie: kwetsbare bouwsteen voor vitale processen

Operationele technologie (OT), binnen industriële netwerken ook wel aangeduid als Industrial Automation and Control Systems (IACS), speelt een centrale rol in het aansturen, monitoren en beheren van fysieke processen binnen (vitale) organisaties. Grootschalige uitval en problemen in de beschikbaarheid van deze systemen kunnen grote maatschappelijke gevolgen hebben. Gebleken is dat cyberactoren geïnteresseerd zijn in het compromitteren van OT. Het beheersen van risico's hieromtrent vereist specifieke kennis, competenties en samenwerking. Ondanks groeiende aandacht voor de weerbaarheid van OT-systemen, is er ruimte voor verbetering. Het is zaak hier verder op in te zetten om de weerbaarheid van vitale processen te waarborgen.

Sleutelbegrippen

Operationele technologie (OT): verzamelnaam voor digitale systemen (hardware en software) die een fysiek proces in werking stellen, monitoren en beheren. Voorbeelden hiervan zijn IACS, toegangssystemen of gebouwautomatiseringssystemen. Waar binnen IT de prioriteit ligt bij vertrouwelijkheid en integriteit van data en in mindere mate bij beschikbaarheid, is dat voor OT precies andersom vanwege de mogelijke fysieke gevolgen van verstoring of uitval.

Industrial Automation and Control Systems (IACS): vormen een onderdeel van OT en worden gebruikt voor het aansturen, automatiseren en monitoren van fysieke processen in de industrie, waaronder in veel vitale sectoren. Onder IACS vallen verschillende monitorings- en besturingssystemen, zoals Supervisory Control and Data Acquisition systemen (SCADA) en Programmable Logic Controllers (PLC)**.** Ook worden er binnen IACS verschillende industriële communicatieprotocollen gebruikt.

Industrial Internet of Things (IIoT): toepassing van het Internet of Things (IoT) in industriële omgevingen voor (onder andere) procesoptimalisatie en diagnostiek, waardoor systemen worden geïntegreerd en (in)direct verbonden kunnen worden met het internet.

Veiligheid OT van vitaal belang, maar kent belangrijke uitdagingen

In vergelijking met reguliere informatietechnologie (IT) wordt er in het publieke debat relatief weinig aandacht besteed aan de veiligheid van OT en de uitdagingen hieromtrent. Dit komt enerzijds doordat in het nieuws vooral aandacht is voor in het oog springende digitale inbreuk op reguliere IT-systemen zoals websites, servers en werkplekken. Anderzijds hebben er, voor zover bekend, relatief weinig verstorende inbreuken op OT plaatsgevonden. OT-systemen vormen echter het fundament van belangrijke fysieke processen, zoals de productie en verwerking van grondstoffen, het zuiveren van drinkwater, de bediening van sluizen en distributie van elektriciteit. Daarmee is de veiligheid van deze systemen van fundamenteel belang voor de Nederlandse maatschappij en economie.

Impact cyberincidenten potentieel groot

Vanwege de belangrijke rol van OT, kunnen grootschalige uitval en problemen omtrent de beschikbaarheid van OT-systemen grote maatschappelijke gevolgen hebben.[100] Incidenten kunnen leiden tot maatschappelijke onrust, economische schade, en verlies aan vertrouwen in digitalisering.[101] Waar incidenten in een IT-omgeving vaak leiden tot reputatie- of financiële schade, kan er bij incidenten in OT-omgevingen ook schade aan industriële apparatuur en de nabije omgeving ontstaan. In uiterste gevallen is het mogelijk dat er slachtoffers vallen.[102]

De kans dat een incident zich voordoet en de impact hiervan zijn sterk afhankelijk van het type compromittatie, de mate van weerbaarheid van de getroffen organisatie en de sector waarin het incident zich voordoet. Ook kunnen er keteneffecten optreden. Dat OT-systemen ook kwetsbaar zijn voor digitale aanvallen is de afgelopen jaren meerdere keren gebleken, met in sommige gevallen grote impact voor de getroffen organisaties en hun omgeving.[II]

Weerbaarheid OT-systemen is een complex vraagstuk

De digitale beveiliging van OT kent een aantal belangrijke uitdagingen.[103] OT-systemen hebben een langere levensduur en de kosten om deze te vervangen zijn vaak hoog. Informatie rondom kwetsbaarheden is vaak diffuus. In veel gevallen ontbreekt concreet handelingsperspectief vanuit leveranciers om de kwetsbaarheden te verhelpen of misbruik hiervan te voorkomen.[104] [105] Verder is het in de praktijk lastig om OT-systemen bij te werken naar nieuwe software versies, omdat dit de beschikbaarheid en interoperabiliteit van OT-systemen kan verstoren. Bovendien zijn representatieve testomgevingen, om patches te testen voordat ze worden uitgerold, vaak duur en complex om te ontwikkelen. Dit alles heeft tot gevolg dat veel processen afhankelijk zijn van verouderde en kwetsbare software. Daar komt bij dat veel systemen in OT-netwerken van oudsher insecure-by-design zijn.[III] Het belang van operationele efficiëntie en het snel kunnen inspelen op onveilige situaties weegt hierin zwaarder dan bijvoorbeeld authenticatie van de gebruiker.[106] [107] De ervaring leert echter dat in netwerken zonder adequate interne controles er een grotere kans op incidenten is. Bovendien is de schade vaak groter en moeilijker te herstellen. Dit geldt ook voor OT-netwerken waar aanvallers met de juiste kennis misbruik kunnen maken van standaard functionaliteiten om een aanval uit te voeren, mogelijk zonder dat hier een kwetsbaarheid aan te pas komt.[108]

Dreiging door groter aanvalsoppervlak en interesse cyberactoren

Het feit dat OT-netwerken van oudsher insecure-by-design zijn, is in toenemende mate problematisch omdat de afgelopen jaren OT steeds meer verweven is geraakt met IT. Toenemende integratie, ook wel IT/OT convergentie genoemd, heeft als doel de zichtbaarheid, efficiëntie en snelheid van operationele processen te verbeteren.[109] Dit biedt aanvallers echter ook meer mogelijkheden om via gecompromitteerde IT-systemen toegang te verkrijgen tot een OT-netwerk.[110] Dit wordt versterkt door de opkomst van het Industrial Internet of Things (IIoT).[111] Ook dit vergroot het aanvalsoppervlak en biedt aanvallers meer mogelijkheden om operationele systemen te compromitteren.[112]

Nieuwe malware ook voor Nederland relevant

Hoe actueel de mogelijkheid tot het compromitteren van operationele systemen is, blijkt onder andere uit de ontdekking van twee nieuwe malware-soorten vorig jaar. Deze malware-soorten blijken gebruikt te kunnen worden voor de sabotage van OT-systemen.[IV] De eerste, Industroyer2, is ingezet tegen een Oekraïense energieleverancier, maar kon tijdig worden geneutraliseerd. ESET en de Oekraïense CERT attribueren Industroyer2 aan de Russische statelijke actor Sandworm.[113] [114] Industroyer2 is de eerste

II Bekende voorbeelden zijn onder andere digitale sabotage van operationele systemen van elektriciteitscentrales in Oekraïne in 2015 en 2016 middels BlackEnergy en Industroyer-malware, alsmede een digitale aanval op een petrochemische fabriek in Saudi-Arabië in 2017, waarbij gebruik werd gemaakt van malware die bekend staat als Triton/TRISIS die zich specifiek richt op veiligheidssystemen. Ook lukte het een aanvaller begin 2021 toegang te krijgen tot de operationele systemen van een drinkwaterbedrijf in Oldsmar (VS) waarmee de toevoer van chemicaliën aan het drinkwater wordt beheerd.

III Anders dan in IT-netwerken wordt er in OT-netwerken minder gebruik gemaakt van authenticatie en autorisatie-methoden om toegang tot systemen te beheren. De veronderstelling hierbij is dat dit kan omdat OT-omgevingen van oudsher gescheiden zijn van andere (IT-)netwerken en dat er in principe uitgegaan kan worden van legitiem netwerkverkeer.

IV Deze twee komen bovenop vijf reeds bekende OT-specifieke malware-soorten, te weten: Stuxnet, HAVEX, BlackEnergy2, Industroyer/Crashoverride en Triton/TRISIS.

OT-malware die voortbouwt op een eerdere variant.[115] De tweede malware-soort, bekend als PIPEDREAM/INCONTROLLER, geeft een aanvaller meerdere opties bij een digitale aanval en slaat onder andere een brug tussen IT- en OT-omgevingen.[116] Volgens Mandiant is PIPEDREAM/INCONTROLLER vermoedelijk ontwikkeld door een statelijke actor, maar werd het ontdekt door onderzoekers voordat deze kon worden ingezet.[117] Opvallend is dat beide malware-soorten breder inzetbaar zijn en ook ingezet kunnen worden buiten het initiële doelwit.

Dergelijke ontwikkelingen zijn ook relevant voor Nederland. Bekend is dat statelijke actoren zich onder andere richten op voorbereidingshandelingen voor sabotage tegen vitale en andere cruciale infrastructuur.[118] Naast sabotage kan het verkrijgen van inzicht in industriële processen door spionage ook een belangrijk motief zijn van statelijke actoren.[V] Voor industriële omgevingen kan een verkennende handeling al leiden tot verstoringen en is dit alleen daarom al zeer ongewenst.

Toenemende interesse door ransomware-actoren in OT-systemen niet uitgesloten

Ransomware-actoren vormen eveneens een risico voor de continuïteit van operationele systemen en fysieke processen. In juli 2022 is bijvoorbeeld een nieuwe ransomware-variant ontdekt, genaamd Luna.[119] Deze variant bevat een lijst met OT-processen die, indien aanwezig, beëindigd worden alvorens over wordt gegaan tot versleuteling. Een dergelijke lijst wordt ook wel een kill-list genoemd. Het gebruik van een kill-list werd eerder al gesignaleerd bij ransomware-varianten zoals EKANS, MegaCortex en LockerGoga.[120] Kill-lists zijn niet per definitie het resultaat van een gerichte poging om OT-netwerken te verstoren. Ze bestaan vaak uit brede en onsamenhangende lijsten aan te beëindigen programma's binnen zowel IT- als OT-omgevingen die vermoedelijk willekeurig zijn samengesteld.[121] Een andere ransomware-variant waarbij gebruik wordt gemaakt van een soortgelijke lijst, Clop, haalde in augustus 2022 het nieuws vanwege een aanval op het Britse bedrijf South Staffs Water. De aanvallers claimden hierbij toegang te hebben tot de OT-systemen van het drinkwaterbedrijf.[122] Zelf stelde de organisatie dat de aanval enkel betrekking had op de IT-omgeving en dat de drinkwatervoorziening nooit in gevaar is geweest.[123]

Het is de verwachting dat ransomware-actoren nieuwe tactieken zullen blijven ontwikkelen om hun slachtoffers verder onder druk te zetten. Ook komen industriële omgevingen steeds meer in beeld als verdienmodel van cyberactoren.[124] Hoewel ook aanvallen die niet direct gericht zijn op OT kunnen leiden tot operationele problemen, kan verdere en mogelijk meer gerichte verstoring van OT-systemen in deze context niet worden uitgesloten.[VI] De toenemende verweving van OT en IT vergemakkelijkt dit.

Hacktivisme vooral opportunistisch en symbolisch van aard

Hacktivisten lijken zich steeds meer te interesseren in het compromitteren van OT, omdat dit gebruikt kan worden als pressiemiddel om ideologische doelstellingen te behalen. Dit blijkt uit een toenemend aantal vermeende aanvallen die hacktivistische groeperingen opeisen.[125] De aangehaalde motieven door hacktivisten zijn gevarieerd van aard. Daarbij wordt onder andere verwezen naar de Russische oorlog tegen Oekraïne, maar ook naar andere maatschappelijke vraagstukken en geopolitieke ontwikkelingen wereldwijd.[126] Dergelijke aanvallen zijn over het algemeen echter opportunistisch van aard en gericht op systemen waar de aanvallers zelf vaak geen specifieke kennis van hebben. Zo wordt door hacktivisten gebruik gemaakt van publiek beschikbare middelen exploit-modules ('middelen') die zijn gericht op OT-systemen die met het internet zijn verbonden.[127]

De impact hiervan lijkt voorlopig zeer beperkt en de uitkomsten van aanvallen ongewis. Claims zijn vaak moeilijk te verifiëren en dienen voornamelijk een symbolisch doel. Bovenal is het compromitteren van een enkel OT-systeem niet voldoende om een gerichte uitkomst te bewerkstelligen. Als aanvallers een gericht effect teweeg willen brengen, moeten ze namelijk precies weten hoe ze een heel netwerk met verschillende systemen kunnen manipuleren.[128] Om aanvallen uit te voeren die langdurige fysieke gevolgen hebben is tijd, kennis en capaciteit nodig. Hierdoor is het onwaarschijnlijk dat ze door een minder-geavanceerde actor kunnen worden uitgevoerd.[VII] Hierbij moet worden opgemerkt dat de capaciteit van hacktivisten ook afhangt van de mate van verbondenheid met statelijke actoren. Zo kan er worden samengewerkt of kunnen hacktivisten als dekmantel worden gebruikt om attributie van digitale aanvallen te bemoeilijken.[129] De mate van verbondenheid is niet altijd duidelijk.

V Het Amerikaanse ministerie van Justitie bracht op 24 maart 2022 bijvoorbeeld twee aanklachten naar buiten tegen vier Russische overheidsfunctionarissen die verantwoordelijk worden gehouden voor meerdere digitale aanvallen gericht op OT-systemen, onder andere voor het verzamelen van inlichtingen bij honderden bedrijven binnen de energiesector in meer dan 135 landen. Deze aanvallen zouden mogelijk ook gelieerd zijn aan voorbereidingshandelingen voor sabotagedoeleinden.

VI Bekende voorbeelden van aanvallen op IT-systemen met grote operationele gevolgen zijn de NotPetya- en WannaCry-aanvallen (2017) waarbij wiperware zich ongecontroleerd kon verspreiden en de ransomware-aanval op Colonial Pipeline, een van de grootste oliepijpleidingen in de VS (2021). Ook vonden er begin 2022 diverse digitale aanvallen plaats op (olie-) opslag/overslaglocaties in Duitsland, België en Nederland. Hoewel de aanvallers het in dit geval gemunt hadden op de IT-systemen van de getroffen partijen, leidde de aanval alsnog tot de tijdelijke ontregeling van verwerkings- en distributieprocessen.

VII Organisaties dienen daarom ook rekening houden met de dreiging die uitgaat van *insider threats*, waaronder werknemers en contractanten. Zo maakte de Spaanse politie in juli 2022 de arrestatie van twee voormalige werknemers bekend die tussen maart en juni 2021 hun kennis inzetten bij het uitvoeren van digitale aanvallen op sensoren die worden gebruikt voor het meten van radioactieve straling.

Ruimte voor verbetering ondanks groeiende aandacht voor weerbaarheid

Uitdagingen omtrent weerbaarheid van OT-systemen

Zoals eerder beschreven zijn de meeste OT-systemen ontworpen in een tijd dat er geen rekening gehouden werd met mogelijk (digitaal) misbruik. De weerbaarheid tegen digitale dreigingen is lange tijd geen prioriteit geweest vanwege de beperkte koppeling van OT- met IT-systemen. De afgelopen jaren groeit de aandacht hiervoor wel. Er worden echter beperkt maatregelen getroffen op OT-netwerken uit zorg voor onvoorzienbare (ernstige) gevolgen voor het correct functioneren van (vitale) operationele processen. Dit leidt in de praktijk tot het ontbreken van basale maatregelen die in een IT-omgeving gebruikelijk zijn, zoals authenticatie, autorisatie en encryptie. Tevens worden OT-systemen niet of nauwelijks gescand op kwetsbaarheden en kwetsbare systemen worden zoals eerder vermeld niet altijd gepatcht (als er al een patch beschikbaar is) om het correct functioneren van deze systemen te garanderen. Daarnaast zijn de detectie en repressie van digitale aanvallen binnen een OT-omgeving bij veel organisaties niet voldoende ingericht.[130] Organisaties zijn hierdoor niet in staat om een aanval tijdig te detecteren (en hierop te reageren) als een aanvaller toegang krijgt tot het OT-netwerk.[131]

De beperkte set aan maatregelen binnen een OT-netwerk betekent niet dat OT-omgevingen niet weerbaar zijn. Zo worden er veel maatregelen getroffen om de veiligheid van het proces te waarborgen in het geval van een (digitale) calamiteit.[132] Daarnaast kenmerkt de digitale weerbaarheid zich door maatregelen die moeten voorkomen dat een aanvaller toegang krijgt tot het OT-netwerk.[133]

Binnen de IT en OT worden verschillende uitgangspunten, standaarden en prioriteiten gehanteerd op het gebied van safety (schade aan personen en/of omgeving) en security (beschikbaarheid, integriteit en vertrouwelijkheid). Bovendien gaan OT-systemen doorgaans vele jaren langer mee dan IT-systemen. Deze verschillen moeten worden meegenomen bij het ontwerp van het koppelvlak tussen IT en OT-omgevingen (en de daardoor gerealiseerde maatregelen). Dit gebeurt nog niet altijd voldoende, deels doordat de teams die zich bezighouden met IT en OT van oudsher los van elkaar opereren.[134]

Groeiende aandacht voor standaarden en publiek-private samenwerking

Ten aanzien van wet- en regelgeving geven enkele organisaties aan te worstelen met het interpreteren van de meldplicht voor incidenten binnen de OT-omgeving.[135] Ook zijn er organisaties die (te) weinig sturing vanuit de overheid ervaren, bijvoorbeeld omdat verplichte cybersecurity audits in bepaalde sectoren ontbreken.[136]

Vanuit de overheid is er wel steeds meer aandacht om organisaties te helpen met de beveiliging van hun OT-omgevingen. Middels de Nederlandse Cybersecuritystrategie zijn prioriteiten gesteld voor de toekomst.[137] Verder is er het afgelopen jaar ingezet op het aanbieden van gedeelde beveiligingsstandaarden. Een voorbeeld is de Basismaatregelen voor de cybersecurity van Industrial Automation & Control Systems (BIACS), die weer is afgeleid van de Cybersecurity Implementatierichtlijn Objecten 3.0 (CSIR), waarin zowel de BIO (Baseline Informatiebeveiliging Overheid) als het IEC 62443 normenkader in verwerkt zijn.[138] [139] Daarnaast worden er verschillende handvatten en tools ontwikkeld om organisaties op weg te helpen met de beveiliging van hun OT-omgevingen, zoals de 'Security Check Procesautomatisering'.[140] In de Cyber Resilience Act (CRA), het voorstel van de Europese Commissie voor beveiligingseisen aan digitale producten, worden daarnaast een aantal aanvullende eisen gesteld voor leveranciers van systemen die veelvuldig in OT-omgevingen gebruikt worden, zoals SCADA-systemen en PLC's.[141]

Ook weten publieke en private organisaties elkaar steeds beter te vinden. Er zijn meerdere samenwerkingsverbanden opgestart om dreigingen en risico's breed inzichtelijk te maken en gezamenlijke best practices te ontwikkelen.

Expertise en focus noodzakelijk voor OT-cybersecurity

Tenslotte is de weerbaarheid van OT-omgevingen gekoppeld aan de medewerkers die deze weerbaarheid realiseren. OT-omgevingen zijn anders dan IT-omgevingen en vereisen andere kennis en competenties op het gebied van cybersecurity. Er is binnen organisaties vaak nog onvoldoende aandacht voor nut en noodzaak van OT-cybersecurity. Zo moeten OT-cybersecurityteams vaak werken met beperkte middelen.[142] Daarnaast is kennis tussen OT-specialisten niet eenvoudig over te dragen door het verschil in OT-omgevingen in verschillende sectoren. Er is een beperkt aantal specialisten die over de benodigde expertise beschikken. Dat komt deels doordat opleidingen zich meer richten op IT-beveiliging. Deels komt dat ook doordat er van oudsher minder aandacht is geweest voor de beveiliging van OT-omgevingen vanwege de scheiding met andere netwerken.[143] [144]

Hoewel de weerbaarheid tegen digitale dreigingen lange tijd geen prioriteit is geweest, wordt de dreiging van verstoringen en het belang van digitale weerbaarheid de laatste jaren steeds meer noodzakelijk en breder erkend. Gegeven het groeiende aanvalsoppervlak en de potentieel ontwrichtende gevolgen van een digitale aanval op OT-systemen, is het zaak hierop voort te bouwen. Investeringen, kennisopbouw en ondersteunende technologische ontwikkelingen zijn hierbij essentieel.[145] [146]

Een IT-storing kan ervoor zorgen dat er geen treinverkeer mogelijk is. Reizigers wachten dan tevergeefs op een trein of zijn genoodzaakt de nacht op het station door te brengen.

5 Reflectie strategische thema's

In het CSBN 2022 heeft de NCTV in samenwerking met partners zes strategische thema's geïdentificeerd die de komende jaren relevant zijn voor de digitale veiligheid van Nederland. Deze zijn nog onverkort van toepassing. Het verkleinen van de in het CSBN 2022 benoemde scheefgroei tussen de digitale dreiging en de weerbaarheid blijft dan ook een grote uitdaging.

Bij de reflectie op deze thema's zijn enkele veranderingen opgevallen:

- de extra eisen voor digitale veiligheid die onder andere voortkomen uit nieuwe Europese wet- en regelgeving;
- de verdere verharding van geopolitieke spanningen;
- het onder druk staan van de verzekerbaarheid van digitale risico's;
- de toenemende onderlinge verwevenheid binnen het bredere ecosysteem;
- de gelegenheidsstructuur die het digitale ecosysteem vormt voor cyberaanvallen.

Een aanvullend 'nieuw' inzicht is dat digitale risico's integraal deel uitmaken van een breder en complex risicopalet en enkele andere bijzondere kenmerken hebben. Daardoor vragen digitale risico's om een bredere manier van beheersing dan andere risico's.

De in het CSBN 2022 benoemde zes strategische thema's worden in dit hoofdstuk kort toegelicht. Nieuwe inzichten die zijn ontstaan of veranderingen die zijn opgetreden, komen in afzonderlijke (sub) paragrafen aan bod. Iedere (sub) paragraaf bevat in de kop de essentie van het nieuwe inzicht of de verandering.

Nieuwe Europese wet- en regelgeving en de Nederlandse Cybersecurity Strategie 2022-2028 en het daarvan afgeleide actieplan leggen verdere eisen op aan digitale veiligheid. Omdat deze eisen effect hebben op alle in dit hoofdstuk genoemde strategische thema's, verdienen zij aparte aandacht.

Strategische thema's genoemd in het CSBN 2022

- Risico's vormen de keerzijde van een gedigitaliseerde samenleving;
- Digitale ruimte is speelveld voor regionale en mondiale dominantie;
- Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet;
- Marktdynamiek compliceert beheersing digitale risico's;
- Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen;
- Beperkingen in digitale autonomie beperken ook digitale weerbaarheid.

EU en Nederland vergroten eisen voor digitale veiligheid

EU vergroot eisen voor digitale veiligheid

De EU vergroot de eisen voor digitale veiligheid met Europese wet- en regelgeving. Zo beoogt de EU met de **Digital Services Act** (DSA) de verantwoordelijkheid en aansprakelijkheid te regelen van internetaanbieders, hostingbedrijven, online platformen, zoekmachines en marktplaatsen. De EU **Digital Markets Act** (DMA) moet gaan zorgen voor extra markt- en fusietoezicht op én concurrentieregels voor de wereldwijd grootste online platforms. De akkoorden over de DMA en DSA moeten vanaf medio 2024 gaan gelden in de lidstaten.[147] Met de **Cyber Resilience Act** (CRA) beoogt

de EU te komen tot een veiligere Europese digitale interne markt en een samenleving waarin onveilige producten van de markt kunnen worden geweerd en gehaald.[148] Nederland beoogt de CRA in 2024 geïmplementeerd te hebben.[149] Verder is de 'Richtlijn Network and information security' (NIS) herzien, wat heeft geresulteerd in de NIS2-richtlijn. De NIS2-richtlijn regelt welke bedrijven aan welke verplichte security-eisen moeten voldoen. Door de NIS2-richtlijn gaan meer organisaties onder de werking van de Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen dan nu. De NIS2-richtlijn scherpt daarnaast nog verschillende andere aspecten van de bestaande richtlijn aan. Het gaat dan bijvoorbeeld om eisen voor risicomanagement, het gebruik van encryptie, een verplichting voor het afhandelen van datalekken en het melden van cybersecurity-incidenten. De NIS2-richtlijn zal in 2024 via de Wbni in Nederland worden geïmplementeerd.[150]

Nederlandse Cybersecuritystrategie stelt hogere eisen aan digitale veiligheid

De nieuwe Nederlandse Cybersecuritystrategie 2022-2028 en het daaraan gekoppelde actieplan stellen hogere eisen aan digitale veiligheid en in het verlengde daarvan aan digitale weerbaarheid. De strategie beoogt een toekomst waarin de scheefgroei tussen digitale dreiging en weerbaarheid zo klein mogelijk is en blijft. Zo verhoogt het kabinet de prikkels voor veiligheid in digitale markten door strengere eisen te stellen aan digitale producten en diensten, risicomanagement van organisaties et cetera. De strategie bouwt nadrukkelijk voort op de hierboven genoemde Europese wet- en regelgeving. Naast het stellen van eisen, benoemt de strategie ook talrijke doelen, ambities en activiteiten om de digitale weerbaarheid van Nederland te vergroten.

Implementatie kost tijd

Organisaties, dienstverleners en producenten moeten zich gaan houden aan de nieuwe wet- en regelgeving. De bewustwording over en verdere uitwerking en implementatie van dat alles vergt wel de nodige doorlooptijd. Op de korte termijn zijn de eisen nog niet afdwingbaar totdat ze in wetgeving in de EU-landen zijn omgezet. Voor de veiligheidseisen voor digitale producten geldt bijvoorbeeld een overgangsregeling. Certificering en toezicht moeten nog worden ingericht. Lange tijd blijven de huidige, voor een deel, onveilige producten in gebruik en komen er nog steeds nieuwe onveilige producten in de markt.[151]

Enkele verbeteringen zijn daarentegen al doorgevoerd of in gang gezet. Zo is het per 1 december 2022 wettelijk toegestaan dat het NCSC dreigingsinformatie ook mag delen met niet-vitale bedrijven. Verder zijn de eerste stappen gezet in het samengaan van het Nationaal Cybersecurity Centrum (NCSC), het Digital Trust Center (DTC) en het Cyber Security Incident Response Team voor digitale dienstverleners (CSIRT-DSP) in één centraal expertisecentrum en informatieknooppunt. Deze nieuwe instelling gaat alle organisaties in Nederland - groot of klein, publiek of privaat, vitaal of niet-vitaal - van passende informatie en kennis voorzien.[152]

Risico's vormen de keerzijde van een gedigitaliseerde samenleving

Toelichting strategisch thema

De Nederlandse samenleving is in hoge mate gedigitaliseerd en de COVID-19-pandemie heeft verdere digitalisering van processen in een stroomversnelling gebracht. Dat heeft een keerzijde: de afhankelijkheid van digitale processen heeft ons ook kwetsbaar gemaakt voor uitval en voor de activiteiten van kwaadwillenden. De hoge mate van digitalisering van onze samenleving en de afhankelijkheid van digitale processen zijn een gegeven. Het beheersbaar krijgen en houden van kwetsbaarheden is onderdeel van risicobeheersing.

Digitale dreigingen onderdeel van dynamisch, complex en breder dreigingslandschap

Digitale dreigingen staan veelal niet op zichzelf en zijn onderdeel van een dynamisch, complex en breder dreigingslandschap. Cyberincidenten kunnen het gevolg zijn van bijvoorbeeld een verstoring van de elektriciteitsvoorziening. Andersom kunnen ze op hun beurt de oorzaak zijn van een verstoring van de elektriciteitsvoorziening.[153]

Bovendien geldt dat een hele kluwen van ontwikkelingen van invloed is op dreigingen die elkaar kunnen versterken of verzwakken. Zo vergroot de energietransitie het digitale aanvalsoppervlak voor kwaadwillenden. Het functioneren van zonneparken en het transporteren van energie afkomstig uit zonnepanelen en windturbines (en dergelijke) is immers afhankelijk van technologie.[154]

Ook kunnen dreigingen zich gestaag onder de radar opbouwen totdat een kantelpunt optreedt waarna het heel moeilijk is om die dreigingen te keren. Dit zijn zogenoemde sluimerende dreigingen. Zo'n gestage opbouw kan bijvoorbeeld spelen bij afhankelijkheden van Big Tech. Waar bedrijven en overheden vanuit (bedrijfs) economische logica 'als vanzelf' kiezen voor grote spelers in de markt, bestaat het risico dat er in de loop der tijd 'als vanzelf' een ongewenste afhankelijkheid ontstaat van het aanbod.

Verder kunnen sluimerende of nieuwe dreigingen voortkomen uit technologische ontwikkelingen. Zo neemt door Quantum computing de rekenkracht toe. Dat kan er in de toekomst bijvoorbeeld voor zorgen dat protocollen en gevoelige gegevens die nu met encryptie adequaat beveiligd zijn, dat straks niet meer zijn.[155] Data die nu vercijferd wordt verstuurd of opgeslagen, kan met toekomstige quantumcomputers alsnog worden ontcijferd.[156] Het moment waarop quantumcomputers een dreiging zullen vormen voor momenteel gebruikte cryptografie is onvoorspelbaar. Het is echter van belang dat organisaties zich hierop voorbereiden en de inzet van bijvoorbeeld post-quantumcryptografie verkennen.[157] Bedrijven investeren volop in de zogeheten metaverse. Het is

moeilijk om in te schatten hoe dat er uit gaat zien en in hoeverre het een rol gaat spelen in onze samenleving en economie. Daarmee is het ook lastig om in te schatten wat de metaverse gaat betekenen voor de digitale veiligheid. De ervaring leert dat nieuwe technologie zowel kansen als risico's met zich meebrengt.

Snelle ontwikkeling en gebruik generatieve AI van invloed op digitale veiligheid

Een duidelijk voorbeeld waaruit blijkt dat andere, in dit geval technologische, ontwikkelingen van invloed kunnen zijn op digitale veiligheid, is dat van 'Generatieve AI'. Dit is een vorm van AI die op basis van door de gebruiker gegeven opdrachten of vragen nieuwe content kan creëren uit bestaande data. ChatGPT, een voorbeeld hiervan, leidde in november 2022 tot een hype en is sindsdien onderwerp van debat. In maart 2023 verscheen een verbeterde versie van het onderliggende taalmodel (GPT-4), dat nog meer geavanceerde resultaten levert.

Het gebruik van en de mogelijkheden van generatieve AI zijn zich nog volop aan het ontwikkelen en de impact op de samenleving kent nog vele onduidelijkheden. Toch zijn tot nu toe in ieder geval vier relevante invalshoeken te onderkennen:

1. De algoritmen en de data waarmee de algoritmen worden gevoed kunnen doelbewust worden gemanipuleerd. Dat kan bijvoorbeeld (maar niet alleen) door middel van cyberaanvallen.

2. Gebruikers kunnen (onbedoeld en onbewust) toegang geven tot zoekvragen en/of gevoelige informatie door de vragen die ze stellen, de informatie die ze invoeren of de informatie waarmee ze de applicaties voeden.[158]

3. Generatieve AI kan worden gebruikt voor cyberaanvallen. Zo kunnen met behulp van AI meer op een ontvanger toegesneden phishing-mails worden gemaakt. Dit geeft een grotere kans dat de ontvanger die als betrouwbaar beoordeelt. Ook kan laagdrempelig malware worden ontwikkeld.[159]

4. Generatieve AI kan worden ingezet ter verdediging tegen cyberaanvallen door bijvoorbeeld cybersecurity-adviezen te genereren.

Bij grootschalig gebruik van deze technieken, kan steeds lastiger de authenticiteit en autoriteit van tekstuele informatie, afbeeldingen, video's en audio worden vastgesteld. Generatieve AI kan, zelfs zonder dat sprake is van kwade bedoelingen, feitelijk onjuiste informatie produceren en verspreiden.

Onverminderde digitale dreiging

Aard digitale risico's niet fundamenteel anders

De reeds in het CSBN 2022 benoemde digitale risico's hebben nog steeds dezelfde aard (zie kader op volgende pagina). De risico's gelden direct of indirect ook voor specifieke sectoren en organisaties én individuele burgers.

Vier risico's voor de nationale veiligheid

1. Ongeautoriseerde inzage in informatie en eventueel publicatie daarvan, in het bijzonder door spionage. Denk aan spionage gericht op communicatie binnen de Rijksoverheid of spionage om de ontwikkeling van innovatieve technologieën te achterhalen. Denk ook aan inzage in informatie over medewerkers of bedrijfsprocessen als springplank voor cyberaanvallen of andere kwaadaardige doeleinden.
2. Ontoegankelijkheid van processen, zoals door (voorbereidingen voor) sabotage van processen die zorgdragen voor de energievoorziening en cybercriminaliteit, waaronder de inzet van ransomware en DDoS-aanvallen.
3. Schending van de (veiligheid van de) digitale ruimte, bijvoorbeeld door misbruik van mondiale ICT-leverancierskketens, misbruik van internetprotocollen of sabotage van kabels.
4. Grootschalige uitval: een situatie waarin één of meer processen zijn verstoord als gevolg van natuurlijke of technische oorzaken of als gevolg van niet-moedwillig menselijk handelen.

Digitale dreigingen onverminderd groot

De verzameling van digitale dreigingen is onverminderd groot. Daar liggen diverse oorzaken aan ten grondslag. Een eerste is de hierboven genoemde wisselwerking met andere, zeker ook niet digitale, dreigingen en ontwikkelingen. Een tweede oorzaak komt voort uit de complexiteit en verwevenheid van digitale processen, systemen en netwerken. Het gevolg daarvan is een groot en groeiend aanvalsoppervlak voor kwaadwillenden en een grotere kans op uitval. Met aanvalsoppervlak wordt gedoeld op manieren waarop een kwaadwillende digitale processen kan aanvallen. Denk daarbij aan (componenten van) hardware, software en netwerken, evenals aan verwevenheid in het bredere ecosysteem (zie verderop). In digitale processen worden keer op keer - organisatorische of menselijke - kwetsbaarheden gevonden die uitgebuit (kunnen) worden. De kans op grootschalige uitval neemt eveneens toe vanwege complexiteit en verwevenheid. Verouderde systemen (legacy) vergroten eveneens het risico van uitval.

Een derde oorzaak komt voort uit de geopolitieke spanningen tussen landen, in het bijzonder de Russische oorlog tegen Oekraïne. Hierdoor kunnen statelijke actoren bijvoorbeeld vaker overgaan tot cyberaanvallen, met bijvoorbeeld keteneffecten als gevolg (zie verder hoofdstuk 3).

Een vierde oorzaak is het aantrekkelijke verdienmodel voor cybercriminelen. Dat geldt zeker voor ransomware-aanvallen,

'commercialisering' van cyberaanvallen in de vorm van Cybercrime-as-a-Service (CaaS) en veredeling en verkoop van buitgemaakte informatie (zie verderop).

Een vijfde oorzaak zijn internationale conflicten en controversiële binnenlandse onderwerpen als mogelijke aanleiding voor hacktivisme. In 2022 was sprake van een opleving van het hacktivisme, met name door de oorlog in Oekraïne (zie hoofdstuk 2 en 3). Over vele onderwerpen bestaan meningsverschillen tussen bevolkingsgroepen in en buiten Nederland en hacktivisten kunnen zich daarbij gaan roeren. Hacktivisten lijken zich steeds meer te interesseren in het compromitteren van OT, omdat dit gebruikt kan worden als pressiemiddel om ideologische doelstellingen te behalen (zie hoofdstuk 4). Zoals eerder aangegeven, geldt wel dat de impact van hacktivistische activiteiten veelal kortdurend en beperkt is. Ook is attributie lastig, omdat hacktivistische groepen over het algemeen losjes zijn georganiseerd en bovendien kan vermenging met statelijke actoren niet worden uitgesloten. Bij hacktivisme in het buitenland kunnen Nederlanders betrokken zijn doordat zij zich aansluiten bij buitenlandse hacktivistische groepen.

Een zesde oorzaak is concentratie van informatie en digitale processen vanuit het belang van bedrijfsvoering. Deze zijn bij uitstek aantrekkelijk voor misbruik door kwaadwillenden. Zo wijst de Autoriteit Persoonsgegevens op de risico's die kleven aan een centrale database met alle persoonsgegevens die mensen aanleveren voor een paspoortaanvraag, zoals vingerafdrukken, handtekeningen en pasfoto's. Zo'n database met gegevens van heel veel Nederlanders brengt grote privacyrisico's mee en er kan onduidelijkheid ontstaan over wie verantwoordelijk is voor de veiligheid van de gegevens.[160] Verder vormt een dergelijke grote concentratie van informatie een aantrekkelijk doelwit voor cyberactoren en bij uitval kunnen vele daaraan gerelateerde processen tot stilstand komen.

Een zevende oorzaak is de beperkte kans voor kwaadwillenden om opgepakt en/of uitgeleverd te worden voor het uitvoeren van een cyberaanval. Soms worden kwaadwillenden wel aangeklaagd, maar kunnen zij zich in eigen land vrij blijven bewegen of worden ze niet uitgeleverd. Niet voor niets werd in CSBN 2022 gesteld dat cyberaanvallen door statelijke actoren wel het nieuwe normaal lijken te zijn. Het aantal gedocumenteerde gevallen waarin criminele actoren zijn opgepakt en berecht, is wereldwijd uiterst gering.

Uiteenlopende bronnen van dreiging

Net als voorgaande jaren zijn statelijke en criminele actoren verantwoordelijk voor het leeuwendeel van de cyberaanvallen. Opgemerkt moet worden dat statelijke en criminele actoren op uiteenlopende wijzen (bewust of onbewust) kunnen samenwerken en dat grenzen niet altijd scherp kunnen worden getrokken. Cybercriminelen zullen naar verwachting een prominent aandeel blijven vormen van verstorende cyberaanvallen in Nederland, vooral met ransomware-aanvallen. Het gevolg kan zijn dat buitgemaakte informatie wordt gepubliceerd of tussen criminelen wordt verhandeld.

Hoewel wellicht minder tot de verbeelding sprekend, gaat van uitval eveneens een dreiging uit. Daar kunnen naast technisch en menselijk falen, ook fysieke oorzaken aan ten grondslag liggen, zoals overstromingen, natuurbranden en uitval van vitale processen.

Ook van hacktivisten gaat een dreiging uit (zie hierboven). Verder moet ook rekening worden gehouden met cyberaanvallen door insiders, bijvoorbeeld een recent ontslagen medewerker, script kiddies, personen die cyberaanvallen uitvoeren voor de lol of om te laten zien wat zij kunnen, en in mindere mate door terroristen.

Alle digitale processen, organisaties en sectoren zijn aantrekkelijk voor cyberactoren

Cyberactoren richten zich actief op het verkrijgen van toegang tot en/of het vergaren van zoveel mogelijk informatie. Nederlandse organisaties zijn bijvoorbeeld op grote schaal doelwit van diverse digitale aanvalscampagnes van staten om hoogwaardige technologie en kennis buit te maken.[161] In het jaarverslag 2022 noemt de AIVD hierbij specifiek China, Iran, Noord-Korea en Rusland. De dienst stelt dat de risico's van deze aanvallen enorm zijn, voor zowel de overheid, bedrijven en kennisinstellingen, als uiteindelijk burgers.[162] Ook de MIVD waarschuwt in het jaarverslag 2022 voor de cyberdreiging van statelijke actoren.[163]

Statelijke actoren gaan actief op zoek naar zwakke schakels in ketens, als opstap naar interessante(re) doelwitten. Verder is het zo dat bijvoorbeeld criminelen continu alle 'digitale deuren' proberen te openen ongeacht de organisatie, met alle gevolgen van dien voor de slachtoffers. Actoren kunnen gestolen informatie gebruiken a) als opstap voor cyberaanvallen of cybercriminaliteit, b) om slachtoffers te chanteren door te dreigen met publicatie, c) door reputatieschade aan te richten met publicatie, of d) door met gestolen data geloofwaardigheid te creëren voor het verspreiden van desinformatie.

Actoren richten zich ook op het ontoegankelijk maken van digitale processen, bijvoorbeeld door middel van ransomware-aanvallen, door DDoS-aanvallen of door andere (voorbereidingshandelingen voor) sabotage. Mogelijke motieven daarvoor zijn onder andere chantage, het aanrichten van reputatieschade, wraak of geopolitieke overwegingen.

Sectoren of organisaties die voor de aanvallers ogenschijnlijk niet interessant zijn, kunnen toch aantrekkelijk zijn als opstap naar een ander primair doelwit. Aanvallers richten zich bij uitstek op doelwitten die een springplank naar andere doelwitten kunnen vormen. Ook worden centrale doelwitten gekozen waarvan veel sectoren, organisaties en processen afhankelijk zijn, zoals ICT-dienstverleners. Dit om zo indirect andere processen, organisaties en sectoren te raken. Doordat verschillende leveranciers van hard- en software een (semi)monopolistische positie hebben verworven, is er sprake van mondiale ecosystemen met grote concentraties van persoonsgegevens. Bijvoorbeeld

organisaties die de salarisadministratie van andere organisaties uitvoeren, verwerken informatie die voor aanvallers heel waardevol kan zijn. De AIVD zag in 2022 onder andere dat verschillende landen met een offensief cyberprogramma probeerden data te stelen in de (Europese) reis- en luchtvaartsector. Die informatie combineren ze met andere informatie om mensen die voor hen interessant zijn, te identificeren, op te sporen of te volgen.[164] Organisaties die veel informatie verwerken, vormen dus een aantrekkelijk doelwit voor cyberactoren. De MIVD meldde in het jaarverslag dat een statelijke actor routers heeft gehackt van Nederlandse particulieren en het midden- en kleinbedrijf. Deze actor kan de gehackte routers misbruiken om heimelijke cyberoperaties tegen Nederlandse belangen of die van bondgenoten uit te voeren.[165]

Symbolische Nederlandse doelwitten, zoals internationaal bekende Nederlandse multinationals of instanties, kunnen eveneens een doelwit vormen met als onderliggend motief wraak op Nederland of de Nederlandse regering (zie Jaarbeeld).

Digitale ruimte is speelveld voor regionale en mondiale dominantie

Toelichting strategisch thema

Een groeiend aantal staten gebruikt de digitale ruimte structureel én intensief voor de behartiging van hun geopolitieke belangen. Cyberaanvallen, bijvoorbeeld voor het vergaren van politieke en economische inlichtingen, zijn daartoe een belangrijk instrument: ze zijn relatief goedkoop en schaalbaar en ze hebben een hoge, vaak langdurige opbrengst. Ook is attributie een lastige kwestie. Verder vindt rond de bouwstenen van de digitale ruimte en hoogwaardige technologieën een geopolitiek steekspel plaats. Individuele burgers, organisaties, sectoren en landen kunnen weinig invloed uitoefenen op die geopolitieke wedijver, terwijl die wel bijdraagt aan de verhoging van risico's.

Verharding geopolitieke spanningen

De geopolitieke situatie is in het afgelopen jaar verhard. Hierdoor grijpen statelijke actoren vaker naar cyberaanvallen als middel om hun belangen te behartigen, met mogelijke keteneffecten als gevolg. Dergelijke keteneffecten kunnen zich onverwacht voordoen. De Russische oorlog tegen Oekraïne is een prominent voorbeeld van de geopolitieke verharding (zie hoofdstuk 3). In het recente Dreigingsbeeld Statelijke Actoren komen vier kernboodschappen aan bod: 1) de territoriale veiligheid van de EU, de NAVO en Nederland staat verder onder druk, 2) statelijke inmenging blijft de sociale en politieke stabiliteit in Nederland raken, 3) Nederland wordt steeds vaker openlijk en heimelijk geconfronteerd met dreigingen tegen de economische veiligheid en 4) de internationale rechtsorde staat in toenemende mate onder druk. Ook wordt gesteld dat Nederland nog steeds doelwit is van offensieve cyberprogramma's van statelijke actoren.[166] Daarnaast waarschuwt de MIVD ook voor fysieke sabotage, bijvoorbeeld van internetkabels. Zo brengt Rusland de vitale maritieme infrastructuur in de Noordzee in kaart, en onderneemt activiteiten die duiden op spionage en voorbereidingshandelingen voor verstoring en sabotage.[167] Als dergelijke activiteiten succesvol zijn, kan dat doorwerken naar de digitale ruimte.

Sectoren en organisaties kunnen wel de gevolgen ondervinden van deze verharding, maar daar weinig aan veranderen. Het vormt dan ook een factor waarmee bij de bepaling van het gewenste niveau van digitale weerbaarheid rekening moet worden gehouden.

Cybercriminaliteit is industrieel schaalbaar, weerbaarheid nog niet

Toelichting strategisch thema

Zware, georganiseerde cybercriminaliteit is zeer schaalbaar geworden en heeft daardoor in de afgelopen jaren qua slachtoffers, schade en criminele opbrengsten een industriële omvang aangenomen. De term schaalbaarheid verwijst naar het vermogen om een systeem of proces aan te passen (op te schalen) om te kunnen voldoen aan een grotere vraag. Zware cybercriminelen en hun dienstverleners zijn primair financieel gemotiveerd en gaan voor maximale opbrengsten, waarbij ze dankbaar gebruik maken van de mogelijkheden die de digitale ruimte biedt. Gezien de aard en groeiende omvang van de cybercriminele dreiging is het schaalbaar maken én houden van de weerbaarheidsketen een fundamentele uitdaging voor de komende jaren.

Criminele afpersing blijft aantrekkelijk verdienmodel

Afpersing door cybercriminelen blijft een aantrekkelijk verdienmodel. Dat geldt zeker voor het versleutelen van bestanden en/of het dreigen met publicatie van buitgemaakte informatie. De professionalisering en commercialisering van cybercriminele tools en diensten neemt verder toe. Niet alleen kunnen technisch vergevorderde criminelen hier aan verdienen, maar ook nemen de mogelijkheden voor een bredere groep van criminelen toe om cyberaanvallen te plegen. Zo ziet de politie dat de wijze waarop criminelen toegang verkrijgen tot het netwerk van slachtoffers steeds complexer worden. Multifactor authenticatie is daardoor bijvoorbeeld niet altijd meer afdoende.[168] Bij ransomware-aanvallen worden enorme geldbedragen geëist en soms ook betaald.

De risico's voor criminelen omgepakt of veroordeeld te worden, blijven relatief laag. Daar waar halverwege 2021 de internationale druk op bijvoorbeeld de Russische overheid toenam om criminelen in eigen land aan te pakken, is deze druk feitelijk niet meer aanwezig als gevolg van het conflict tussen Rusland en Oekraïne en de daaropvolgende geopolitieke isolatie van Rusland. Dit creëert

meer ruimte voor cybercriminelen in Rusland om relatief ongestoord hun gang te gaan.

Toch blijven er wel risico's bestaan voor cybercriminelen. Bekende ransomware-groepen veranderen van naam, of splitsen zich op in kleinere cellen. Dit kan meerdere oorzaken hebben. Het kan gaan om pogingen om de groeiende druk door internationale opsporingsdiensten en internationale sancties het hoofd te bieden. Dat een rebranding of opheffing van een groep vaak plaatsvindt na media-aandacht met betrekking tot grote incidenten of aanvallen met grote impact, onderschrijft dit. Mogelijk vrezen deze groepen mede door de zogeheten Conti-leaks dat binnen grotere groepen de kans op onderlinge conflicten groter is. Gelekte chatgesprekken van de Conti-groep onthulden details over de omvang, het leiderschap en de operaties van de beruchte ransomware-groep. De documenten zijn vermoedelijk gelekt als vergelding voor Conti's pro-Russische houding.[169] Door de oorlog is de kans op onenigheid of verschillende loyaliteiten van groepsleden groter. Hierdoor zijn de risico's op overlopers naar andere groepen, of leden die bijvoorbeeld broncodes lekken van door de groepen zelf ontwikkelde malware, eveneens groter.[170]

Het aantal geregistreerde gevallen van cybercriminaliteit, zoals hacken, het plegen van DDoS-aanvallen of ransomware-aanvallen, is in het kalenderjaar 2022 licht gedaald ten opzichte van 2021. De politie registreerde in 2022 13.949 incidenten, een afname van 2 procent in vergelijking met 2021.[171] Het aantal ransomware-aanvallen (ook op Nederlandse organisaties) leek in 2022 eveneens tijdelijk te dalen, om aan het eind van het jaar weer toe te nemen. Vermoedelijk speelt hier de impact van de Russische oorlog tegen Oekraïne op het cybercriminele ecosysteem een rol. Beide landen zijn belangrijke bronlanden van zware, georganiseerde cybercriminaliteit.[172] Criminelen kozen een kant in de oorlog, wat bestaande samenwerkingsverbanden onder druk zette. Toch moet deze – al dan niet tijdelijke – daling in het juiste perspectief worden gezien. De politiecijfers zijn nog steeds zorgwekkend hoog. Bedrijven, maar ook gemeenten en publieke instellingen lopen onverminderd het risico slachtoffer te worden van ransomware of andere vormen van cybercriminaliteit. Er wordt niet altijd aangifte gedaan, bijvoorbeeld om imagoschade te voorkomen.[173]

Uit politieonderzoek bleek dat criminelen buitgemaakte informatie verrijken met andere informatie én doorverkopen. Dit blijkt lucratief te zijn. Uit datzelfde onderzoek bleek dat criminelen soms ook buitgemaakte informatie veredelen en verkopen, terwijl het slachtoffer de criminelen heeft betaald om publicatie van informatie te voorkomen.[174]

Criminelen lijken vaker cyberaanvallen uit te voeren tegen vitale sectoren

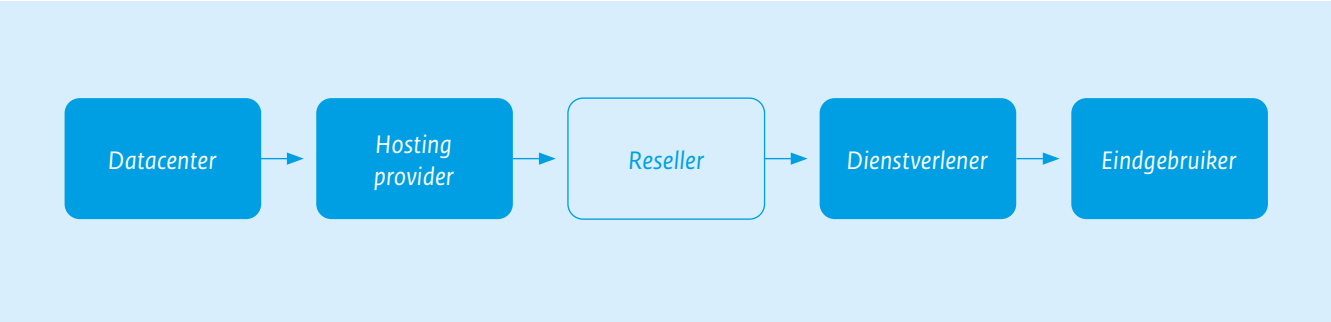
Ransomware-aanvallen lijken zich, zeker in de VS, steeds vaker te richten op vitale sectoren, waaronder de energiesector.[175] In Europa waren diverse bedrijven in de energiesector slachtoffer van cyberaanvallen.[176] [177] In één geval had dit ook impact op een dochterbedrijf in Nederland. In België slaagde een ransomware-groep erin om gevoelige data te stelen van de politie.[178] Verder hebben zich ook ransomware-aanvallen voorgedaan op gemeenten. Dat heeft er onder andere toe geleid dat gemeentelijke taken gedurende enige tijd niet of verminderd konden worden uitgevoerd, terwijl er voor de uitvoering van die gemeentelijke taken geen alternatieven bestaan (zie Jaarbeeld). Vitale sectoren vormen aan de ene kant een aantrekkelijk doelwit doordat de gevolgen van ransomware dusdanig groot kunnen zijn dat die sectoren sneller bereid zouden kunnen zijn om te betalen. Aan de andere kant vormen ze geen aantrekkelijk doelwit doordat dergelijke aanvallen tot meer aandacht van overheden leiden. Dat kan in het nadeel van de criminelen uitpakken.

Cybercriminelen afhankelijk van malafide en bonafide digitale ecosysteem en daardoor kwetsbaar

Net als legale organisaties ontkomen ook cybercriminelen er niet aan om onderdeel te zijn van een breder digitaal ecosysteem. Dat ecosysteem vormt een gelegenheidsstructuur voor cybercriminelen. Door toenemende specialisatie onder cybercriminelen worden ook zij steeds afhankelijker van elkaars (online) diensten in het kader van cybercrime-as-a-service. Deze afhankelijkheid geldt ook voor het afnemen van legale diensten. Webhosting is een goed voorbeeld. Nederlandse bonafide hostingbedrijven verhuren ruimte op het internet voor bijvoorbeeld het plaatsen van een website of clouddienst. Zij verhuren vaak onbewust ruimte op hun servers aan buitenlandse bedrijven, zogenoemde resellers. Malafide, vaak Russische, resellers verhuren deze servers op hun beurt willens en wetens door aan criminelen, zo constateert de politie. Ransomware-bendes maken hier graag gebruik van voor het uitvoeren van hun aanvallen.[179] Verder maken statelijke actoren al jaren gebruik van de Nederlandse digitale infrastructuur.[180]

Een cybercrimineel die van de eindgebruiker een slachtoffer wil maken, heeft een hele keten nodig om zijn misdrijven uit te voeren. Naast webhosting, geldt de afhankelijkheid van cybercriminelen voor tal van andere internetdiensten. Bijvoorbeeld communicatiediensten als VPN, domeinregistraties, en zelfs regionale internet registers en transit providers. Deze afhankelijkheden gaan hand in hand met de enorme schaalbaarheid van cybercriminaliteit. Sterker: zonder zowel de legale, als de malafide dienstverleners (en het grijze gebied daartussen), kunnen cybercriminelen niet opereren.

De afhankelijkheid van het bredere digitale ecosysteem vormt een zwakke plek voor cybercriminelen, maar ook voor kwaadwillende statelijke actoren. Deze afhankelijkheid biedt kansen voor het verhogen van de digitale weerbaarheid door barrières tegen het malafide gebruik op te werpen. In de financiële sector is wet- en regelgeving ter voorkoming van witwassen gemeengoed, waardoor bijvoorbeeld ongebruikelijke transacties standaard gemeld moeten worden. Als het om internetdiensten in de brede zin gaat, zijn principes als aanvaardbaar gebruik, ken-je-klant, het zorgvuldigheidsbeginsel en antimisbruikbepalingen veelal nog



Afbeelding 1 *afhankelijkheden binnen webhosting*

vrijblijvend, met alle ruimte voor het wel of niet naleven ervan als gevolg. Dit biedt cybercriminelen vele kansen om anoniem én schaalbaar te werk te gaan. Kansen die zij niet onbenut laten.

Marktdynamiek compliceert beheersing digitale risico's

Toelichting strategisch thema

In digitale markten komen vraag en aanbod naar digitale diensten, (componenten van) hardware, software en netwerken samen. Deze markten hebben enkele unieke kenmerken. Bijvoorbeeld de (semi)monopolistische status van bepaalde leveranciers, de hoge mate van onderlinge verwevenheid en de focus op het vergaren van zoveel mogelijk data. Ook zijn in deze markten prikkels voor digitale veiligheid niet (altijd) doorslaggevend. Die kenmerken compliceren de beheersing van risico's voor individuele burgers, organisaties, sectoren en landen. Daarbij doet zich een paradox voor. Aan de ene kant kunnen individuele keuzes van burgers, organisaties, sectoren en landen risico's voor anderen vergroten of verkleinen. Aan de andere kant is de ruimte om autonome keuzes te maken voor risicobeheersing juist beperkt vanwege een gebrek aan reële of veilige(re) alternatieven.

Verzekerbaarheid digitale risico's staat onder druk

Hoewel organisaties veel kunnen doen aan digitale weerbaarheid, kunnen cyberincidenten zich toch voordoen en/of is schade niet altijd te voorkomen. Cyberverzekeringen kunnen schade dekken wanneer zich een cyberincident heeft voorgedaan, ondersteuning bieden tijdens een cyberincident en eisen stellen aan weerbaarheid alvorens een verzekering kan worden afgesloten.

De verzekerbaarheid van digitale risico's staat onder druk om een aantal redenen. Een eerste reden die verzekeraars noemen is de toename van digitale risico's. Het aantal cyberaanvallen neemt al jaren toe en daarmee ook de schade. De claims zorgen ervoor dat verzekeraars hun polisvoorwaarden opschroeven en dat de premies stijgen. Ook moeten steeds meer klanten voldoen aan hoge beveiligingseisen. Wie ruim onvoldoende scoort, krijgt geen polis.[181] Verzekeringen staan ook onder druk doordat cyberincidenten kunnen uitgroeien tot een systemische crisis en daardoor onverzekerbaar zijn.[182] Incidenten als Wannacry en NotPetya in het verleden spelen bij dat inzicht een rol. Zo moet een Amerikaanse verzekeringsmaatschappij 1,4 miljard dollar schade vergoeden die een farmaceutisch bedrijf door NotPetya leed.[183] Verder geldt dat de markt voor cybersecurityverzekeringen in Nederland beperkt is in omvang en in de kinderschoenen staat. Dat heeft volgens De Nederlandse Bank (DNB) te maken met een gebrek aan historische data, waardoor data over incidenten en de daaruit voortvloeiende schade beperkt zijn. Ook zijn veel bedrijven en huishoudens zich niet bewust van de potentiële schade die digitale risico's met zich kunnen meebrengen. In combinatie met de onbekendheid van veel incidenten belemmert dat de verdere ontwikkeling van deze verzekeringsmarkt.[184]

Ook is er vaak onduidelijkheid over de dekking van risico's als gevolg van cyberincidenten binnen bestaande (traditionele) verzekeringen. Dit wordt aangeduid als 'silent cyber', de dekking van cyberschade in traditionele polissen, terwijl dit niet expliciet in deze polissen is voorzien. De Europese toezichthouder EIOPA ziet hierdoor risico's voor toenemende onduidelijkheid over de dekking van risico's als gevolg van cyberincidenten. Deze onduidelijkheid is mede het gevolg van onduidelijke definities als het gaat om cyberincidenten. Dit kan voor polishouders leiden tot onduidelijkheid over de dekkingsgraad van hun polissen en het nut en de noodzaak van eventuele aanvullende cyberverzekeringen.[185]

DNB waarschuwt voor uitsluiting van klanten met een verhoogd risicoprofiel.[186] Naast uitsluiting kunnen organisaties ook te maken krijgen met zodanig hoge premies of eisen dat zij moeten afzien van een verzekering. Dit alles kan er uiteindelijk toe leiden dat financieel gezonde organisaties ten onder gaan aan schade die zij lijden als gevolg van cyberincidenten.

Samenhangend en geïntegreerd risicomanagement staat nog in de kinderschoenen

Toelichting strategisch thema

Een samenhangend en geïntegreerd risicomanagement binnen en tussen de niveaus van organisaties, sectoren en nationaal, staat nog in de kinderschoenen. De weerbaarheid in Nederland is nog niet voldoende op niveau. Digitale risico's nemen nog geen structurele plaats in het bredere risicomanagement in en een samenhangende aanpak is nodig.

Als gevolg van nieuwe Europese wet- en regelgeving krijgen bestuurders van veel organisaties binnen de EU een grotere wettelijk verankerde verantwoordelijkheid als het gaat om het beheersen van digitale risico's.

Onderdeel zijn van een breder ecosysteem compliceert risicobeheersing

Of het nu gaat om landen, sectoren of organisaties, weinigen kunnen onafhankelijk functioneren van een breder ecosysteem. Dat compliceert risicobeheersing.

Onderdeel zijn van een breder ecosysteem heeft vele voordelen, onder andere voor de digitale veiligheid. Dat geldt bijvoorbeeld voor cloudvoorzieningen, die de technische infrastructuur voor hun rekening nemen. Dat is inmiddels zo complex geworden, dat uitbesteding een rationele keuze kan zijn en juist bij kan dragen aan digitale veiligheid. Het zogeheten 'netwerk-as-a-service' voorziet dan ook in een steeds grotere behoefte.[187]

Onderdeel zijn van een breder ecosysteem heeft ook nadelen. De risico's zijn lastig inzichtelijk te maken. Het is niet langer voldoende om enkel de toeleverancierssketens van de eigen organisatie, sector of land te bezien. Zo worden sectoren en dienstverleners actief in meer verbanden en raken zij daardoor op steeds meer lagen en lijnen verbonden. Daardoor raken risico's ook verbonden.[188] Voor een individuele sector of organisatie is het lang niet altijd duidelijk welke afhankelijkheden – en dus kwetsbaarheden – er bestaan. Veelal blijkt pas bij een incident dat een groot aandeel van de organisaties binnen een sector diensten afneemt van één partij. Incidenten bij een dergelijke partij, ongeacht de aard of oorzaak, heeft mogelijk een grootschalige nationale of zelfs grensoverschrijdende impact tot gevolg.

Een prominent voorbeeld hiervan deed zich voor in maart 2023. Bedrijven en organisaties, waaronder enkele grote, nemen diensten af van marktonderzoekbureaus, welke op hun beurt klant zijn bij dezelfde softwareleverancier. Een actor kreeg toegang tot het netwerk van de softwareleverancier en zou ook daadwerkelijk gegevens hebben buitgemaakt. Daardoor kwamen de gegevens van naar schatting rond de 2 miljoen Nederlanders in de openbaarheid.[189] In dit voorbeeld werden dus klanten van bedrijven en organisaties slachtoffer van een datalek bij de softwareleverancier van marktonderzoeksbureaus. Het gaat daarbij om slachtoffers in de derde lijn.

Risico's die het gevolg zijn van incidenten bij anderen, zijn lastig te beheersen. De belangen van een organisatie die slachtoffer is geworden van een cyberincident kunnen bijvoorbeeld botsen met die van andere organisaties die daarvan afhankelijk zijn. Een organisatie kan bijvoorbeeld prioriteit geven aan het weer operationeel krijgen van digitale processen na een ransomware-aanval. Het inzichtelijk krijgen welke informatie van welke klanten is gelekt en/of als pressiemiddel al is gepubliceerd, kan in zo'n geval achterwege blijven, maar wel leiden tot schade bij klanten in de keten. Ook bevoegdheden zijn bij dergelijke incidenten niet altijd helder, zoals bijvoorbeeld bleek tijdens de ransomware-aanval bij een grote leverancier voor toepassingen rondom authenticatie en toegangspassen[190] en uit bovengenoemde casus.[191] Mag bijvoorbeeld een door een slachtoffer ingehuurd cybersecuritybedrijf bevindingen delen met het NCSC en/of de politie en/of de Chief Information Security Officer van een departement dat klant is? Welke informatie mogen die partijen opvragen aan de organisatie die is getroffen en moet die daarop reageren?

Impact digitale dreiging beperkt inzichtelijk en onvoorspelbaar

Wat de impact van de digitale dreiging kan zijn, is beperkt inzichtelijk en in hoge mate onvoorspelbaar. Dat geldt ook bij de beoordeling van de gevolgen van cyberincidenten die zich voordoen.[VIII] Dat geldt zeker voor het niveau van nationale veiligheid en sectoren.

Voor het beoordelen van de gevolgen van concrete cyberincidenten geldt dat vele actoren en factoren van invloed zijn. Zo laten de gevolgen van een concrete digitale spionagecampagne zich lastig beoordelen: wat is ontvreemd, door wie, over welke periode, wat is de gebruikswaarde ervan voor de dader én wat is dan de financiële en/of reputatieschade op korte of lange termijn (en dergelijke)? Die vragen zijn lastig, zo niet onmogelijk te beantwoorden. Omdat er talloze situaties denkbaar zijn als het gaat om cyberincidenten, zeker in combinatie met een mogelijke doorwerking naar het fysieke domein, is in het Landelijk Crisisplan Digitaal voor een aantal bouwstenen gekozen. Deze bouwstenen hebben betekenisvolle verschillen voor de gevolgen van een cyberincident. Het gaat om de volgende bouwstenen: oorzaak, bron, actor, geraakt domein, geraakt gebied en technisch oplossingsperspectief.[192]

De gevolgen van alle cyberincidenten binnen een sector of in Nederland zijn nog lastiger objectief in kaart te brengen. Zo

VIII Gevolgen wordt vooral gebruikt in combinatie met cyberincidenten. Impact wordt vooral gebruikt in combinatie met dreiging.

kunnen de gevolgen van een digitale spionagecampagne op enkele bedrijven ogenschijnlijk meevallen. Toch kan over een langere termijn digitale spionage een aanhoudend 'lek' creëren van hoogwaardige economische kennis naar het buitenland en gevolgen hebben voor de vitaliteit van de Nederlandse economie. De uitwerking van een dergelijk 'lek' is echter onzeker en ontvouwt zich over een lange termijn.[193]

Digitale risico's vergen bredere manier van beheersing

Al diverse jaren besteedt het CSBN aandacht aan het belang van risicomanagement om Nederland, sectoren en organisaties weerbaarder te maken tegen de digitale dreiging. Wel is het zo dat digitale risico's enkele bijzondere kenmerken hebben die een bredere manier van beheersing vragen dan andere risico's. Dat geldt op het niveau van organisaties, maar zeker op sectoraal en landelijk niveau. Gewezen is op de zes strategische thema's die specifiek voor digitale risico's ieder op zich en in samenhang complicaties vormen voor risicobeheersing. Digitale risico's maken verder deel uit van een breder, dynamisch én complex risicopalet. Ook geldt dat ten opzichte van andere risico's de digitale ruimte een uiterst complex systeem is. Informatie over cyberincidenten is weliswaar deels beschikbaar, maar lang niet voor iedereen. Het is onderling slechts in beperkte mate vergelijkbaar en lastig te interpreteren. Voor de beheersing van ongevallen met vliegtuigen of overstromingen is bijvoorbeeld veel meer informatie beschikbaar en over een langere periode. Het simuleren van incidenten of het bouwen van modellen om het verloop van incidenten en gevolgen in kaart te brengen, is behulpzaam voor risicomanagement. Voor digitale risico's is dat uiterst complex. En, het internet laat zich uiteraard niet een dag uitzetten om te kijken wat er gebeurt.

Nog een bijzonder kenmerk is dat op nationaal, sectoraal en organisatieniveau sprake is van een onvolledig beeld van de kosten en baten van investeringen in digitale weerbaarheid en van diverse onzekerheden.[194] Menigmaal is gebleken dat lang niet alle politici en bestuurders zich lijken bewust te zijn van digitale risico's. Toezichthouders signaleerden een vernauwing van scope bij risicomanagement. Door te veel te focussen op bepaalde soorten dreigingen, bijvoorbeeld criminele actoren, blijven andere risico's voor de continuïteit van dienstverlening on(der)belicht.[195] Wel leiden incidenten, zoals de ransomware-aanval op de Universiteit Maastricht in 2019 en die op de gemeente Hof van Twente in 2020 tot extra bewustwording en extra maatregelen door soortgelijke organisaties.

Digitale veiligheid is een enorme uitdaging voor gemeenten

Professor Bibi van den Berg stelt in dat kader: "*Zolang het goed gaat blijven de risico's abstract. Je weet gewoon niet precies wat er kan gebeuren, laat staan hoe je 'het' kunt voorkomen. En als je bepaalde maatregelen neemt, weet je vaak niet eens of ze helpen want die zitten digitaal verstopt in de techniek. In tegenstelling tot bijvoorbeeld een heel groot slot op de deur; dat kun je gewoon zien. Dat maakt het lastiger om de noodzaak tot investeren in digitale veiligheid te onderkennen. Het is best ingewikkeld om te bepalen of een bepaald incident zich niet voordoet omdat je een maatregel hebt getroffen of dat het gewoon toeval is. Ik kan me dus goed voorstellen dat je als gemeentebestuur zegt: dat geld besteden we liever aan het sociaal domein. Totdat het fout gaat en je geconfronteerd wordt met hoe enorm wijdvertakt digitale systemen zijn. En er ineens niks meer werkt.' [….] Bij een digitale inbraak zijn de daders soms al maanden binnen zonder dat je het merkt. En lang niet altijd zijn je digitale juwelen weg; stelen is in de digitale wereld vaak kopiëren. Dit maakt dat we anders na moeten denken over veiligheid dan we gewend waren bij fysieke veiligheid.*"[198]

Op welke wijze zouden digitale risico's (nog) beter te beheersen zijn? Hoewel CSBN niet bedoeld is om een handelingsperspectief te schetsen of maatregelen voor te stellen, hieronder een paar brede overwegingen.

Basismaatregelen blijken nog steeds een effectieve barrière te vormen tegen vele soorten cyberaanvallen. Microsoft stelt dat basismaatregelen beschermen tegen maar liefst 98% van de cyberaanvallen.[196] Het NCSC benoemt eveneens basismaatregelen die elke organisatie zou moeten treffen om cyberaanvallen tegen te gaan. Bij cyberincidenten ziet het NCSC dat organisaties kwetsbaar zijn als deze maatregelen niet genomen zijn. Hoogleraar Bibi van den Berg pleit onder andere voor het verhogen van de veerkracht van organisaties die te kampen hebben (gehad) met cyberincidenten en het opwerpen van barrières voor uiteenlopende cyberincidenten. Het segmenteren van netwerken is een voorbeeld van een barrière die kan helpen tegen diverse soorten incidenten.[197] Daar waar segmentering in gebouwen gebruikelijk is om de gevolgen van een eventuele brand te beheersen, is segmentering lang niet altijd gebruikelijk in de technische infrastructuur. Ook adequaat getrainde medewerkers en burgers vormen een barrière voor uiteenlopende cyberincidenten. Hoogleraar Jan van den Berg bepleit dan ook bijvoorbeeld het adequaat opleiden van mensen zodat zij in hun diverse rollen de juiste digitale activiteiten kunnen uitvoeren.

Uit de aard van het belang van digitale veiligheid en de aard van de digitale dreiging vloeit voort dat beheersing van digitale risico's zeker niet alleen een vraagstuk is voor technische experts. Het is ook, of wellicht vooral, een vraagstuk van governance en/of risicomanagement voor politici en bestuurders op het niveau van organisaties, sectoren en landen. Bovendien zijn digitale risico's een integraal onderdeel van een breder risicopalet en vragen ook daarom om integraal risicomanagement.

Als er één terrein is waarvoor geldt dat ervaringen uit het verleden geen garanties bieden voor de toekomst, is dat wel digitale veiligheid. Vandaar de oproep om breder te kijken dan incidenten die zich hebben voorgedaan en breder te kijken dan eisen waaraan moet worden voldaan. Dat geldt bijvoorbeeld voor het anticiperen op mogelijke gevolgen voor digitale veiligheid van technologische ontwikkelingen. Een andere invalshoek is die van 'assume breach', oftewel: ga ervan uit dat er al sprake is van een cyberincident.

Beperkingen in digitale autonomie beperken ook digitale weerbaarheid

Toelichting strategisch thema

Voor Europese landen en Nederland (verder Nederland) gelden beperkingen in digitale autonomie. Die autonomie omvat het vermogen en de middelen die Nederland heeft om zelfstandig beslissingen te kunnen nemen over (verdere) digitalisering én de gewenste mate van digitale weerbaarheid. Beperkingen in digitale autonomie brengen ook beperkingen voor weerbaarheid met zich mee. De autonomie staat onder druk door diverse oorzaken, die samenhangen met de andere strategische thema's. Die oorzaken verminderen de beïnvloedings- en keuzemogelijkheden voor en controle over de digitale weerbaarheid van Nederland.

Dit thema, zoals kort toegelicht in bovenstaand kader, is nog onverkort van toepassing.

Een storing in de watervoorziening kan ervoor zorgen dat er geen of weinig water uit de kraan komt. De grote vraag aan water uit de winkel zorgt voor lege schappen.

6 Dreigingsscenario's

In de voorgaande hoofdstukken werd aandacht besteed aan digitale dreigingen, en aan weerbaarheid en belangen die in het geding zijn wanneer cyberincidenten zich voordoen. Daarbij is gewezen op risico's die voortkomen uit het feit dat organisaties onderdeel zijn van een breder ecosysteem. Voor dit hoofdstuk hebben het Nationaal Cyber Security Centrum en het Digital Trust Center drie fictieve scenario's opgesteld waarbij een cyberincident in een ecosysteem niet alleen leidt tot problemen binnen de organisatie waar het incident zich voordoet, maar ook tot schade voor de maatschappij of andere organisaties in het ecosysteem. De schade van cyberincidenten beperkt zich niet alleen tot directe financiële schade, maar kan bijvoorbeeld ook gevaar opleveren voor medewerkers en de omgeving. De gevolgen van een cyberincident werken vaak lang door, met name als het vertrouwen in een organisatie is geschaad.

U kunt deze scenario's gebruiken om na te gaan hoe het gesteld is met de digitale weerbaarheid van uw organisatie, klanten en/of leveranciers. Informatie om meer grip te krijgen op digitale risico's vindt u op de websites van het DTC[IX] en het NCSC.[X]

De onderstaande scenario's zijn fictief. Iedere gelijkenis met bestaande producten, organisaties, personen of gebeurtenissen berust puur op toeval en is niet zo bedoeld.

IX Doe de Basisscan Cyberweerbaarheid van het Digital Trust Center: https://www.digitaltrustcenter.nl/tools/doe-de-basisscan-cyberweerbaarheid

X Lees de 'Factsheet Risico's beheersen: de waarde van informatie als uitgangspunt' van het Nationaal Cyber Security Centrum: https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing

Geen melk in de schappen

Beschrijving gebeurtenissen

Net voor een lang weekend begin maart 2022, krijgt de planning van transportbedrijf Negotium BV uit Zwolle meldingen van chauffeurs dat ze bij de verkeerde boerderij staan. Ook melden boeren dat hun melk niet wordt opgehaald. De planning zorgt er alsnog voor dat de lege auto's naar de 'vergeten' boeren gaan. Probleem opgelost. De planning geniet van het lange weekend. Op dinsdagochtend opent de planning de mailbox: die zit vol. Vanaf 7 uur gaat de telefoon. Tankwagens staan verkeerd en boeren zijn gedwongen melk te lozen doordat hun opslagcapaciteit vol is. De melkfabrieken hangen aan de lijn. Hun voorraden voor het maken van dagverse melk zijn bijna op doordat er geen melk meer wordt aangeleverd.

De IT afdeling van Negotium BV start een onderzoek. Het probleem blijkt in het planningssysteem te zitten. Dit systeem is verouderd en er is al 2 jaar geen update meer geleverd. De directeur moet de leverancier Aedificium BV bellen om op locatie te komen. Aedificium BV heeft alleen een groter probleem. Zij worden overspoeld met vragen want hun pakket wordt bij meer transporteurs gebruikt en werkt ook daar niet goed.

De oorzaak blijkt, na dagen onderzoek, te zitten in een veelgebruikte library die zorgt voor het vastleggen van informatie vanuit de gebruikerszijde in de database. De ingevoerde data na 22-02-2022 blijkt onbetrouwbaar. De library kan niet correct omgaan met data na deze datumnotatie en registreert dus afspraken niet op de juiste manier.

Inmiddels is er geen verse melk meer in de schappen. Ook bestaan er zorgen over de kwaliteit van het oppervlaktewater doordat boeren hun melk lozen of aangeven dat te gaan doen. Negotium BV kan weliswaar handmatig vrachtwagens plannen en sturen, maar de melkfabriek mag de melk zonder de volledige elektronische registratie niet accepteren van de toezichthouder. De schappen voor dagverse melk blijven daardoor nog wel even leeg. Ook de productie van andere zuivelproducten ligt stil. Er is een run op houdbare producten. Het duurt nog weken voordat de supermarkten weer regulier bevoorraad kunnen worden met verse melk en zuivel. Negotium BV en alle andere klanten van Aedificium BV gaan een nieuw planningssysteem gebruiken. Dit kan alleen niet iedereen tegelijk. Het duurt langer dan gedacht voordat iedereen over is en er weer goed gepland kan worden.

Duiding

Als het niet kapot is, blijf er dan vanaf. Een waarheid die vroeger werkte, maar zeker niet geldt voor veel soft- en hardware. Dagelijks worden daarin fouten ontdekt. Niet alleen in de programmatuur of systemen zelf, maar juist ook in de onderliggende componenten. Toch zijn niet alle bedrijven en organisaties bekend met de risico's van het gebruik van verouderde soft- en hardware. Ook is organisaties vaak niet bekend welke systemen zij gebruiken en welke software-onderdelen daarin zijn verwerkt. Het gebeurt zelfs dat de verstoring van primaire processen, zeker in 24/7 bedrijfsvoering, dermate impact heeft dat de gehele bedrijfsvoering stopt. Dit kan dus grote consequenties hebben. Mocht dit gebeuren dan is het in zo'n situatie lastig uit te zoeken waarom een fout optreedt, waar die optreedt en hoe deze hersteld kan worden. Daarnaast kunnen dit soort fouten niet alleen directe impact hebben op het bedrijf zelf, maar ook op de keten waarmee het digitaal is verbonden. Ook kan het gevolgen krijgen in de fysieke wereld, zoals in dit geval voor zuivelproducten in de schappen.

Kernvragen voor de lezer

1. Weet u welke soft- en hardware u in huis heeft?
2. Weet u of al uw soft- en hardware en onderliggende onderdelen up-to-date zijn?
3. Heeft u een continuïteitsplan als de IT-ondersteuning van uw primaire proces stokt? En wanneer heeft u dat voor het laatst getest?
4. Welke ondersteuningsafspraken heeft u gemaakt met uw leveranciers van IT, soft- en hardware?
5. Hoe goed kent u uw keten en heeft u inzicht in de gezamenlijke risico's als er een schakel bij uw leveranciers, dienstverleners of afnemers in de keten gecompromitteerd wordt en hoe zijn de verantwoordelijkheden en bevoegdheden geregeld als een incident zich voordoet?

Niet zo slim, die apparaten

Beschrijving gebeurtenissen

Op maandagochtend belt een cliënt met notariskantoor M.M. Katz. Het gaat over een afspraak die gepland staat voor het tekenen van een koopakte voor een grote loods op een beschutte locatie op een half uurtje rijden van de Maasvlakte. Er klinkt een combinatie van angst en woede in de stem van de cliënt.

De avond daarvoor is hij thuis bezocht door twee onbekende en gewapende personen. Ze hadden een kopie van zijn paspoort in de hand om zeker te weten dat ze de juiste persoon zouden bedreigen. Een groep criminelen had namelijk de zinnen gezet op de loods om deze te gebruiken voor illegale praktijken. De cliënt werd gedwongen om als dekmantel te fungeren door de loods op zijn naam te hebben staan en zou daarvoor wat zwijggeld ontvangen. En als hij niet zou gehoorzamen, dan zou dat 'doodzonde' zijn volgens de bedreigers, want dit was geen kinderspel.

Op maandagochtend belt de cliënt toch met de notaris. De woede in zijn stem komt door de overtuiging dat zijn gegevens gelekt zijn via de notaris. De notaris schrikt en zegt digitaal forensisch onderzoek te laten doen.

Het onderzoek wijst uit dat criminelen al langere tijd vertrouwelijke gegevens van de notaris hebben kunnen inzien en dossiers hebben gekopieerd en gedownload. Dit konden ze doen omdat ze toegang tot een beheeraccount op het netwerk hadden bemachtigd. Met een Single Sign-On-systeem kon de notaris eenvoudig inloggen om verschillende belangrijke bronnen te raadplegen, zoals de registers van het Kadaster en de Kamer van Koophandel. Dit Single Sign-On-systeem bleek niet weerbaar tegen een aanval en gaf het wachtwoord van een beheeraccount prijs.

De eerste stap in deze aanval was om überhaupt verbinding te maken met het bedrijfsnetwerk. Een met het internet verbonden slimme thermosstaat bleek de zwakke schakel te zijn. De notaris had deze in het kantoor geïnstalleerd om energie te besparen. Een bezoekende hacker trof het apparaatje aan in een onbewaakte ontvangstruimte en was in staat deze te manipuleren, zodat de thermosstaat op afstand toegang gaf tot het netwerk van de notaris.

De onderzoekers konden niet uitsluiten dat deze aanval is overgesprongen naar andere onderdelen van de notariële keten. En zo niet, dan zou het alsnog herhaalbaar zijn bij andere kantoren. De notaris besluit toch aangifte te doen en waarschuwt ook haar ambtgenoten.

Duiding

In deze aanval is de vertrouwelijkheid van een bedrijfsnetwerk geschaad en dat heeft serieuze gevolgen voor de notaris en haar cliënten. Het incident kan ook doorwerken naar landelijke bestanden, doordat daarin onjuiste (gemanipuleerde) informatie kan worden geplaatst. Van eventueel gemanipuleerde informatie kan een kwaadwillende verder misbruik maken en ook anderen ondervinden de gevolgen daarvan. In een uiterst geval, wanneer misbruik op grote schaal zou plaatsvinden, kan het zelfs leiden tot aantasting van het vertrouwen in een beroepsgroep en/of van landelijke registraties. Alledaagse informatie voor de ene organisatie, kan dus in verkeerde handen grote waarde hebben en dient adequaat beveiligd te worden. De zwakste schakel bepaalt uiteindelijk de sterkte van het geheel. Organisaties kunnen digitale incidenten voorkomen of tijdig detecteren door het treffen van basismaatregelen.

Uit het voorbeeld van de notaris worden de risico's duidelijk van een smart device, hier in de vorm van een thermosstaat, dat is verbonden met het bedrijfsnetwerk, zonder het netwerk te scheiden of te segmenteren van bedrijfskritische systemen en applicaties. Voor het beheeraccount was geen multifactor authenticatie vereist dus voor de hackers was een wachtwoord voldoende om controle te hebben. Dankzij log-informatie waren forensisch onderzoekers in staat de aanval te ontleden. Organisaties kunnen met behulp van loginformatie een digitale inbraak eerder detecteren om schade te voorkomen.

Kernvragen voor de lezer

1. Weet u welke apparaten op uw bedrijfsnetwerk zijn aangesloten, en of deze aan uw beveiligingsstandaarden voldoen? Houdt u toezicht op nieuw aangesloten apparaten?
2. Welke maatregelen heeft u getroffen om mobiele apparaten en *smart devices* van medewerkers en bezoekers die gebruik maken van wifi te scheiden van het netwerkverkeer van beheerde apparaten?
3. Heeft u in beeld welke organisatieprocessen en data van bijzondere waarde kunnen zijn voor (georganiseerde) criminelen, statelijke actoren of hacktivisten?
4. Heeft u zelf monitoring- en detectiecapaciteit beschikbaar of ingekocht als dienst? Bent u bekend wat er precies gemonitord wordt en welke type dreigingen hiermee wel en niet worden gedetecteerd?
5. Bent u bekend met of gebruikt u een *assume breach* strategie? In andere woorden: indien ervan uitgegaan wordt dat uw organisatie een keer te maken kan krijgen met een cyberincident, wat is dan uw handelingsperspectief?
6. Heeft u wel eens nagedacht welk bedrijf u zou kunnen inschakelen wanneer zich een cyberincident bij u voordoet en heeft u dan ook het bedrijf benaderd voor het geval dat?

Hack door hacktivisten tijdens staking

Beschrijving gebeurtenissen

Een doordeweekse dag, maar in de fabriekshal van BIV Plastics is niemand te vinden. Dit middelgrote bedrijf produceert kunststoffen met kritische toepassingen voor onder andere de lucht- en ruimtevaart en raffinaderijen. Medewerker Wim is echter het meest trots op de dagelijkse levering van medische verpakkingen voor ziekenhuizen in de regio. Maar vandaag even niet. Er wordt namelijk gestaakt. Na geruime tijd onderhandelen over een nieuwe CAO zijn de gesprekken vastgelopen en daarop hebben de werknemers het werk neergelegd.

Devon is de zoon van Wim. Thuis spreken ze over de frustraties van het werk en de stijgende inflatie. Zelf is Devon ook gefrustreerd door het bedrijf waar zijn vader werkt. Hij heeft zich aangesloten bij een groepering van milieuactivisten en is bang dat de productie van BIV Plastics schadelijk is voor mens en omgeving. Als het aan hem ligt blijft de fabriek langer dicht. Naast milieubescherming heeft Devon nog een nieuwe passie ontdekt: hacken. Hoewel hij nog niet zijn eigen codes kan ontwikkelen, heeft hij al wel snel geleerd om toegankelijke, kant-en-klare hacktools te vinden en gebruiken.

De gedachte was al eerder bij Devon opgekomen, maar als zijn vader thuiskomt van weer een dag staken zonder doorbraak, besluit hij actie te ondernemen. Hij gaat digitaal rondneuzen bij de plasticfabriek. Met de speciale zoekmachine Shodan ontdekt hij dat verschillende apparaten van BIV Plastics verbonden zijn met het internet. Hij vindt zelfs enkele sensoren die als operationele techniek (OT) het productieproces begeleiden. Omdat hij niet weet wat er precies gebeurt als hij aan de sensoren gaat knoeien, zoekt hij verder naar een meer publiek zichtbaar systeem.

Hij vindt een ander doelwit. De software die het mogelijk maakt de website te beheren en informatie daarop te plaatsen, het Content Management System (CMS), blijkt niet up-to-date. Devon weet met zijn tools de toegang te kraken. Ook raadt hij eenvoudig de gebruikersnaam en het wachtwoord die toegang geeft tot het portaal van de webhoster (admin, BIV12345). Eenmaal in het CMS besluit hij de website te defacen, oftewel digitaal te bekladden. Op de voorpagina staat groot de slogan van zijn groepering: ‘People & PLANET’ en een dikke streep door ‘Profit’. Via sociale media verspreidt de actiegroep razendsnel hun actie. Ook verandert Devon de wachtwoorden voor toegang tot de webhoster en die van de e-mailadressen. Na 24 uur weet BIV Plastics de website offline te halen en weer toegang te krijgen tot de webhoster. Het zal tot na het einde van de staking duren voordat de website weer in oude staat is hersteld. Verrast door het gemakkelijke succes van Devon weten mede-activisten in de weken daarna de defacement te herhalen bij websites van andere bedrijven die zij vervuilend vinden.

Duiding

Een website is meer dan een visitekaartje. Het is vaak ook een platform om bestellingen aan te nemen en diensten te leveren, en kan op verschillende manieren worden gehackt. In dit scenario heeft een persoon met een activistisch motief en met gratis en gemakkelijk te gebruiken aanvalsmiddelen schade aan weten te richten. In dit geval ook nog eens op een kwetsbaar moment.

Het had ook anders kunnen aflopen. Een aanvaller met een ander motief en meer ervaring had mogelijk ook de productielijn kunnen saboteren met alle gevolgen van dien, of verder misbruik kunnen maken van de toegang bij de webhoster. En wat als de aanval niet van buitenaf, maar van binnenuit was gekomen? Had Devon via de werklaptop van Wim, of een medewerker vanuit de fabriek, ook andere systemen kunnen aanvallen?

Kernvragen voor de lezer

1. Weet u welke systemen van uw organisatie via het internet te benaderen zijn?
2. Hoe beheert u tot welke systemen verschillende medewerkers toegang hebben, en kunt u die toegang ook adequaat aanpassen bij het veranderen of het beëindigen van de functie? Registreert u ook de activiteiten van medewerkers op de systemen?
3. Welke controles toetsen het correct functioneren van uw systemen en OT-apparatuur (zoals sensoren)?
4. Heeft u in uw continuïteitsplan ook een communicatieplan opgenomen als u geen toegang heeft tot uw officiële communicatiekanalen?
5. Weet u welke verplichtingen u heeft wanneer zich een cyberincident voordoet vanwege regelgeving en verzekeraars? Weet u hoe u aangifte kunt doen bij de politie?

Bijlage 1

Verantwoording totstandkoming

Het Cybersecuritybeeld Nederland is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en het Nationaal Cyber Security Centrum (NCSC). Het wordt jaarlijks door de NCTV vastgesteld. Daarbij wordt dankbaar gebruik gemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, organisaties in vitale processen, de wetenschap en andere partijen. De totstandkoming van het CSBN kent drie fasen:

1. Analyseren

De NCTV verzamelt en analyseert relevante informatie over incidenten, trends en verschuivingen op het gebied van de driehoek belang, dreiging en weerbaarheid. De volgende vragen liggen ten grondslag aan het CSBN:

1. Welke relevante incidenten hebben in de periode 1 maart 2022 t/m februari 2023 in Nederland plaatsgehad? Om welk type incidenten gaat het? Waardoor zijn ze veroorzaakt en welke schade/impact hebben ze gehad?

2. Welke gebeurtenissen, ontwikkelingen of inzichten zijn van invloed op de strategische thema's zoals geïdentificeerd in CSBN 2022 en welke invloed gaat daarvan uit?

3. Welke veranderingen zijn te identificeren die van invloed zijn op belangen die kunnen worden aangetast wanneer cyberincidenten zich voordoen en wat kan de impact daarvan zijn?

4. Welke veranderingen zijn te identificeren die van invloed kunnen zijn op digitale dreigingen die de nationale veiligheid aantasten?

5. Welke veranderingen zijn te identificeren in de mate waarin Nederland weerbaar is tegen die digitale dreigingen?

6. In hoeverre treden veranderingen op in de grootste risico's voor de nationale veiligheid van Nederland?

In de analysefase zijn analisten van de NCTV aan de gang gegaan met deze vragen en heeft een eerste inventarisatie plaatsgevonden van 'ingrediënten' voor het CSBN. Ook zijn enkele mogelijke thema's geïdentificeerd voor de themahoofdstukken. De resultaten zijn aan externe overheidspartners en collega's van het NCSC voorgelegd, besproken en aangevuld. Op basis hiervan is gekozen voor een afzonderlijk themahoofdstuk over operationele technologie (hoofdstuk 4) en over de Russische oorlog tegen Oekraïne (hoofdstuk 3).

2. Schrijven en collegiaal toetsen

Na afronding van de analysefase zijn concepthoofdstukken geschreven door afzonderlijke (teams van) auteurs.

Kernbeeld	NCTV
Hoofdstuk 1	NCTV
Hoofdstuk 2	NCTV en NCSC
Hoofdstuk 3	NCTV
Hoofdstuk 4	NCSC
Hoofdstuk 5	NCTV, met aanvulling van de politie wat betreft ransomware en 'digitale ecosystemen vormt gelegenheidsstructuur voor cyberaanvallen'
Hoofdstuk 6	NCSC samen met DTC
Verantwoording	NCTV

De gehele tekst wordt binnen de NCTV en het NCSC meerdere keren collegiaal getoetst. Enkele concepthoofdstukken zijn ook tussentijds getoetst. Alle hoofdstukken komen tot stand onder redactionele eindverantwoordelijkheid van de NCTV.

3. Valideren

Het CSBN kent een uitgebreid validatietraject, waarbij de concepttekst voorgelegd wordt aan externe partners ter commentaar. Na het verwerken van het verzamelde commentaar wordt de definitieve tekst opgemaakt en door de NCTV vastgesteld. Na de publicatie van het CSBN vindt een evaluatie plaats. De verzamelde feedback wordt vervolgens verwerkt in het CSBN-traject van het volgende jaar.

Bijlage 2

Bronnen en referenties

1 Sinds het CSBN2021 wordt een herzien begrippenkader gehanteerd, waar bij de totstandkoming dankbaar gebruik is gemaakt van: J. van den Berg, 'A basic set of mental models for understanding and dealing with the cybersecurity challenges of today', Journal of Information Warfare 19:1 (2020). https://repository.tudelft.nl/islandora/object/uuid%3A41a590a2-e11b-4ad3-b5aa-f3e51b2b7313

2 'Grote treinstoring opnieuw veroorzaakt door falend back-upsysteem ProRail', Security.nl, 02-08-2022, https://www.security.nl/posting/763403/Grote+treinstoring+opnieuw+veroorzaakt+door+falend+back-upsysteem+ProRail

3 'Rapport: Europese landen bespioneren burgers maar zijn daar niet open over', Nu.nl, 08-11-2022, https://www.nu.nl/tech/6234738/rapport-europese-landen-bespioneren-burgers-maar-zijn-daar-niet-open-over.html

4 'An Overview of the Increasing Wiper Malware Threat', Fortinet, 28-04-2022, https://www.fortinet.com/blog/threat-research/the-increasing-wiper-malware-threat

5 'The Year of the Wiper', Fortinet, 24-01-2023, https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper

6 'SwiftSlicer: New destructive wiper malware strikes Ukraine', ESET, 27-01-2023, https://www.welivesecurity.com/2023/01/27/swiftslicer-new-destructive-wiper-malware-ukraine/

7 'Fantasy – a new Agrius wiper deployed through a supply-chain attack', ESET, 7-12-2022, https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/

8 'LokiLocker ransomware family spotted with built-in wiper', The Register, 16-03-2022, https://www.theregister.com/2022/03/16/blackberry_lokilocker_ransomware/

9 'Hackers Targeted U.S. LNG Producers in Run-Up to Ukraine War', Bloomberg, 07-03-2022, https://www.bloomberg.com/news/articles/2022-03-07/hackers-targeted-u-s-lng-producers-in-run-up-to-war-in-ukraine

10 'Bug in software van Alstom leidt tot problemen op het spoor', Executive People, 18-03-2022, https://executive-people.nl/693857/bug-in-software-van-alstom-leidt-tot-problemen-op-het-spoor.html 'Outage disrupts Polish trains as Ukrainian refugees head west', Reuters, 17-03-2022, https://www.reuters.com/world/europe/technical-fault-halts-polish-railways-key-ukraine-exit-route-2022-03-17/

11 'Datalek bij woningcorporaties na ransomware-aanval op ict-dienstverlener', Security.nl, 06-04-2022, https://www.security.nl/posting/749309/Datalek+bij+woningcorporaties+na+ransomware-aanval+op+ict-dienstverlener

12 'Breaking! Black Byte Ransoming 11.000 PDF Scans Of GEBE St Maarten Customers, Internal Powerplant Operations, Technical Scans And Financial BAU records', St Maarten News, 30-03-2022, https://stmaartennews.org/breaking-black-byte-ransoming-11-000-pdf-scans-of-gebe-st-maarten-customers-internal-powerplant-operations-technical-scans-and-financial-bau-records/

'GEBE investigating cyberattack, says efforts focused on minimising impact', The Daily Herald, 31-03-2022, https://www.thedailyherald.sx/islands/gebe-investigating-cyberattack-says-efforts-focused-on-minimising-impact

13 'Nederlandse windmolens konden door ransomware-aanval niet proefdraaien', Security.nl, 17-08-2022, https://www.security.nl/posting/764826/Nederlandse+windmolens+konden+door+ransomware-aanval+niet+proefdraaien 'Nordex Group impacted by cyber security incident', Nordex Online, 02-04-2022, https://www.nordex-online.com/en/2022/04/nordex-group-impacted-by-cyber-security-incident/ 'Antwoord op vragen van het lid Eerdmans over het hacken van windturbines', Tweede Kamer, 16-08-2022, https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2022Z13483&did=2022D32554

14 'ESET onderzoek: Lazarus valt wereldwijd lucht-, ruimtevaart- en defensiebedrijven aan via LinkedIn en WhatsApp', ESET, 01-06-2022, https://www.eset.com/nl/over/newsroom/persberichten-overzicht/persberichten/lazarus-valt-wereldwijd-aan/

'Noord-Koreaanse hackers keken mee in systemen van Nederlands defensiebedrijf', Nu.nl, 01-06-2022, https://www.nu.nl/tech/6204153/noord-koreaanse-hackers-keken-mee-in-systemen-van-nederlands-defensiebedrijf.html#coral_talk_wrapper

'Noord-Koreaanse hackers vielen Nederlands defensiebedrijf binnen', Techzine, 01-06-2022, https://www.techzine.nl/nieuws/security/490085/noord-koreaanse-hackers-vielen-nederlands-defensiebedrijf-binnen/.

15 'I-SEC attacked by Conti threat actors', DataBreaches.net, 05-04-2022, https://www.databreaches.net/i-sec-attacked-by-conti-threat-actors/

'Persoonsgegevens gelekt bij Schiphol-beveiligingsbedrijf I-SEC', Nu.nl, 03-05-2022, https://www.nu.nl/tech/6198666/persoonsgegevens-gelekt-bij-schiphol-beveiligingsbedrijf-i-sec.html

16 'Bestanden van Gelderse gemeenten staan op darkweb na ransomwareaanval', Tweakers, 21-04-2022, https://tweakers.net/nieuws/195868/bestanden-van-gelderse-gemeenten-staan-op-darkweb-na-ransomwareaanval.html

'Datadiefstal gemeente Buren', Gemeente Buren, 08-07-2022, https://www.buren.nl/nieuws/gegevens-aangeboden-op-het-darkweb/7399/

17 'Datalek gemeente Veenendaal door technische handeling softwareleverancier', Security.nl, 23-06-2022, https://www.security.nl/posting/758076/Datalek+gemeente+Veenendaal+door+technische+handeling+softwareleverancier

'Persbericht: Onderzoek naar datalek raadsinformatiesysteem afgerond', Gemeente Veenendaal, 21-06-2022, https://veenendaal.raadsinformatie.nl/document/11618256/1/PERS2022_33+-+Onderzoek+-naar+datalek+raadsinformatiesysteem+afgerond

'Datalek gemeente Veenendaal veroorzaakt door menselijke fout', VPNGids, 23-06-2022, https://www.vpngids.nl/nieuws/datalek-gemeente-veenendaal-veroorzaakt-door-menselijke-fout/

18 'Artis getroffen door ransomware: hackers eisen 1 miljoen losgeld', RTL Nieuws, 28-06-2022, https://www.rtlnieuws.nl/tech/artikel/5317902/artis-dierentuin-hackers

'ARTIS doelwit van cyberaanval', ARTIS, 28-06-2022, https://www.artis.nl/nl/ontdek/nieuws/2022/06/28/ARTIS-doelwit-cyberaanval/

'Artis betaalde hackers geen miljoen euro aan cryptovaluta', Het Parool, 18-07-2022, https://www.parool.nl/amsterdam/artis-betaalde-hackers-geen-miljoen-euro-aan-cryptovaluta~bee568of/

19 'Ransomware-aanval in Noordenveld: mogelijk gevolgen voor afhandeling bijstandsuitkeringen', RTV Drenthe, 29-07-2022, https://www.rtvdrenthe.nl/nieuws/14848823/ransomware-aanval-in-noordenveld-mogelijk-gevolgen-voor-afhandeling-bijstandsuitkeringen

'Gemeente Noordenveld getroffen door ransomware-aanval', Security.nl, 01-08-2022, https://www.security.nl/posting/763248/Gemeente+Noordenveld+getroffen+door+ransomware-aanval

20 'Grote treinstoring opnieuw veroorzaakt door falend back-upsysteem ProRail', Security.nl, 02-08-2022, https://www.security.nl/posting/763403/Grote+treinstoring+opnieuw+veroorzaakt+door+-falend+back-upsysteem+ProRail

'ProRail opnieuw geconfronteerd met falende back-up tijdens ICT-storing', SpoorPro, 01-08-2022, https://www.spoorpro.nl/spoorbouw/2022/08/01/prorail-opnieuw-geconfronteerd-met-falende-back-up-tijdens-ict-storing/?gdpr=deny

21 'Informatiepagina cyberincident augustus 2022, Colosseum Dental, 08-08-2022, https://www.colosseumdental.nl/mededeling-cyberincident

'Meer dan 100 tandartspraktijken dagen dicht door cyberaanval', RTL Nieuws, 05-08-2022, https://www.rtlnieuws.nl/economie/bedrijven/artikel/5325232/meer-dan-100-tandartspraktijken-dicht-door-cyberaanval

22 'Hackers vallen softwareleverancier van vijf Limburgse gemeenten aan', Tweakers, 17-08-2022, https://tweakers.net/nieuws/200002/hackers-vallen-softwareleverancier-van-vijf-limburgse-gemeenten-aan.html

'Vijf Limburgse gemeenten getroffen door hack', Binnenlands Bestuur, 17-08-2022, https://www.binnenlandsbestuur.nl/digitaal/vijf-gemeenten-limburg-getroffen-door-cyberhack

23 'informatie over het herstellen van onze diensten na de cyberaanval op ista.', Ista, 29-07-2022, https://www.ista.com/nl/updates

'Woningcorporaties melden datalek na cyberaanval op energiedienstverlener ista', Security.nl, 04-08-2022, https://www.security.nl/posting/763659/Woningcorporaties+melden+datalek+na+cyberaanval+op+energiedienstverlener+ista

'Bij ista gestolen privédata van 146.000 mensen op internet gepubliceerd', Security.nl, 25-08-2022, https://www.security.nl/posting/765725/Bij+ista+gestolen+priv%C3%A9data+van+146_000+mensen+op+internet+gepubliceerd

'UPDATE: Geen datalek bij ISTA Nederland. Gegevens van gebruikers zijn veilig', Havensteder, 23-08-2022, https://www.havensteder.nl/nieuws/2981/ista-een-leverancier-van-havensteder-is-getroffen-door-een-cyberaanval

24 'Grote storing Maastricht UMC+: afspraken poli's afgezegd', 1Limburg, 08-09-2022, https://www.1limburg.nl/nieuws/1839619/grote-storing-maastricht-umc-afspraken-polis-afgezegd

'Technische oorzaak IT-storing', Maastrict UMC+, 20-09-2022, https://www.mumc.nl/actueel/nieuws/technische-oorzaak-it-storing

25 'DigiD was urenlang beperkt beschikbaar vanwege ddos-aanvallen', Nu.nl, 12-09-2022, https://www.nu.nl/tech/6223663/digid-was-urenlang-beperkt-beschikbaar-vanwege-ddos-aanvallen.html

26 'Incident Statement @ ID-ware', ID-ware, n.d., https://www.id-ware.com/en/about/news/incident-statement.html

'Gegevens van toegangspassen Tweede Kamerleden gelekt door hack', NOS, 07-10-2022, https://nos.nl/artikel/2447439-gegevens-van-toegangspassen-tweede-kamerleden-gelekt-door-hack

'High Tech Campus slachtoffer van hack bij leverancier toegangspassen', Omroep Brabant, 15-10-2022, https://www.omroepbrabant.nl/nieuws/4164616/high-tech-campus-slachtoffer-van-hack-bij-leverancier-toegangspassen

'Adresgegevens duizenden studenten TU Eindhoven liggen op straat na hack', Nu.nl, 20-10-2022, https://www.nu.nl/tech/6231140/adresgegevens-duizenden-studenten-tu-eindhoven-liggen-op-straat-na-hack.html

'Privégegevens personeel Hogeschool Utrecht op darkweb na hack', RTV Utrecht, 20-10-2022, https://www.rtvutrecht.nl/nieuws/3487233/privegegevens-personeel-hogeschool-utrecht-op-darkweb-na-hack

'Data Kamerleden gelekt door hack bij ict-bedrijf: gegevens toegangspassen online', De Volkskrant, 07-10-2022, https://www.volkskrant.nl/nieuws-achtergrond/data-kamerleden-gelekt-door-hack-bij-ict-bedrijf-gegevens-toegangspassen-online~b7051db9/

27 'Nederlands vaccinbedrijf Bilthoven Biologicals getroffen door ransomware', Security.nl, 11-11-2022, https://www.security.nl/posting/774235/Nederlands+vaccinbedrijf+Bilthoven+Biologicals+getroffen+door+ransomware

'Nederlands vaccinbedrijf gehackt, gestolen data op dark web', RTL Nieuws, 11-11-2022, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5345841/vaccinbedrijf-ransomware-bilthoven-biologicals

'Ransomware bij vaccinmaker in Bilthoven, onderzoeksdata gestolen', NOS, 11-11-2022, https://nos.nl/artikel/2452020-ransomware-bij-vaccinmaker-in-bilthoven-onderzoeksdata-gestolen

28 'Landelijke politienummers moeilijk of zelfs niet bereikbaar door storing', Nu.nl, 18-10-2022, https://www.nu.nl/tech/6230635/landelijke-politienummers-moeilijk-of-zelfs-niet-bereikbaar-door-storing.html

'Politienummer moeilijk bereikbaar door landelijke storing: 'Bij tips over Amber Alert kan je 112 bellen'', Noordhollands Dagblad, 18-10-2022, https://www.noordhollandsdagblad.nl/cnt/dmf20221018_48887529

29 'Hacker (19) maakt tienduizenden zorgdossiers buit bij digitale inbraak Nedap Groenlo', De Gelderlander, 25-10-2022, https://www.gelderlander.nl/achterhoek/hacker-19-maakt-tienduizenden-zorgdossiers-buit-bij-digitale-inbraak-nedap-groenlo~ab723a6a/

'Zorginstellingen melden datalek na inbraak bij digitaal zorgplatform Carenzorgt', Security.nl, 02-11-2022, https://www.security.nl/posting/773253/Zorginstellingen+melden+datalek+na+inbraak+bij+digitaal+zorgplatform+Carenzorgt

'Kwetsbaarheid in Carenzorgt', Carenzorgt, n.d., https://carenzorgt.freshdesk.com/support/solutions/articles/75000112826-kwetsbaarheid-in-carenzorgt

'Zorginstellingen melden datalek na diefstal van documenten bij Carenzorgt', Opgelicht!? – AVROTROS, 03-11-2022, https://opgelicht.avrotros.nl/alerts/artikel/zorginstellingen-melden-datalek-na-hack-bij-carenzorgt/

30 'Grote ict-storing Pantar waarschijnlijk door inbraak op systeem', Security.nl, 04-12-2022, https://www.security.nl/posting/776668/Grote+ict-storing+Pantar+waarschijnlijk+door+inbraak+op+systeem

'ICT-storing Stichting Panta', Raad van Toezicht Stichting Pantar Amsterdam, 02-12-2022, https://amsterdam.raadsinformatie.nl/document/12138703/1/2022-12-02_brief_ICT_storing_Pantar_brief_-_RvT_aan_Wth_RGW

'Vragen en antwoorden – Hack bij Pantar', Pantar, 22-12-2022, https://pantar.nl/hack/

31 'Datalek Caiway en Delta raakt waarschijnlijk tienduizenden klanten', Security.nl, 06-12-2022, https://www.security.nl/posting/777008/Datalek+Caiway+en+Delta+raakt+waarschijnlijk+tienduizenden+klanten

'Data theft at DELTA Mobile and Caiway Mobile', Deltafiber, 06-12-2022, https://www.deltafiber.nl/en/news/data-theft-at-delta-mobile-and-caiway-mobile/

'Datadiefstal bij DELTA Mobiel', Delta, n.d., https://www.delta.nl/klantenservice/datadiefstal/

32 'Cyberaanval veroorzaakt problemen bij groothandel Makro', Nu.nl, 08-12-2022, https://www.nu.nl/tech/6241024/cyberaanval-veroorzaakt-problemen-bij-groothandel-makro.html

'@MakroNederland', Twitter, 08-12-2022, https://twitter.com/MakroNederland/status/1600781020793634816

33 'Leids UMC was ook doelwit van ddos-aanval', AD, 31-01-2023, https://www.ad.nl/leiden/leids-umc-was-ook-doelwit-van-ddos-aanval~a5b6ae2c

34 'Ook Maastricht UMC en instantie Z-CERT doelwit van pro-Russische cyberaanval', AD, 31-01-2023, https://www.ad.nl/maastricht/ook-maastricht-umc-en-instantie-z-cert-doelwit-van-pro-russische-cyberaanval~a0b1aae3

35 'DDoS-aanval op websites UMCG duurt voort, verschillende diensten uit de lucht', RTV Noord, 28-01-2022, https://www.rtvnoord.nl/nieuws/993500/ddos-aanval-op-websites-umcg-duurt-voort-verschillende-diensten-uit-de-lucht-update

36 'Russische DDOS-aanvallers vallen Nederlandse ziekenhuizen aan', NOS Nieuws, 30-01-2022, https://nos.nl/artikel/2461833-russische-ddos-aanvallers-vallen-nederlandse-ziekenhuizen-aan

37 'Weekend met DDoS aanvallen op Nederlandse cyberspace en ESXi kwetsbaarheid', Emerce, 06-02-2023, https://www.emerce.nl/wire/weekend-ddos-aanvallen-nederlandse-cyberspace-esxi-kwetsbaarheid

'Your banks are unable to transact. If you do not respect the Quran, we will not respect you. https://regiobank.nl - down @RegioBank #opholland #holland #bank #cyberattack #botnet #breaking #news #breakingnews #cyber #hack #hacker #hacking #hacked #banking #database #security', @thtghostkiller, 13-02-2023, https://twitter.com/thtghostkiller/status/1625225884075433984

38 'How the French fiber optic cable attacks accentuate critical infrastructure vulnerabilities', Cyberscoop, 28-04-2022, https://cyberscoop.com/french-fiber-optic-cables-attack-critical-infrastructure/

39 'Pegasus spyware targets top Catalan politicians and activists', Politico, 18-04-2022, https://www.politico.eu/article/pegasus-spyware-targets-top-catalan-politicians-and-activists/

40 'Spanish prime minister's phone 'targeted with Pegasus spyware'', The Guardian, 02-05-2022, https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware

41 Costa Rica declares state of emergency over ransomware attack, NBC News, 11-05-2022, https://www.nbcnews.com/tech/tech-news/costa-rica-declares-state-emergency-ransomware-attack-rcna28415

42 'Polish officials found to be targeted with Israeli NSO group's spyware', Times of Israel, 08-07-2022, https://www.timesofisrael.com/polish-officials-found-to-be-targeted-with-israeli-nso-groups-spyware/

43 'Albania shuts down government websites, services due to wide ranging cyberattack', The Record, 18-07-2022, https://therecord.media/albania-shuts-down-government-websites-services-due-to-wide-ranging-cyberattack/

'Albania severs diplomatic ties with Iran over cyber-attack', BBC News, 07-09-2022, https://www.bbc.com/news/world-europe-62821757

44 EU Commission alarmed by new spyware case against Greek socialist leader, Euractiv, 27-07-2022, https://www.euractiv.com/section/politics/news/eu-commission-alarmed-by-new-spyware-case-against-greek-socialist-leader/

45 'BlackCat ransomware claims attack on European gas pipeline', Bleepingcomputer, 01-08-2022, https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-european-gas-pipeline/

46 'Another European nation hit by hackers, Montenegro grapples with ongoing ransomware attack', Cyberscoop, 02-09-2022, https://cyberscoop.com/montenegro-ransomware-attack/

47 'Bosnia and Herzegovina investigating alleged ransomware attack on parliament', The Record, 19-09-2022, https://therecord.media/bosnia-and-herzegovina-investigating-alleged-ransomware-attack-on-parliament/

48 'Major German energy supplier hit by cyberattack', The Record, 27-10-2022, https://therecord.media/major-german-energy-supplier-hit-by-cyberattack/

49 'European Parliament website hit by cyberattack after Russian terrorism vote', Politico, 23-11-2022, https://www.politico.eu/article/cyber-attack-european-parliament-website-after-russian-terrorism/

'Russische hackers claimen aanval op Europees Parlement', Computable, 24-11-2022, https://www.computable.nl/artikel/nieuws/overheid/7438668/250449/russische-hackers-claimen-aanval-op-europees-parlement.html

'European Parliament website hit by DDoS cyberattack from Russia's Killnet', TechMonitor, 24-11-2022, https://techmonitor.ai/technology/cybersecurity/european-parliament-cyberattack-ddos-killnet

'Pro-Russia Killnet Group Takes Down the European Parliament Website', SpiceWorks, 24-11-2022, https://www.spiceworks.com/it-security/security-general/news/european-parliament-ddos-attack/

50 'Rusthuizen schakelen over op pen en papier na massale cyberaanval op Antwerpse stadsdiensten', HLN.be, 06-12-2022, https://www.hln.be/antwerpen/rusthuizen-schakelen-over-op-pen-en-papier-na-massale-cyberaanval-op-antwerpse-stadsdiensten~a24d88fa

'PLAY ransomware group claims responsibility for Antwerp attack as second Belgian city confirms new incident', The Record, 12-12-2022, https://therecord.media/play-ransomware-group-claims-responsibility-for-antwerp-attack-as-second-belgian-city-confirms-new-incident/

51 'Here's what cyber pros are watching in the Ukraine conflict', Washington Post, 24-2-2022, https://www.washingtonpost.com/politics/2022/02/24/heres-what-cyber-pros-are-watching-ukraine-conflict/

52 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', Wired, 22-8-2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

53 'Cyber War and Ukraine', the Center for Strategic and International Studies, 16-6-2022, https://www.csis.org/analysis/cyber-war-and-ukraine

54 '24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis', AIVD/MIVD, 20-2-2023, https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenis

55 'MIVD Jaarverslag 2022', MIVD, 19-04-2023

56 'Evaluating the International Support to Ukrainian Cyber Defense', Carnegie Endowment for International Peace, 3-11-2022, https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322

57 'MIVD Jaarverslag 2022', MIVD, 19-04-2023

58 'MIVD Jaarverslag 2022', MIVD, 19-04-2023

59 '24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis', AIVD/MIVD, 20-2-2023

60 'Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape', Google, 16-2-2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

61 'Oekraïne blijft doelwit van Russische wiper en ransomware', Dutch IT-channel, 1-2-2023, https://dutchitchannel.nl/714156/russische-apt-groepen-blijven-oekraine-aanvallen.html

62 'Russia hacked an American satellite company one hour before the Ukraine invasion', MIT Technology Review, 10-5-2022, https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/#:~:text=The%20attack%20on%20Viasat%20showcases%20cyber%27s%20emerging%20role%20in%20modern%20warfare.&text=Just%20an%20hour%20before%20Russian,EU%2C%20and%20UK%20said%20today.

63 'Cyberattack against Ukrtelecom on March 28: the details', State Service of Special Communications and Information Protection of Ukraine, 6-4-2022, https://cip.gov.ua/en/news/kiberataka-na-ukrtelekom-28-bereznya-detali

64 'Mustang Panda Uses the Russian- Ukrainian War to Attack Europe and Asia Pacific Targets', BlackBerry, 12-6-2022, https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets

65 'NCSC-dreigingsanalyse, Q4 2022: oktober – december', NCSC, 7-2-2023

66 'Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape', Google, 16-2-2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

67 'Analyse van de gelekte interne Conti chat', Orange Cyberdefense, 3-3-2022, https://www.orangecyberdefense.com/nl/blog/cyberdefense/analyse-van-de-gelekte-interne-conti-chat

68 'Russia-based ransomware group Conti issues warning to Kremlin foes', Reuters, 25-2-2022, https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/

69 'Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine', Recorded Future, 31-1-2023, https://www.recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine

70 'Cybersecuritybeeld Nederland 2022', NCTV, juni 2022

71 'In Cyber, Differentiating Between State Actors, Criminals Is a Blur', DOD News, 14-5-2021, https://www.defense.gov/News/News-Stories/Article/Article/2618386/in-cyber-differentiating-between-state-actors-criminals-is-a-blur/

72 'Hacktivism Is Back and Messier Than Ever', Wired, 27-12-2022, https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos

73 'Anonymous: the hacker collective that has declared cyberwar on Russia', The Guardian, 27-2-2022, https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia

74 'Digitale oorlog in Oekraïne: nog geen grote aanvallen, wel 'online pesterijen', NOS, 4-3-2022, https://nos.nl/nieuwsuur/collectie/13893/artikel/2419749-digitale-oorlog-in-oekraine-nog-geen-grote-aanvallen-wel-online-pesterijen

75 ''Cyberpartisans' hack Belarusian railway to disrupt Russian buildup', the Guardian, 25-1-2022, https://www.theguardian.com/world/2022/jan/25/cyberpartisans-hack-belarusian-railway-to-disrupt-russian-buildup

76 'Een internationaal cyberleger tegen Rusland met een Nederlander in de hoofdrol', de Volkskrant, 24-9-2022, https://www.volkskrant.nl/kijkverder/v/2022/een-internationaal-cyberleger-te-gen-rusland-met-een-nederlander-in-de-hoofdrol~v5802287/?referer=https%3A%2F%2Fwww.google.nl%2F

77 'Hacktivism Is Back and Messier Than Ever', Wired, 27-12-2022, https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos

78 'Dark Covenant 2.0: Cybercrime, the Russian State, and the War in Ukraine', Recorded Future, 31-1-2023, https://www.recordedfuture.com/dark-covenant-2-cybercrime-russian-state-war-ukraine

79 'Cybersecuritybeeld Nederland 2022', NCTV, juni 2022

80 'Vier cybersecuritylessen uit één jaar oorlog in Oekraïne', NCSC, 21-2-2023, https://www.ncsc.nl/documenten/publicaties/2023/februari/21/vier-cybersecuritylessen-uit-een-jaar-oorlog-in-oekraine

81 'Hoe helpt Microsoft Oekraïne in de oorlog met Rusland? 'Dit is het eerste dataconflict uit de geschiedenis'', Knack, 31-10-2022, https://www.knack.be/nieuws/wereld/hoe-helpt-microsoft-oekraine-in-de-oorlog-met-rusland-dit-is-het-eerste-dataconflict-uit-de-geschiedenis/

82 'Ukrainian vice prime ministers asks Elon Musk for Starlink satellites as Russia invades', New York Post, 26-2-2022, https://nypost.com/2022/02/26/ukrainian-vice-prime-minister-asks-elon-musk-for-starlink-satellites-as-russia-invades/

83 'Ukraine's engineers battle to keep the internet running while Russian bombs fall around them', Forbes, 22-3-2022, https://www.forbes.com/sites/thomasbrewster/2022/03/22/while-russians-bombs-fall-around-them-ukraines-engineers-battle-to-keep-the-internet-running/

84 'Ukraine war: Major internet provider suffers cyber-attack', BBC, 28-2-2022, https://www.bbc.com/news/60854881

85 'MIVD Jaarverslag 2022', MIVD, 19-04-2023

86 'MIVD Jaarverslag 2022', MIVD, 19-04-2023

87 'Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape', Google, 16-2-2023, https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf

88 '24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis', AIVD/MIVD, 20-2-2023, https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenis

89 'Big tech onder druk om mee te doen tegen desinformatie', NOS, 28-2-2022,https://nos.nl/collectie/13888/artikel/2419291-big-tech-onder-druk-om-meer-te-doen-tegen-desinformatie-oekraine-oorlog

90 'Online platforms beperking in EU toegang tot Russische staatsmedia', NOS, 1-3-2022, https://nos.nl/collectie/13888/artikel/2419312-online-platforms-beperken-in-eu-toegang-tot-russische-staatsmedia

91 'AIVD Jaarverslag 2022', AIVD, 17-04-2023

92 'MIVD Jaarverslag 2022', 19-04-2023

93 'Nederland zet 17 Russische diplomaten uit vanwege spionage', NOS, 29-3-2022, https://nos.nl/artikel/2423081-nederland-zet-17-russische-diplomaten-uit-vanwege-spionage

94 'Polen wijst 45 Russische diplomaten uit, Moskou dreigt met vergelding', NOS, 24-2-2022, https://nos.nl/collectie/13888/artikel/2422364-polen-wijst-45-russische-diplomaten-uit-moskou-dreigt-met-vergelding

95 'AIVD Jaarverslag 2022', AIVD, 17-04-2023

96 '24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis', AIVD/MIVD, 20-2-2023, https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenis

97 '24/2, De Russische aanval op Oekraïne: een keerpunt in de geschiedenis', AIVD/MIVD, 20-2-2023, https://www.aivd.nl/documenten/publicaties/2023/02/20/24-2---de-russische-aanval-op-oekraine-een-keerpunt-in-de-geschiedenis

98 'Digitale aanvallen oorlog Oekraïne', NCSC, n.d. https://www.ncsc.nl/onderwerpen/oekraine

99 'Cybersecuritybeeld Nederland 2022', NCTV, juni 2022

100 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 26-09-2022, https://www.nctv.nl/documenten/publicaties/2022/09/26/rijksbrede-risicoanalyse-nationale-veiligheid

101 'Voorbereiden op digitale ontwrichting', WRR, 09-09-2019, https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting

102 Zie bijvoorbeeld het scenario cyberaanval ICS - chemische sector in 'Themarapportage cyberdreigingen', onderdeel van de 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 26-09-2022, https://www.nctv.nl/documenten/publicaties/2022/09/26/themarapportages-cyberdreigingen-2022

103 Robert M. Lee en Tim Conway, 'The Five ICS Cybersecurity Critical Controls', SANS Whitepaper, oktober 2022, https://www.sans.org/white-papers/five-ics-cybersecurity-critical-controls/

104 2021 ICS Cybersecurity Year in Review, Dragos, 29-12-2022, https://www.dragos.com/year-in-review/

105 Richard Thomas, Joe Gardiner, Tom Chothia, Manolis Samanis, Awais Rashid en Joshua Perrett. Catch Me If You Can: An In-Depth Study of CVE Discovery Time and Inconsistencies for Managing Risks in Critical Infrastructures. CPSIOTSEC, 2022

106 'The Ultimate Guide to Understanding OT Security', Verve Industrial, 29-12-2022, https://verveindustrial.com/resources/blog/the-ultimate-guide-to-understanding-ot-security/

107 'OT:ICEFALL', Vedere Labs (2022), 29-12-2022, https://www.forescout.com/resources/ot-icefall-report/

108 Ralph Langner, 'What does "insecure by design" actually mean for OT/ICS security?', OT base, 03-03-2019, https://www.langner.com/2019/03/what-does-insecure-by-design-actually-mean-for-ot-ics-security/

109 'The Convergence of IT and Operational Technology: Cyber Risks to Critical Infrastructure on the Rise', Microsoft, Cyber Signals, December 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5daTD

110 Mary Gutierrez-May, 'Transparently Insecure Operational Technology: A Contextual Analysis', SANS, 06-01-2022, https://www.giac.org/research-papers/transparently-insecure-operational-technology-a-contextual-analysis/

111 'Industrial Internet of Things (IIoT)', Trend Micro, 29-12-2022, https://www.trendmicro.com/vinfo/us/security/definition/industrial-internet-of-things-iiot

112 Dean Parsons, 'The State of OT/ICS Cybersecurity in 2022 and Beyond', SANS, 27-10-2022, https://www.sans.org/white-papers/state-ics-ot-cybersecurity-2022-beyond/

113 'Industroyer2: Industroyer reloaded', ESET Research, 12-04-2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/

114 'Sandworm Group (UAC-0082) cyberattack on Ukrainian energy facilities using INDUSTROYER2 and CADDYWIPER MALWARE (CERT-UA#4435)', CERT-UA, 12-04-2022, https://cert.gov.ua/article/39518

115 Daniel Kapellmann Zafra, Raymond Leong, Chris Sistrunk, Ken Proska, Corey Hildebrandt, Keith Lunden en Nathan Brubaker, 'INDUSTROYER. V2: Old Malware Learns New Tricks', Mandiant, 25-04-2022, https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks

116 'CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS)', Dragos, 13-04-2022, https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/

117 Nathan Brubaker, Keith Lunden, Ken Proska, Muhammad Umair, Daniel Kapellmann Zafra, Corey Hildebrandt en Rob Caldwell, 'INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems', Mandiant, 13-04-2022, https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool

118 'Dreigingsbeeld Statelijke Actoren 2', AIVD, MIVD, NCTV, november 2022, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2

119 Marc Rivero, Jornt van der Wiel, Dmitry Galov en Sergey Lozhkin, 'Luna and Black Basta — new ransomware for Windows, Linux and ESXi', Securelist, Kaspersky, 20-07-2022, https://securelist.com/luna-black-basta-ransomware/106950/

120 Daniel Kapellmann Zafra, Keith Lunden, Nathan Brubaker en Jeremy Kennelly, 'Ransomware Against the Machine: How Adversaries are Learning to Disrupt Industrial Production by Targeting IT and OT', Mandiant, 24-02-2022, https://www.mandiant.com/resources/blog/ransomware-against-machine-learning-to-disrupt-industrial-production

121 Nathan Brubaker, Daniel Kapellmann Zafra, Keith Lunden, Ken Proska en Corey Hildebrandt, 'Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families', Mandiant, 15-07-2022, https://www.mandiant.com/resources/blog/financially-motivated-actors-are-expanding-access-into-ot

122 @malwrhunterteam 'Among the usual stuffs like passport photos and etc, Clop ransomware gang published these screenshots in the leak page for Thames Water...', MalwareHunterTeam, 18-08-2022, https://twitter.com/malwrhunterteam/status/1559249802130497538

123 'Important Statement', South Staffs Water, 15-08-2022, https://www.south-staffs-water.co.uk/news/important-statement

124 Dragos, ICS/OT CYBERSECURITY YEAR IN REVIEW 2022, https://www.dragos.com/year-in-review/

125 Vedere Labs, 'The Increasing Threat Posed by Hacktivist Attacks: An Analysis of Targeted Organizations, Devices and TTPs', Forescout, 01-12-2022, https://www.forescout.com/blog/the-increasing-threat-posed-by-hacktivist-attacks-an-analysis-of-targeted-organizations-devices-and-ttps/

126 'Global Hacktivism on the Rise', CYBLE, 25-07-2022, https://blog.cyble.com/2022/07/25/global-hacktivism-on-the-rise/

127 David Krivobokov, 'GhostSec Now Targeting Iranian ICS in Support of Hijab Protests', OTORIO, 06-10-2022, https://www.otorio.com/blog/ghostsec-now-targeting-iranian-ics-in-support-of-hijab-protests/

128 Michael J. Assante en Robert M. Lee, 'The Industrial Control System Cyber Kill Chain', SANS Whitepaper, 05-10-2015, https://www.sans.org/white-papers/36297/

129 Mandiant, 'GRU: Rise of the (Telegram) MinIOns', 23-09-2022, https://www.mandiant.com/resources/blog/gru-rise-telegram-minions

130 Bart Gijsen, Yoram Meijaard en Bram Poppink. Herstelvermogen binnen OT infrastructuren. TNO, 2022.

131 ENISA, 'NIS Investments 2022', 23-11-2022, https://www.enisa.europa.eu/publications/nis-investments-2022

132 Bart Gijsen, Yoram Meijaard en Bram Poppink. Herstelvermogen binnen OT infrastructuren. TNO, 2022.

133 Steve McIntosh, 'How to Overcome Vulnerability & Patch Management Challenges in Your OT Environment', Industrial Defender, 28-04-2021, https://www.industrialdefender.com/blog/how-to-overcome-vulnerability-patch-management-challenges-in-ot

134 J. Vos, P. Van den Brink en T. van Schie; TNO 2019 R11304 Succesfactoren voor digitaal veilige Operationele Technologie. TNO, 2019

135 Bart Gijsen, Yoram Meijaard en Bram Poppink. Herstelvermogen binnen OT infrastructuren. TNO, 2022.

136 Bart Gijsen, Yoram Meijaard en Bram Poppink. Herstelvermogen binnen OT infrastructuren. TNO, 2022.

137 NCTV, 'Nederlandse Cybersecuritystrategie 2022-2028', 10-10-2022, https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028

138 Ministerie van Infrastructuur en Waterstaat, 'Basismaatregelen voor cybersecurity van IACS', 10-10-2022, https://www.ncsc.nl/documenten/publicaties/2022/oktober/10/basismaatregelen-voor-cybersecurity-van-iacs

139 Rijkswaterstaat &, 'Nieuwe richtlijn cybersecurity: veilig én werkbaar', Rijkswaterstaat, https://www.magazinesrijkswaterstaat.nl/zakelijken-innovatie/2022/01/cybersecurity

140 Digital Trust Center, 'Doe de Security Check Procesautomatisering', https://www.digitaltrustcenter.nl/tools/doe-de-security-check-procesautomatisering

141 Europese Commissie, 'Cyber Resilience Act', 15-09-2022, https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

142 Ralph Moonen, Sjoerd Peerlkamp, Bram Blauwendraad, 'Onderzoeksrapport Competenties IACS Security Teams', Secura, 18-11-2021, https://www.ncsc.nl/onderzoek/documenten/rapporten/2021/november/19/onderzoeksrapport-competenties-iacs-security-teams

143 Ralph Moonen, Sjoerd Peerlkamp, Bram Blauwendraad, 'Onderzoeksrapport Competenties IACS Security Teams', Secura, 18-11-2021, https://www.ncsc.nl/onderzoek/documenten/rapporten/2021/november/19/onderzoeksrapport-competenties-iacs-security-teams

144 ENISA, 'NIS Investments 2022', 23-11-2022, https://www.enisa.europa.eu/publications/nis-investments-2022

145 Cyber Security Raad, 'Adviesrapport Integrale Aanpak Cyberweerbaarheid', 06-04-2021, https://www.rijksoverheid.nl/documenten/rapporten/2021/04/06/tk-bijlage-csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

146 NCTV, 'Nederlandse Cybersecuritystrategie 2022-2028', 10-10-2022, https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028

147 'Europees akkoord over vernieuwing basis digitale economie', Rijksoverheid.nl,23-04-2022, https://www.rijksoverheid.nl/actueel/nieuws/2022/04/22/europees-akkoord-over-vernieuwing-basis-digitale-economie.

148 'Beoordeling Verordening Cyber Resilience Act (CRA). Fiche van de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC)', Rijksoverheid.nl, 21-10-2022, https://open.overheid.nl/repository/ronl-3f800b4a35a8c2684d7337c14231b1e7441abfa8/1/pdf/fiche-1-verordening-cyber-resilience-act.pdf.

149 'Actieplan Nederlandse Cybersecuritystrategie 2022-2028', NCTV, oktober 2022.

150 'Europees Parlement publiceert wet die bedrijfsleven strenge securityeisen oplegt', Tweakers.nl, 27-12-2022, Europees Parlement publiceert wet die bedrijfsleven strenge securityeisen oplegt - IT Pro - Nieuws – Tweakers; 'Nederlandse Cybersecuritystrategie 2022-2028', NCTV, oktober 2022; 'Actieplan Nederlandse Cybersecuritystrategie 2022-2028', NCTV, oktober 2022.

151 Voor dat laatste: 'Onveilige 'slimme' apparaten straks van de markt geweerd, maar risico's blijven', NOS.nl, 23-10-2022,https://nos.nl/artikel/2449517-onveilige-slimme-apparaten-straks-van-de-markt-geweerd-maar-risico-s-blijven.

152 'Meer mogelijkheden NCSC om dreigings- en incidentinformatie te delen', NCSC, 01-12-2022, https://www.ncsc.nl/actueel/nieuws/2022/december/01/mogelijkheden-voor-het-delen-van-dreigings--en-incidentinformatie; 'Nationale cybersecurity organisaties gaan krachten bundelen', 07-09-2022, https://www.ncsc.nl/actueel/nieuws/2022/september/7/nationale-cybersecurity-organisaties-gaan-krachten-bundelen.

153 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, juli 2022.

154 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, juli 2022.

155 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, juli 2022; ' Themarapportage Cyberdreigingen van het Analistennetwerk Nationale Veiligheid, Analistennetwerk Nationale Veiligheid, juli 2022.

156 'Bereid je voor op de dreiging van quantumcomputers', AIVD, 23 september 2021

157 'Het PQC-migratie handboek', AIVD, 4 april 2023

158 'ChatGPT and large language models: what's the risk?', NCSC, 14-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

159 'ChatGPT and large language models: what's the risk?', NCSC, 14-03-2023, https://www.ncsc.gov.uk/blog-post/chatgpt-and-large-language-models-whats-the-risk.

160 'AP: centrale database paspoortgegevens groot risico', Autoriteit Persoonsgegevens, 30-01-2023,https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/ap-centrale-database-paspoortgegevens-groot-risico.

161 'Dreigingsbeeld Statelijke Actoren 2', AIVD, MIVD en NCTV, november 2022, p. 19, 33, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

162 'Jaarverslag AIVD 2022', AIVD, 17-04-2023, https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022.

163 'Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Openbaar jaarverslag 2022', Ministerie van Defensie, 19-04-2023, file:///H:/Downloads/openbaar-jaarverslag-mivd-2022.pdf.

164 'Jaarverslag AIVD 2022', AIVD, 17-04-2023, https://www.aivd.nl/onderwerpen/jaarverslagen/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022.

165 'Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Openbaar jaarverslag 2022', Ministerie van Defensie, 19-04-2023, file:///H:/Downloads/openbaar-jaarverslag-mivd-2022.pdf.

166 'Dreigingsbeeld Statelijke Actoren 2', AIVD, MIVD en NCTV, november 2022, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

167 'MIVD Jaarverslag 2022', MIVD, 19-04-2023

168 Informatie van Team High Tech Crime.

169 'Conti ransomware's internal chats leaked after siding with Russia', 27-02-2022, https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/;

'Checkpoint, Leaks of conti ransomware group paint picture of a surprisingly normal tech start up sort of', 10-03-2022, https://research.checkpoint.com/2022/leaks-of-conti-ransomware-group-paint-picture-of-a-surprisingly-normal-tech-start-up-sort-of/.

170 'Russia-Linked Ransomware Groups Are Changing Tactics to Dodge Crackdowns', The Wall Street Journal, 2-6-2022, https://www.wsj.com/articles/russia-linked-ransomware-groups-are-changing-tactics-to-dodge-crackdowns-11654178400

171 'Impact en schade cybercrime onverminderd groot', politie.nl, 19-1-2023, https://www.politie.nl/nieuws/2023/januari/19/politie-regis-treert-minder-cybercrime.html.

172 Informatie van Team High Tech Crime.

173 'Impact en schade cybercrime onverminderd groot', politie.nl, 19-1-2023, https://www.politie.nl/nieuws/2023/januari/19/politie-regis-treert-minder-cybercrime.html.

174 'Hackers opgepakt voor stelen miljoenen persoonsgegevens', NOS.nl,,23-02-2023, https://nos.nl/artikel/2464987-hackers-opgepakt-voor-stelen-miljoenen-persoonsgegevens.

175 'Ransomware Hackers Will Still Target Smaller Critical Infrastructure, CISA Director Warns'", Nextgov.com, 26-7-2022, https://www.nextgov.com/cybersecurity/2022/07/ransomware-hackers-will-still-target-smaller-critical-infrastructure-cisa-director-warns/374953/.

176 'Cyber-attack strikes German fuel supplies', BBC, 1-2-2022, https://www.bbc.com/news/technology-60215252

177 'BlackCat ransomware claims attack on Italian energy agency', Bleepingcomuter, 2-9-2022, https://www.bleepingcomputer.com/news/security/blackcat-ransomware-claims-attack-on-italian-energy-agency/

178 'Ransomwaregroep steelt gevoelige data van politie in het Belgische Zwijndrecht', Security.nl, 25-11-2022, https://www.security.nl/posting/775732/Ransomwaregroep+steelt+gevoelige+data+van+politie+in+het+Belgische+Zwijndrecht

179 'Politie waarschuwt hostingsector voor hosting resellers', Politie, 12-10-2022, https://www.politie.nl/nieuws/2022/oktober/12/11-politie-waarschuwt-hostingsector-voor-hosting-resellers.html.

180 'Dreigingsbeeld Statelijke Actoren 2', AIVD, MIVD en NCTV, november 2022, https://www.nctv.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-2.

181 'Verzekeraar waarschuwt: cybersecurity straks moeilijker te verzekeren dan klimaatschade', NRC,27-12-2022,https://www.nrc.nl/nieuws/2022/12/27/verzekeraar-waarschuwt-cybersecurity-straks-moeilijker-te-verzekeren-dan-klimaatschade-a4152668.

182 'Verzekeraar waarschuwt: cybersecurity straks moeilijker te verzekeren dan klimaatschade', NRC,27-12-2022,https://www.nrc.nl/nieuws/2022/12/27/verzekeraar-waarschuwt-cybersecurity-straks-moeilijker-te-verzekeren-dan-klimaatschade-a4152668; 'DNB: 'Nederland slecht verzekerd tegen cybercrime', Data&Privacyweb, 17-11-2022, <https://privacy-web.nl/nieuws/dnb-nederland-slecht-verzekerd-tegen-cybercrime/; 'Lloyd's stopt volgend jaar dekking voor catastrofale statelijke cyberaanvallen', Security.nl, 22-08-2022, https://www.security.nl/posting/765265/Lloyd%27s+stopt+volgend+jaar+dekking+voor+catastrofale+statelijke+cyberaanvallen; 'Verzekeraars in een veranderende wereld. Kansen en risico's in tijden van klimaatverandering, digitalisering en inflatie', De Nederlandsche Bank, 16-11-2022,https://www.dnb.nl/media/elrpseou/dnb-verzekeraars-in-een-veranderende-wereld.pdf.

183 Verzekeraar moet 1,4 miljard dollar schade door NotPetya bij Merck vergoeden, security.nl, 4-5-20223, https://www.security.nl/posting/795246/Verzekeraar+moet+1%2C4+miljard+dollar+schade+door+NotPetya+bij+Merck+vergoeden.

184 'Verzekeraar waarschuwt: cybersecurity straks moeilijker te verzekeren dan klimaatschade', NRC,27-12-2022,https://www.nrc.nl/nieuws/2022/12/27/verzekeraar-waarschuwt-cybersecurity-straks-moeilijker-te-verzekeren-dan-klimaatschade-a4152668; 'DNB: 'Nederland slecht verzekerd tegen cybercrime', Data&Privacyweb, 17-11-2022, <https://privacy-web.nl/nieuws/dnb-nederland-slecht-verzekerd-tegen-cybercrime/.

185 'Meer aandacht nodig voor silent cyber risico op traditionele verzekeringen', Verbond van verzekeraars, 17-6-2022, https://www.verzekeraars.nl/publicaties/actueel/meer-aandacht-nodig-voor-silent-cyber-risico-op-traditionele-verzekeringen;

'EIOPA publishes supervisory statements on exclusions related to systemic events and the management of non-affirmative cyber exposures', European Insurance and Occupational Pensons authority, 22-09-2022,https://www.eiopa.europa.eu/eiopa-publishes-supervisory-statements-exclusions-related-systemic-events-and-management-non-2022-09-22_en;

'Supervisory statement on the management of non-affirmative cyber exposures', European Insurance and Occupational Pensons authority, 22-09-2022, https://www.eiopa.europa.eu/publications/supervisory-statement-management-non-affirmative-cyber-exposures_en.

186 'Verzekeraar waarschuwt: cybersecurity straks moeilijker te verzekeren dan klimaatschade', NRC,27-12-2022,https://www.nrc.nl/nieuws/2022/12/27/verzekeraar-waarschuwt-cybersecurity-straks-moeilijker-te-verzekeren-dan-klimaatschade-a4152668; 'DNB: 'Nederland slecht verzekerd tegen cybercrime', Data&Privacyweb, 17-11-2022, <https://privacy-web.nl/nieuws/dnb-nederland-slecht-verzekerd-tegen-cybercrime/.

187 ''Negen op de tien bedrijven willen over op netwerk-as-a-service'', TECHZINE, 20-10-2022, https://www.techzine.nl/nieuws/infrastructure/505860/negen-op-de-tien-bedrijven-willen-over-op-netwerk-as-a-service/; 'Network-as-a-service: opkomst van soepel netwerk', Computable.nl, 20-7-2022, https://www.computable.nl/artikel/blogs/management/7361407/5260614/network-as-a-service-opkomst-van-soepel-netwerk.html.

188 'Toezichthouders publiceren samenhangend beeld cybersecurity vitale processen', Inspectie Justitie en Veiligheid,06-07-2022, https://www.inspectie-jenv.nl/actueel/nieuws/2022/07/06/toezichthouders-publiceren-samenhangend-beeld-cybersecurity-vitale-processen;'Samenhangend inspectiebeeld cybersecurityvitale processen 2021-2022', Agentschap Telecom, juni 2022.

189 'Nebu moet aan Blauw informatie verstrekken over datalekken', de Rechtspraak, 06-04-2023, https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Rotterdam/Nieuws/Paginas/Nebu-moet-aan-Blauw-informatie-verstrekken-over-datalekken.aspx ;'Datalek Nederlandse bedrijven steeds groter: zeker 2 miljoen klanten getroffen', NOS.nl, 30-03-2023,https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen.

190 Voor dat laatste: 'We zagen het lek, maar mochten niets zeggen',De Volkskrant, 14-01-2023.

191 'Nebu moet aan Blauw informatie verstrekken over datalekken', de Rechtspraak, 06-04-2023, https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Rotterdam/Nieuws/Paginas/Nebu-moet-aan-Blauw-informatie-verstrekken-over-datalekken.aspx ;'Datalek Nederlandse bedrijven steeds groter: zeker 2 miljoen klanten getroffen', NOS.nl, 30-03-2023,https://nos.nl/artikel/2469510-datalek-nederlandse-bedrijven-steeds-groter-zeker-2-miljoen-klanten-getroffen.

192 'Landelijk Crisisplan Digitaal', NCTV, december 2022,https://open.overheid.nl/documenten/ronl-43856896b0650c82103312680f9c830c09b5f485/pdf.

193 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, juli 2022.

194 'Risicorapportage cyberveiligheid economie 2019', Centraal Planbureau, 17-10-2019, https://www.cpb.nl/sites/default/files/omnidownload/cpb-notitie-risicorapportage-cyberveiligheid-2019.pdf.

195 'Toezichthouders publiceren samenhangend beeld cybersecurity vitale processen', Inspectie Justitie en Veiligheid,06-07-2022, https://www.inspectie-jenv.nl/actueel/nieuws/2022/07/06/toezichthouders-publiceren-samenhangend-beeld-cybersecurity-vitale-processen;'Samenhangend inspectiebeeld cybersecurityvitale processen 2021-2022', Agentschap Telecom, juni 2022.

196 'Microsoft Digital Defense Report 2022', Microsoft, 2022, p. 108, https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022.

197 Gebaseerd op een gesprek met hoogleraar Bibi van de Berg op 11 januari 2023.

198 'Een digitaal veilige gemeente begint niet bij de burgemeester', Nederlands Genootschap van Burgemeesters,3-1-2023,https://www.burgemeesters.nl/actueel/nieuws/een-digitaal-veilige-gemeente-begint-niet-bij-de-burgemeester/.

Colofon

Het Cybersecuritybeeld Nederland 2023 (CSBN 2023) biedt inzicht in de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de digitale weerbaarheid en tot slot digitale risico's. Daarnaast heeft het CSBN 2023 tot doel om inzicht te geven in mogelijke veranderingen in de strategische thema's die in het CSBN 2022 zijn uitgewerkt. Deze thema's vormden een inhoudelijke basis voor de Nederlandse Cybersecurity Strategie 2022-2028. Dit CSBN vormt een inhoudelijke basis voor de evaluatie van het daarvan afgeleide actieplan. De focus ligt op de nationale veiligheid.

Het CSBN is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Daarbij is nauw samengewerkt met het Nationaal Cyber Security Centrum (NCSC). Het CSBN wordt jaarlijks door de NCTV vastgesteld.

De NCTV draagt samen met partners uit het veiligheidsdomein bij aan een veilig en stabiel Nederland door dreigingen te onderkennen en de weerbaarheid en bescherming van nationale veiligheidsbelangen te versterken. Doel is het voorkomen en beperken van maatschappelijke ontwrichting. Sinds de oprichting van de NCTV is er binnen de Rijksoverheid één organisatie verantwoordelijk voor terrorismebestrijding, cybersecurity, nationale veiligheid en crisisbeheersing.

Het NCSC is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Het NCSC draagt bij aan het vergroten van de digitale weerbaarheid van de Nederlandse samenleving. Daarnaast heeft zij als doel de vitale infrastructuur en Rijksoverheid van Nederland te beschermen door de digitale weerbaarheid van Nederland te vergroten en de gevolgen van cyberincidenten te beperken.

Uitgave
Nationaal Coördinator
Terrorismebestrijding
en Veiligheid (NCTV)
Postbus 20301, 2500 EH Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5050

Meer informatie
www.nctv.nl
info@nctv.minjenv.nl
@nctv_nl

Juni 2023