Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

Cybersecuritybeeld Nederland 2024

Coverbeeld: Statelijke actoren intensiveren hun activiteiten en verbreden hun capaciteiten, waarbij zij gebruik maken van verschillende middelen uit een bredere gereedschapskist. Ook vitale infrastructuur in Nederland, bijvoorbeeld windmolenparken, kan daardoor doelwit worden van digitale spionage of sabotage.

Inhoudsopgave

Reizigers op Eindhoven Airport zijn gestrand door een grote storing die het vliegverkeer van en naar Eindhoven Airport volledig heeft platgelegd. Het bleek te gaan om een fout in software op een ICT-netwerk van Defensie. Deze storing trof ook het communicatie- en alarmeringssysteem van hulpdiensten, waardoor ze onderling moeilijker konden communiceren. Pas aan het einde van de dag werd de storing verholpen.

Turbulente tijden, onvoorziene effecten

Digitale risico's zijn dynamisch en worden beïnvloed door vele factoren die ook niet-digitaal kunnen zijn. Zeker sinds enkele jaren hebben turbulente geopolitieke tijden hun weerslag op de digitale dreiging. Nederland is doelwit van cyberaanvallen, of ondervindt de impact van cyberaanvallen die doorwerken binnen het digitale ecosysteem. Daarnaast kunnen storingen leiden tot grootschalige uitval. Digitale risico's zijn complex en in hoge mate met elkaar verbonden. Dat alles kan leiden tot onvoorziene effecten. Het risico dat de nationale veiligheid wordt geraakt, kan daardoor toenemen. Om digitale risico's het hoofd te kunnen bieden, is het van belang een brede manier van risicobeheersing aan te nemen.

Hoofdbevindingen CSBN 2024

1. De digitale dreiging tegen Nederland is groot en divers, en cyberaanvallen zijn voornamelijk afkomstig van statelijke en criminele actoren. In deze turbulente geopolitieke tijden intensiveren statelijke actoren hun activiteiten en verbreden zij hun capaciteiten, waarbij zij gebruik maken van een bredere gereedschapskist. Criminele actoren voeren op grote schaal aanvallen uit en handelen daarbij opportunistisch. Grootschalige uitval van digitale processen vormt eveneens een dreiging.
2. Digitale risico's vragen om een brede manier van beheersing. Ze zijn dynamisch en worden beïnvloed door vele verschillende factoren. Het bredere digitale ecosysteem, met daarbinnen monoculturen, en de hoge mate van digitalisering zorgen ervoor dat risico's met elkaar verbonden raken.
3. De veiligheid van digitale processen is en blijft essentieel in onze maatschappij en is dus onlosmakelijk verbonden met de nationale veiligheid. Het belang van digitale veiligheid concurreert met andere belangen.

Digitale dreiging tegen Nederland is groot en divers

Statelijke en criminele actoren vormen de grootste dreiging tegen Nederland als het gaat om cyberaanvallen. Nieuwe manieren voor aanvallen zijn misbruik van edge devices, zoals VPN-servers en routers. Aanvallen via edge devices zijn aantrekkelijk, omdat monitoring en detectie hierop zeer complex is.

Statelijke actoren intensiveren activiteiten en verbreden capaciteiten

Meerdere statelijke actoren intensiveren hun cyberactiviteiten. Zo voeren Rusland en China hun activiteiten op. Ook sommige andere landen investeren in hun cyberprogramma, waardoor nieuwe cybermachten opkomen. Naast intensivering van cyberactiviteiten, is voor een aantal landen ook sprake van verbreding van de capaciteiten: ze voegen nieuwe methoden toe aan hun bestaande arsenaal of gebruiken andere, ook niet-digitale, middelen. Bovenop het gebruik van andere middelen uit een bredere gereedschapskist, is de inzet of betrokkenheid van niet-statelijke actoren onderdeel van die verbreding. Zo werd in 2023 een groter deel van de Russische digitale spionage-, sabotage- en beïnvloedingsactiviteiten uitgevoerd door 'hacktivistische' collectieven. Soms waren dit zogenoemde cover-operaties, soms waren het daadwerkelijk hacktivistische groeperingen die handelden in het verlengde van de Russische staat. Het Chinese offensieve cyberprogramma is mede gestoeld op samenwerking tussen bedrijfsleven, universiteiten en Chinese inlichtingendiensten. De scheidslijnen tussen organisaties zijn daarbij onduidelijk: personen vervullen soms zowel een wetenschappelijke rol als een rol in het Chinese veiligheidsapparaat en werken daarbij samen met Chinese (staats) bedrijven.

Cybercriminelen onverminderd in staat om schade toe te brengen aan digitale processen

Cybercriminelen zijn onverminderd in staat om omvangrijke schade toe te brengen aan digitale processen. Met name de inzet van ransomware kan grote gevolgen krijgen voor de nationale veiligheid. Opvallend was dat sommige ransomware-actoren zich enkel focusten op het exfiltreren van data. In plaats van het versleutelen van data en slachtoffers daarmee afpersen, deden zij dit door te dreigen met publicatie.

Grootschalige uitval vormt ook dreiging, zeker als gevolg van monoculturen

Naast cyberaanvallen, gaat ook van grootschalige uitval een dreiging uit. Uitval van digitale processen kan verschillende oorzaken hebben, waaronder technische problemen en niet-moedwillig menselijk handelen. In de zomer van 2024 deden zich twee grootschalige uitval-incidenten voor als gevolg van een softwarefout, waardoor bijvoorbeeld ziekenhuiszorg, luchtvaart en overheidstaken grote hinder ondervinden. De incidenten maakten duidelijk wat de mogelijk vergaande en onvoorziene gevolgen zijn van een digitale monocultuur, waarin vele organisaties afhankelijk zijn van een klein aantal aanbieders.

Cyberincidenten passen in dreigingsbeeld

De cyberincidenten beschreven in het Jaarbeeld passen in de voorgaande dreigingsbeelden. Zo kunnen incidenten voor een deel worden geplaatst in de context van geopolitieke spanningen. Het gaat dan vooral om de oorlog tegen Oekraïne, de strijd tussen Israël en Hamas en de spanningen tussen het westen en China. Wereldwijd ondervonden aanbieders van vitale processen hinder van cyberaanvallen. Opvallend waren de voorbereidingsactiviteiten in de VS voor digitale sabotage door een aan China gelinkte hackersgroep. In 2023 waren er in Nederland geen meldingen van informatiebeveiligingsincidenten boven de zogeheten drempelwaardes. Ransomware-aanvallen haalden opnieuw het nieuws, waarbij ook sprake was van datalekken in combinatie met afpersing. Een aantal Nederlandse zorginstellingen werd geraakt door cyberaanvallen, dit had voor zover bekend geen impact gehad op de te verlenen zorg. Organisaties kregen ook te maken met de gevolgen van cyberaanvallen bij andere organisaties. Verder waren er diverse verstoringen van digitale processen als gevolg van menselijk of technisch falen, zoals die als gevolg van de wereldwijde storing van Microsoft systemen door een foutieve update van de software van CrowdStrike. In Nederland raakten diverse digitale processen verstoord door een softwarefout op een netwerk van Defensie.

Digitale risico's staan niet op zichzelf, maar worden beïnvloed door vele verschillende factoren

Net als voorgaande jaren, hebben we gezien dat diverse factoren digitale risico's beïnvloeden en compliceren. Ook ontwikkelingen die ogenschijnlijk niets met cybersecurity van doen hebben, kunnen blijvend van invloed zijn op de digitale dreiging en weerbaarheid. Dat geldt bijvoorbeeld voor geopolitieke en technologische ontwikkelingen. Zo vormt een toekomstige krachtige quantumcomputer, een technologische ontwikkeling, nu al een risico voor de nationale veiligheid. Versleutelde data die nu onderschept en opgeslagen wordt, kan mogelijk namelijk op een later moment ontsleuteld worden met een quantumcomputer.

De mondiale datahandel is een voorbeeld van een niet-digitale factor die van invloed is op digitale risico's. Sommige bedrijven veredelen de verkregen persoonsgevoelige data met andere data, stellen profielen op van gebruikers en verkopen deze. De

grootschaligheid en precisie van die datahandel en mogelijk misbruik daarvan, kan de nationale veiligheid schaden.

Een ander voorbeeld is het tekort aan cybersecuritydeskundigen in Nederland. Dat tekort kan uiteindelijk zijn weerslag hebben op de digitale weerbaarheid van Nederland. Daarnaast kan het voor kwaadwillenden interessant worden om te bezien bij welke organisaties de grootste tekorten bestaan – en daarmee mogelijk de zwakste verdediging.

Digitale risico's vragen om brede manier van beheersing

Digitale risico's worden beïnvloed door vele, ook niet-digitale, factoren. Bovendien zijn digitale processen in hoge mate met elkaar verbonden en verweven en vormen zij gezamenlijk een breder digitaal ecosysteem. Een incident bij een organisatie kan doorwerken naar vele andere organisaties, zoals de foutieve software-update van CrowdStrike en de softwarefout op een netwerk van Defensie demonstreerden. Niet-vitale organisaties kunnen voor kwaadwillenden een aantrekkelijke springplank zijn naar vitale organisaties. Statelijke actoren kunnen cyberaanvallen uitvoeren in combinatie met andere, ook niet-digitale, middelen. Ook kunnen individuele cyberaanvallen in samenhang met elkaar worden ingezet. Die combinatie kan grote impact hebben.

Een brede manier van risicobeheersing past bij het diverse en dynamische karakter van digitale risico's, en past ook bij het beheersen van de mogelijk onvoorziene effecten van een incident. Daarbij kan het nuttig zijn om bij het inrichten en beheren van een netwerk als uitgangspunt te hanteren dat er al een kwaadwillende in je netwerk zit (assume breach). Verder vormen basismaatregelen nog altijd een effectieve barrière tegen vele soorten cyberaanvallen. De basisprincipes, opgesteld door het NCSC en het DTC, kunnen hiervoor een vertrekpunt vormen.

Veiligheid digitale processen essentieel, en onlosmakelijk verbonden met nationale veiligheid

Digitale processen vormen het zenuwstelsel van de maatschappij, en veiligheid van die processen is essentieel. Digitale veiligheid is daardoor onlosmakelijk verbonden met de nationale veiligheid. Digitale veiligheid is ook nodig om vertrouwen te behouden in digitale processen. Wanneer dat vertrouwen verdwijnt, kan dat voor grote problemen zorgen in onze gedigitaliseerde samenleving.

Een wezenlijke ontwikkeling is dat het belang van digitale veiligheid verankerd raakt in nieuwe Europese en Nederlandse wet- en regelgeving. Het heeft echter tijd nodig voordat wetgeving daadwerkelijk leidt tot verandering in de digitale weerbaarheid en invloed heeft op digitale risico's. Dat heeft niet alleen te maken met het vormgeven van wetgeving, maar hangt ook samen met bewustwording en voorbereiding bij bedrijven, uitvoeringsorganisaties, en toezichthouders.

Structurele en nieuw beschreven uitdagingen voor digitale veiligheid[1]

Structurele uitdagingen voor digitale veiligheid, ook in eerdere edities van het CSBN beschreven	Nieuwe uitdagingen voor digitale veiligheid, niet in eerdere edities van het CSBN beschreven
Geopolitiek en technologische ontwikkelingen beïnvloeden dreiging	• Statelijke actoren intensiveren activiteiten en verbreden capaciteiten. Zij maken gebruik van een bredere gereedschapskist, waar cyberaanvallen “slechts” een onderdeel van zijn. • Toekomstige krachtige quantumcomputer vormt nu al een risico voor de nationale veiligheid.
Statelijke en criminele actoren nemen leeuwendeel van cyberaanvallen voor hun rekening	• Actoren zoeken nieuwe wegen om cyberaanvallen uit te voeren. Living-off-the-Land en targeting edge devices kenmerkende modus operandi in 2023. • Statelijke actoren intensiveren activiteiten en verbreden capaciteiten.
Iedere organisatie kan doelwit zijn van kwaadwillenden	• Grootschalige effecten door digitale monoculturen.
Veiligheid digitale processen is en blijft essentieel in gedigitaliseerde samenleving	• Digitale veiligheid randvoorwaardelijk voor vertrouwen in digitale processen
Digitale risico’s vragen om brede manier van beheersing	• Fysieke en digitale incidenten dienen in samenhang met elkaar te worden bezien. • Statelijke actoren maken gebruik van een bredere gereedschapskist, waar cyberaanvallen “slechts” een onderdeel van zijn. • Grootschalige handel in persoonsgevoelige data vormt dreiging voor nationale veiligheid. • Grootschalige concentratie bij grootste cloudaanbieders vormt risico. • Grootschalige effecten door digitale monoculturen.
Wetgeving consolideert, implementatie onderweg	• Het belang van digitale veiligheid raakt verder verankerd in wet- en regelgeving.
Niet-digitale ontwikkelingen beïnvloeden digitale veiligheid	• Grootschalige concentratie bij grootste cloudaanbieders vormt risico. • Grootschalige effecten door digitale monoculturen. • Weerbaarheid in geding door schaarse cybersecuritycapaciteit • Grootschalige handel in persoonsgevoelige data vormt dreiging voor nationale veiligheid
Strategische thema’s nog steeds van toepassing	• Enkele extra uitdagingen voor risicobeheersing: • Staten intensiveren activiteiten en verbreden capaciteiten, en statelijke cyberaanvallen staan niet op zichzelf maar zijn onderdeel van een bredere gereedschapskist. • Actoren zoeken nieuwe wegen als start voor cyberaanvallen. • Grootschalige concentratie bij grootste cloudaanbieders vormt risico • De mondiale online datahandel. • De noodzaak van vertrouwen om gebruik te willen (blijven) maken van digitale processen.

I De linkerkolom van de tabel correspondeert met bevindingen uit Hoofdstuk 4, de rechterkolom correspondeert met bevindingen uit Hoofdstuk 3.

Infrastructuur in Nederland, zoals bruggen en snelwegen, zijn al lange tijd afhankelijk van technische systemen voor bediening en veiligheid. Dit zorgt ook voor toenemende kwetsbaarheid voor cyberincidenten. De afgelopen jaren waren verschillende sluizen, bruggen en tunnels tijdelijk gestremd doordat bedienings- en veiligheids-systemen niet werkten. Dit zorgde voor lange files.

1 Inleiding

Doel en afbakening

Het Cybersecuritybeeld Nederland 2024 (CSBN 2024) 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 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. Het CSBN 2024 vormt een inhoudelijke basis voor de evaluatie van het daarvan afgeleide actieplan.

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. Het CSBN richt zich 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 beschikbaar voor het brede publiek.

Leeswijzer

Dit CSBN bestaat uit het voorgaande hoofdstuk waarin de hoofdboodschappen zijn verwoord en uit verdiepende hoofdstukken. Deze indeling beoogt dat lezers uit verschillende doelgroepen 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 2023 t/m juni 2024 en de duiding daarvan.
- Hoofdstuk 3 beschrijft nieuwe uitdagingen, veranderingen in bestaande uitdagingen of nieuwe inzichten die als relevant zijn beoordeeld voor strategie- en beleidsvorming.
- Hoofdstuk 4 geeft inzage in structurele uitdagingen voor digitale veiligheid. Deze uitdagingen zijn eerder al aan bod gekomen in eerdere Cybersecuritybeelden van de afgelopen jaren en zijn, met kleine nuanceverschillen nog onverkort van toepassing. In tegenstelling tot de andere hoofdstukken vindt geen expliciete verantwoording van de bronnen plaats. Over deze uitdagingen is immers al eerder gepubliceerd in eerdere editie van het CSBN.

Bijlage 1 bevat een verantwoording van de totstandkoming van het CSBN. Bijlage 2 bevat een methodologische toelichting op de gebruikte cijfers over ransomware-aanvallen. Bijlage 3 bevat de vijf basisprincipes voor digitale weerbaarheid, opgesteld door het NCSC en DTC. Bijlage 4 bevat de bronnen en referenties.

Toelichting 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:** 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).
- **Weerbaarheid:** : het vermogen om (relevante) risico's tot een aanvaardbaar niveau te reduceren door middel van een verzameling van maatregelen om cyberincidenten te voorkomen. Hieronder valt ook het ontdekken van cyberincidenten, en wanneer deze zich voordoen het beperken van schade en het eenvoudiger maken van herstel. 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.

Verschillende typen aanvallen

Analytisch zijn vele verschillende typen aanvallen te onderkennen. Hieronder zijn enkele typen beschreven in alfabetische volgorde:

- **DDoS-aanval (Distributed Denial-of-Service):** een aanval op de capaciteit van onlinediensten of de ondersteunende servers en netwerkapparatuur. Het resultaat van deze aanval is dat digitale diensten slecht of helemaal niet meer bereikbaar zijn voor medewerkers of klanten.[2] Een DDoS-aanval is laagdrempelig in te zetten en het achterhalen wie erachter zit, is lastig. Daarentegen kunnen organisaties relatief goed weerbaar zijn tegen dit type aanvallen en is de impact ervan beperkt. Een voorbeeld is de DDoS-aanval in april 2023 tegen de websites van de internationale organisatie die de luchtverkeersleiding in Europa coördineert (zie Jaarbeeld).
- **Defacement (digitale bekladding):** een actor verandert de inhoud op de webpagina's of voegt nieuwe webpagina's toe. Soms laat de actor bij de uitvoering van een defacement malware achter, waardoor bezoekers van de website besmet kunnen raken.[3] Een defacement tast dus de integriteit van webpagina's aan door foutieve informatie te verstrekken of kan, in het geval van de plaatsing van malware, leiden tot een vervolgaanval bij bezoekers. Defacements worden veelal uitgevoerd door hacktivisten, waarbij zij de inhoud van websites veranderen in overeenstemming met de boodschap van de betreffende groep. In 2022 defaceten pro-Oekraïense hacktivisten Russische overheidswebsites[4] met intimiderende teksten. Pro-Russische hacktivisten deden hetzelfde bij Oekraïense overheidswebsites.[5]
- **Digitale sabotage:** een actor tast opzettelijk en langdurig de beschikbaarheid van digitale diensten, processen of systemen aan (door in extreme gevallen de vernietiging daarvan). Dit is mogelijk door voorbereidingshandelingen daartoe, door zich toegang te verschaffen tot en zich in te nestelen in ICT- en/of OT-systemen.[II][6] Voorbereidingshandelingen kunnen lang duren (maanden of jaren), vereisen specifieke technische kennis en zijn voornamelijk afkomstig vanuit statelijke actoren. Digitale sabotage kan tot ingrijpende gevolgen leiden. Een voorbeeld van voorbereidingshandelingen voor digitale sabotage zijn de activiteiten van de Chinese APT Volt Typhoon in de vitale infrastructuur van de VS (zie Jaarbeeld).
- **Digitale spionage:** een actor tast de vertrouwelijkheid aan van informatie door die te kopiëren of weg te nemen.[7] De onderliggende motivatie is het verkrijgen van gevoelige of geclassificeerde gegevens of intellectueel eigendom. Digitale spionage vindt primair plaats door statelijke actoren. Een voorbeeld is de Chinese digitale spionage in Nederland door middel van geavanceerde malware die de MIVD heeft blootgelegd op een computernetwerk bij de krijgsmacht (zie Jaarbeeld).
- **Ransomware-aanval:** een actor versleutelt bestanden van gebruikers met behulp van ransomware(software), met als doel om deze later te ontsleutelen in ruil voor losgeld. In extreme gevallen blokkeert de ransomware de toegang tot het systeem door ook systeembestanden te versleutelen die essentieel zijn voor de goede werking van het systeem. Een actor kan met behulp van geavanceerde soorten ransomware naast lokale systemen ook harde schijven, databases, back-ups, USB-sticks en gegevens in de cloud versleutelen. Een ransomware aanval tast in ieder geval de beschikbaarheid van systemen en data aan. Bij een gerichte ransomware-aanvallen heeft de actor toegang tot de systemen en dat brengt mogelijk de integriteit en de vertrouwelijkheid van data in gevaar. Met name cybercriminelen voeren ransomware-aanvallen uit.
- **Supply chain-aanval:** een actor tast doelbewust de vertrouwelijkheid, integriteit of beschikbaarheid aan van een of meer onderdelen binnen een supply chain (toeleveringsketen) om zo een springplank te krijgen voor aanvallen op andere organisaties, die veelal het primaire doelwit zijn. Actoren kunnen door middel van een supply chain-aanval bijvoorbeeld toegang verkrijgen tot beveiligde ICT-systemen van organisaties en daarmee onder andere tot diens gevoelige gegevens, processen en financiën. De aanval heeft een gelaagd karakter (minstens twee aanvallen) en is gericht, complex, duur en vereist daardoor vergaande capaciteit en planning van de actor. Het motief voor de aanval is meestal spionage, maar kan ook gericht zijn op sabotage of financieel gewin. Een voorbeeld vond plaats in maart 2023, waarbij hackers waarschijnlijk de netwerken van duizenden bedrijven compromitteerden als gevolg van een supply chain-aanval op het zakelijke telefoonbedrijf 3CX (zie Jaarbeeld).

II Operationele technologie (OT) wordt binnen industriële netwerken ook wel aangeduid als Industrial Automation and Control Systems (IACS)

Een lege wachtkamer in het Scheper ziekenhuis in Emmen. De spoedeisende hulp van het streek-ziekenhuis werd op 19 juli 2024 gesloten vanwege een wereldwijde computerstoring. Operaties moesten worden geannuleerd. Vliegvelden, overheidsorganisaties en vele andere bedrijven werden mondiaal getroffen. Het bleek te gaan om een foutieve update van de software van CrowdStrike.

2 Jaarbeeld

Cyberincidenten in de rapportageperiode passen in het dreigingsbeeld. Incidenten, waaronder DDoS aanvallen, (voorbereidingshandelingen voor) sabotage en spionage, kunnen voor een deel worden geplaatst in de context van geopolitieke spanningen en verschuivende internationale machtsverhoudingen. Het gaat dan vooral om de oorlog tegen Oekraïne, de strijd tussen Israël en Hamas en de rol van China op het wereldtoneel. Ransomware-aanvallen haalden opnieuw het nieuws, waarbij regelmatig ook sprake is van datalekken in combinatie met afpersing. Volgens de Autoriteit Persoonsgegevens hebben zich in Nederland in ieder geval 178 ransomware-aanvallen voorgedaan in 2023. Daarbij moet worden opgemerkt dat het aantal slachtofferorganisaties en getroffen burgers exponentieel groter is. Cyberincidenten binnen het bredere digitale ecosysteem werken immers door naar andere organisaties en burgers. Bij de meeste cyberaanvallen komen statelijke actoren en cybercriminelen naar voren als meest waarschijnlijke actor, en bij DDoS aanvallen meestal hacktivisten. Naast cyberaanvallen, zijn er opnieuw tal van voorbeelden van storingen als gevolg van niet moedwillig handelen. Internationale operaties van handhavings- en opsporingsinstanties verstoorden delen van de criminele infrastructuur. Ook werden enkele cybercriminelen die internationaal opereren gearresteerd en zijn op initiatief van Nederland cybercriminelen door de EU op de sanctielijst geplaatst.

Cyberincidenten passen in dreigingsbeeld

Beschikbaarheid digitale processen aangetast door ransomware, DDoS en storingen

Deze rapportageperiode waren digitale processen niet beschikbaar door ransomware-aanvallen, DDoS-aanvallen en storingen. Zo werd de werking van diverse websites meermaals verstoord door DDoS-aanvallen, waaronder ook in Nederland. De impact bleef beperkt en het is hacktivisten dan ook vooral te doen om media-aandacht en angst aanjagen. Ransomware-aanvallen hadden een grotere impact. In het geval van de ransomware-aanval op maritiem dienstverlener Royal Dirkzwager duurde het (bijna) een week voordat systemen waren hersteld en dienstverlening kon worden hervat. Daarnaast waren er diverse verstoringen als gevolg van menselijk of technisch falen, zoals de wereldwijde storing van Microsoftsystemen door een update van CrowdStrike. Deze storing had wereldwijd grote impact, ook in Nederland ondervonden onder meer het vliegverkeer en de gezondheidszorg problemen. In Nederland volgde in augustus nog een nationale storing toen er

problemen waren met een netwerk van Defensie. Daarbij ondervonden overheidsorganisaties en Eindhoven Airport grote hinder.

DDoS-aanvallen tegen Nederlandse organisaties vloeien voort uit geopolitieke spanningen

Geopolitieke spanningen hebben onder andere geleid tot DDoS-aanvallen tegen Nederlandse organisaties. Deze rapportageperiode kende de nodige incidenten waarbij DDoS-aanvallen (kortstondig) digitale processen verstoorden. Een deel van de aanvallen werd opgeëist door pro-Russische actoren die zich profileerden als hacktivisten. Ook het conflict in Gaza heeft geleid tot DDoS-aanvallen. Zo werd bijvoorbeeld het Centrum Informatie en Documentatie Israël in oktober en november 2023 slachtoffer van aanhoudende DDoS-aanvallen. Het is niet bekend wie voor die aanvallen verantwoordelijk is. Hoewel DDoS-aanvallen beperkt en symbolisch van aard zijn, kunnen deze wel (tijdelijk) invloed hebben op de beschikbaarheid, informatieverstrekking en/of dienstverlening van de getroffen website(s).

Statelijke actoren voeren cyberaanvallen uit, waaronder in Nederland

Landen met een offensief cyberprogramma voerden ook in deze periode cyberaanvallen uit, onder meer in de context van de oorlog in Oekraïne. Ook in Nederland kwamen statelijke cyberaanvallen aan het licht. Zo zag een cybersecuritybedrijf hackers meerdere cyberaanvallen uitvoeren op Nederlandse telecom- en mediabedrijven, waarschijnlijk om persoonlijke informatie te vergaren. Daarnaast maakte het ministerie van Defensie bekend Chinese spionagesoftware op een ongerubriceerd onderzoeksnetwerk van de krijgsmacht te hebben aangetroffen. Over deze malware, COATHANGER genaamd, hebben de inlichtingen- en veiligheidsdiensten en het NCSC een rapport gepubliceerd.

Datalekken door ransomware-actoren

Wereldwijd, waaronder ook in Nederland, waren er deze rapportageperiode veelvuldig incidenten door ransomware-actoren. Die actoren persten organisaties lang niet altijd alleen af door losgeld te eisen voor het ontsleutelen van bestanden, maar ook door te dreigen met publicatie van buitgemaakte data. Daarnaast legden sommige ransomware-actoren zich toe op afpersing door enkel te dreigen met publicatie van gestolen data. Illustratief in dat kader is bijvoorbeeld de grootschalige data-exfiltratie[III] bij het MOVEit-incident. Bij deze aanval werd er door de ransomware-actoren geen gebruik gemaakt van versleuteling van bestanden, maar werd een grote hoeveelheid gegevens gestolen waarna organisaties werden afgeperst. Een aantal Nederlandse bedrijven werd hier ook het slachtoffer van. Bij ransomware-aanvallen is niet in alle gevallen publiekelijk bekend of er ransomware is ingezet, of dat de actoren alleen data hebben gestolen. Hoe dan ook lijkt dubbele afpersing nog steeds vaak voor te komen. In ongeveer 50% van de door de Autoriteit Persoonsgegevens (AP) onderzochte ransomware-aanvallen vond data-extractie plaats in combinatie met versleuteling. Dat speelde eind 2023 meer dan aan het begin van 2023.[8]

Minimaal 178 ransomware-aanvallen in Nederland in 2023; aantal slachtoffers vele malen groter

In 2023 hebben in ieder geval 178 ransomware-aanvallen plaatsgevonden in Nederland volgens de AP. De AP baseert de cijfers op een analyse van de wettelijk verplichte datalekmeldingen.[9] Het publiek-private samenwerkingsproject Melissa komt daarentegen uit op minimaal 147 ransomware-aanvallen bij grotere organisaties (vanaf ca. 100 fte) in Nederland in 2023.[10] Melissa heeft deze cijfers gebaseerd op primaire onderzoeksgegevens, zoals politie-aangiftes, geanonimiseerde informatie van cybersecuritybedrijven die direct betrokken zijn bij de afhandeling van deze cyberincidenten en meldingen bij het NCSC.[IV]

Naast de direct getroffen organisaties van een ransomware-aanval, kunnen vele andere organisaties en klanten van die organisaties ook slachtoffer zijn geweest. Aanvallen op digitale serviceproviders (denk bijvoorbeeld aan Internet Service Providers, datacenters en telecombedrijven) kunnen veel andere organisaties, en indirect ook burgers, treffen omdat die afhankelijk zijn van de diensten van deze organisaties. Door de afhankelijkheid van toeleveranciers voor bepaalde producten en diensten, bestaat het risico dat afnemers van deze diensten secundair slachtoffer kunnen worden via de toeleverancierskeketen bij een aanval op een toeleverancier. Alleen al één aanval resulteerde in een datalek van ongeveer 2,5 miljoen Nederlandse personen (zie hieronder).

Aanvallen op toeleveranciers zorgen voor problemen verderop in de keten

Een cyberaanval op de leverancierskeketen veroorzaakt niet alleen schade bij het gecompromitteerde bedrijf, maar ook bij andere organisaties. Deze periode hebben we diverse aanvallen gezien waarbij een bedrijf dat digitale processen verzorgt voor (vele) andere organisaties slachtoffer werd van een cyberaanval, waarna andere bedrijven in de keten in de problemen kwamen. In Nederland waren de dienstverleners Nebu en AddComm slachtoffers van cyberaanvallen. Hierna meldden zowel directe als indirecte klanten van deze bedrijven (potentiële) datalekken. Het kan toeval zijn dat juist deze bedrijven worden aangevallen, maar het kan ook een doelbewuste opstap zijn naar andere organisaties, of bedoeld om de druk van afpersing op te voeren. Deze periode waren er in ieder geval ook aanvallen door geavanceerde actoren die mogelijk bedoeld waren als supplychain-aanval. Zo werd software van 3CX geïnfecteerd met malware, waarna mogelijk de netwerken van duizenden bedrijven gecompromitteerd zijn. Een ander opvallend incident is de backdoor die is aangetroffen in de veelgebruikte

III Data-exfiltratie, ook wel datadiefstal, is een proces tijdens een cyberaanval waarbij data wordt gestolen.

IV Voor een methodologische toelichting op deze cijfers en een verklaring van het verschil, zie bijlage 2.

Linux-software, de datacompressieapplicatie XZ Utils. Hoewel deze aanval nog niet definitief geattribueerd is, wordt er in open bronnen vanuit gegaan dat het een statelijke actor betreft. Hierdoor zou de actor een grote hoeveelheid organisaties hebben kunnen compromitteren. Deze casus toont aan de ene kant dat open source software kwetsbaar kan zijn voor het aanbrengen van een backdoor, maar aan de andere kant het voordeel dat deze manipulatie kan worden ontdekt.

Misbruik van kwetsbaarheden vormde start van een deel van de cyberaanvallen

Het misbruik van kwetsbaarheden blijft een belangrijk startpunt voor een aanval (aanvalsvector). Deze rapportageperiode waren er wereldwijd diverse incidenten waarbij (zeroday) kwetsbaarheden werden misbruikt. Uit gecombineerde data van Google en Mandiant blijkt bijvoorbeeld dat er 97 zerodays zijn misbruikt in heel 2023, tegenover 62 in 2022.[11] Een voorbeeld hiervan is het grootschalige misbruik van de kwetsbaarheden van de VPN-oplossing Ivanti Connect Secure. In dit product zaten meerdere kwetsbaarheden die door zowel statelijke actoren als cybercriminelen zijn misbruikt. Ook in Nederland zijn meerdere organisaties hierdoor getroffen.

Zorgorganisaties slachtoffer van cybercriminelen, ook in Nederland organisaties geraakt

Meer dan eens hebben we deze rapportageperiode gezien dat zorgorganisaties het slachtoffer zijn geworden van cyberaanvallen. Veelal ging het hierbij om ransomware en/of afpersing met gestolen gegevens. Een groot deel daarvan vond plaats in het buitenland en had impact op de te verlenen zorg. Ook is een aantal Nederlandse zorginstellingen geraakt door cyberaanvallen. In Nederland hebben deze voor zover bekend geen impact gehad op de te verlenen zorg. Wel werden organisaties afgeperst met gestolen gegevens en werden gegevens gelekt. Daarbij gaat het veelal om gevoelige persoonsinformatie. Zorginstellingen werden direct getroffen door cyberaanvallen. Maar er waren ook incidenten bij toeleveranciers van de zorg die problemen veroorzaakten voor zorginstellingen. Z-CERT stelt dat leveranciers van zorginstellingen vaker worden getroffen dan zorginstellingen zelf.[12] In het buitenland werd dit geïllustreerd door de ransomware-aanval op een informatiesysteem van Roemeense ziekenhuizen waardoor deze terug moesten naar pen en papier. Ook was er een aanval op een dienstverlener van Britse ziekenhuizen waardoor operaties moesten worden afgezegd. In de VS werd een financiële dienstverlener getroffen door ransomware waardoor de Amerikaanse gezondheidzorg niet meer betaald kreeg en apotheken geen medicijnen konden verstrekken. Dat zorginstellingen direct of indirect worden geraakt, wil niet zeggen dat er sprake is van gerichte doelwitkeuze.

Wereldwijd ondervinden aanbieders van vitale processen hinder van cyberaanvallen

Deze rapportageperiode was er berichtgeving over uiteenlopende soorten (geslaagde) cyberaanvallen waarbij bedrijven in vitale sectoren in westerse landen werden geraakt. Hierbij kan onderscheid worden gemaakt tussen bewuste (voorbereidingshandelingen voor) sabotage, spionage en operaties die ingegeven worden door financieel gewin. Opvallend waren de voorbereidingsactiviteiten voor digitale sabotage door de aan China gelinkte APT Volt Typhoon in de militaire en civiele infrastructuur van de VS. In Ierland vond een cyberincident plaats waarbij vitale processen daadwerkelijk werden verstoord, hoewel de impact hiervan beperkt was en de watervoorziening slechts kortstondig onderbroken werd. Hackers hadden het hierbij gemunt op digitale apparatuur die de watervoorziening regelde. Ook in de VS werden waterautoriteiten gecompromitteerd, al was daar geen sprake van impact op de operationele activiteiten. In dit kader waarschuwde Microsoft ook voor aanvallen op slecht beveiligde OT-systemen. Sinds eind 2023 heeft Microsoft een toename waargenomen in het aantal meldingen van aanvallen gericht op aan internet blootgestelde, slecht beveiligde OT-apparaten. Hierbij zag het kort na het uitbreken van de oorlog tussen Israël en Hamas een stijging in het aantal meldingen van aanvallen tegen OT-systemen van Israëlische makelij.[13] Waarschijnlijk was deze doelwitkeuze gelegen in het gebruik van apparatuur van een Israëlische firma en niet tegen de getroffen organisaties zelf. In Australië hadden diverse grote havens te kampen met de gevolgen van een cyberaanval. DP World, de op een na grootste havenbeheerder van het land, had uit voorzorg het internetverkeer stilgelegd nadat er een cyberaanval was ontdekt. Op Curaçao werden de interne systemen en de klantenservice van elektriciteitsbedrijf Aqualectra getroffen door een ransomware-aanval waardoor deze tijdelijk niet beschikbaar waren.

Als door een incident de gevolgen voor de continuïteit van een dienstverlening een sectorspecifieke drempelwaarde overschrijden, moet een vitale organisatie vanuit de huidige Wet beveiliging netwerk- en Informatiesystemen (Wbni) het incident melden bij het Nationaal Cyber Security Centrum (NCSC).[14] Ondanks incidenten die aangeven dat vitale infrastructuur zeker niet gevrijwaard wordt van cyberincidenten, zijn er in Nederland in 2023 geen meldingen van informatiebeveiligingsincidenten boven de zogeheten drempelwaarde ontvangen.

2023

Maart

Binnenland

- Gevoelige gegevens van werknemers van Attent Zorg en Behandeling gelekt na ransomware-aanval
- Persoonlijke gegevens van 48.000 bezoekers van de Amsterdamse Waterleidingduinen gelekt
- Gegevens gelekt van maritiem dienstverlener Royal Dirkzwager na ransomware-aanval
- Gegevens van 2,5 miljoen klanten van 190 organisaties gelekt na ransomware-aanval op softwareleverancier Nebu

Buitenland

- Spoedafdeling Brussels ziekenhuis Sint-Pieter tijdelijk gesloten na cyberaanval
- Datadiefstal bij tientallen organisaties door misbruik van zerodaylek in GoAnywhere MFT
- Supplychain-aanval op VoIP bedrijf 3CX van vermoedelijke Noord-Koreaanse hackers

April

Binnenland

- Gegevens gepubliceerd van cliënten en medewerker van Joris Zorg door ransomwaregroep
- Tijdelijk geen diensten van provider SKP door ransomware-aanval

Buitenland

- Hackers verstoren websites van de overheid in meer dan de helft van de Duitse deelstaten
- Cybercriminelen stalen gegevens van de Belgische gemeente Herselt met behulp van inloggegevens van een softwareleverancier
- Bereikbaarheid websites van Eurocontrol aangetast door DDoS-aanvallen

Mei

Binnenland

- Rechtspraak.nl en website van de Staten-Generaal tijdelijk slecht tot niet bereikbaar door DDoS-aanvallen
- Klantenportaal van HVC ontoegankelijk door een cyberaanval op een IT-leverancier

Buitenland

- Compromittatie van vitale infrastructuur in de VS

Juni

Binnenland

- Grootschalige gegevensdiefstal na misbruik van kwetsbaarheden in MOVEit, ook Nederlandse organisaties geraakt
- Websites van Nederlandse havens tijdelijk onbereikbaar door DDoS-aanvallen
- Treinverkeer in en rond Amsterdam plat door IT-storing

Juli

Binnenland

- Gegevens van inwoners vier gemeenten gelekt door softwarefout in burgerportaal

Buitenland

- Bedrijfsvoering van Noorse ministeries verstoord, voorstelbaar dat data is gestolen

Augustus

Binnenland

- Bereikbaarheid diverse Nederlandse websites aangetast door DDoS-aanvallen

Buitenland

- Poolse treinen tot stilstand gebracht door vervalst radiostopsignaal

September

Binnenland

- Klanten van Lyca Mobile konden tijdelijk niet bellen en opwaarderen door cyberaanval

Oktober

Binnenland

- Gerichte cyberaanval op International Criminal Court (ICC), impact onbekend, mogelijk data buitgemaakt
- Centrum Informatie en Documentatie Israël (CIDI) doelwit van DDoS-aanvallen

Buitenland

- Strategische documenten van de NAVO gestolen en online gezet door hackers
- Database van European Telecommunications Standards Institute gestolen

2024

November

Binnenland

- Landelijke storing bij noodknopsysteem ouderen en kwetsbaren door ransomware-aanval

Buitenland

- Compromittatie Deense vitale infrastructuur
- Operaties Australische havens verstoord door cyberaanval
- Inwoners Iers dorp twee dagen zonder water door cyberaanval op lokale drinkwatervoorziening
- Compromittatie meerdere waterfaciliteiten VS, maar geen impact op drinkwatervoorziening

December

Binnenland

- Systemen en klantenservice Aqualectra niet bereikbaar door ransomware-aanval

Buitenland

- Aan Iran gelinkte hackers claimen cyberaanvallen op parlement en telecombedrijf Albanië

Januari

Binnenland

- Hackers van APT Sea Turtle richten zich op telecom- en mediabedrijven in Nederland
- Actief misbruik van kwetsbaarheden in Ivanti Connect Secure, ook Nederlandse bedrijven gecompromitteerd

Februari

Binnenland

- Computersysteem Nederlandse defensie gecompromitteerd door Chinese hackers

Buitenland

- Tientallen ziekenhuizen Roemenië offline na ransomware-aanval op IT-platform
- Apotheken en zorgbetalingen in VS ontregeld door ransomware-aanval op dienstverlener

April

Binnenland

- Cybercriminelen stelen gegevens bij chipmaker Nexperia
- Geheime afmeldcodes van duizenden alarmsystemen opvraagbaar door softwarefout
- Russische propaganda te zien op kinderzender na opzettelijke verstoring
- Actief misbruik van kwetsbaarheid in Palo Alto product

Buitenland

- Backdoor ontdekt in veelgebruikte Linux-software

Mei

Binnenland

- Diverse organisaties melden datalek na ransomware-aanval op AddComm
- Malware ontdekt bij verschillende scheepvaartbedrijven
- Problemen met pintransacties door grote landelijke pinstoring

Juni

Binnenland

- Websites politieke partijen tijdelijk niet goed bereikbaar door DDoS-aanvallen
- Webex meta-data inzichtelijk door kwetsbaarheden
- Storingen van mobiel bankieren-apps zorgen voor problemen bij gebruikers
- Gegevens van 60.000 mensen gelekt door slecht beveiligde software
- Deel online dienstverlening RDW niet continu beschikbaar door storing
- Bellen en internetten tijdelijk onmogelijk voor klanten van Odido door problemen met router

Buitenland

- Britse ziekenhuizen annuleren operaties wegens ransomware-aanval op laboratorium
- IT-systeem TeamViewer gecompromitteerd door Russische hackers
- Gevoelige persoonlijke informatie van dienst voor identiteit- en leeftijdsverificatie online toegankelijk

Juli

Binnenland

- Onder meer vliegverkeer en gezondheidszorg ontregeld door wereldwijde computerstoring als gevolg van foutieve update

Augustus

Binnenland

- Overheidsdiensten en vliegverkeer Eindhoven verstoord door softwarefout op netwerk Defensier

Opvallende incidenten Nederland 2023

Maart 2023

Gevoelige gegevens van werknemers van Attent Zorg en Behandeling gelekt na ransomware-aanval
Cybercriminelen van de Qilin ransomwaregroep hebben kopieën van paspoorten, salarisstroken, geheimhoudingsverklaringen en vertrouwelijke interne communicatie gelekt van werknemers die werkzaam zijn of waren bij Attent Zorg en Behandeling. De organisatie werd in februari slachtoffer van een ransomware-aanval. Na de hack waren de interne IT-systemen en het e-mail- en telefoniesysteem niet meer toegankelijk. De cybercriminelen stelden dat zij honderden gigabytes aan data hadden gestolen, waarvan een deel werd gepubliceerd.[15]

Persoonlijke gegevens van 48.000 bezoekers van de Amsterdamse Waterleidingduinen gelekt
Hackers hebben gegevens van mensen die tussen 2015 en 2021 online parkeer- en toegangstickets voor de Amsterdamse Waterleidingduinen kochten weten te bemachtigen. Het betreft de namen en de rekeningnummers van 48.000 bezoekers die vermoedelijk eerder via een beveiligingslek in de website van Waternet zijn gestolen. Dit kwam aan het licht tijdens een grootschalig politieonderzoek naar computervredebreuk, datadiefstal, afpersing, afdreiging en witwassen.[16]

Gegevens gelekt van maritiem dienstverlener Royal Dirkzwager na ransomware-aanval
De Nederlandse maritiem dienstverlener Royal Dirkzwager is getroffen door een ransomware-aanval van de Play ransomwaregroep. Het bedrijf had ongeveer een week nodig om zijn systemen volledig te herstellen en de diensten te hervatten. Klanten moesten noodmaatregelen treffen, waaronder fysiek toezicht op boorplatforms.[17] Daarnaast lekte de hacker vertrouwelijke gegevens van de organisatie, waaronder werknemers-ID's, paspoorten en contracten.[18]

Gegevens van 2,5 miljoen klanten van 190 organisaties gelekt na ransomware-aanval op softwareleverancier Nebu
Als gevolg van een ransomware-aanval op softwareleverancier Nebu zijn persoonsgegevens van ongeveer 2,5 miljoen personen van 190 organisaties in Nederland gelekt.[19] Zo zijn gegevens gelekt van vijf tot tien marktonderzoeksbureaus. Hierbij gaat het hoofdzakelijk om namen, e-mailadressen en telefoonnummers. De marktonderzoeksbureaus maakten gebruik van de software van Nebu.[20] Deze data bevatte persoonsgegevens die de klanten van de marktonderzoeksbureaus aan hen hadden verstrekt.

April 2023

Gegevens gepubliceerd van cliënten en medewerker van Joris Zorg door ransomwaregroep
Cybercriminelen hebben gestolen gegevens van cliënten en medewerkers van de Brabantse zorginstelling Joris Zorg gepubliceerd. In december 2022 deed zich bij de organisatie een cyberaanval voor, waarbij hackers van de LockBit ransomwaregroep losgeld eisten. De criminelen claimden dat er honderd gigabyte aan data is gestolen. Zij publiceerden deze vervolgens in april 2023, nadat er niet werd betaald.[21]

Tijdelijk geen diensten van provider SKP door ransomware-aanval
De provider Stichting Kabeltelevisie Pijnacker (SKP) kon tijdelijk geen internet- en televisiediensten leveren aan klanten door een ransomware-aanval. De provider kampte eveneens met problemen met de telefoniedienst.[22]

Mei 2023

Rechtspraak.nl en website van de Staten-Generaal tijdelijk slecht tot niet bereikbaar door DDoS-aanvallen
Het openbare deel van Rechtspraak.nl was een aantal dagen niet of slecht bereikbaar door een DDoS-aanval. Om dezelfde reden was de website van de Staten-Generaal tijdelijk moeilijk bereikbaar.[23] Volgens een cybersecuritybedrijf zijn pro-Russische hacktivisten vermoedelijk verantwoordelijk.[24]

Klantenportaal van HVC ontoegankelijk door een cyberaanval op een IT-leverancier
Een klantenportaal van energieleverancier en afvalverwerker HVC was tijdelijk ontoegankelijk door een cyberaanval op een datacentrum van een IT-leverancier. Voor HVC betekende de aanval dat medewerkers het klantsysteem niet in konden en de facturering werd vertraagd. Mogelijk hebben kwaadwillenden ook gegevens van klanten ingezien of gestolen. Het bedrijf vermoedt dat dit niet het geval is, maar kan het ook niet uitsluiten.[25] Er zou geen losgeld zijn geëist van HVC.[26]

Juni 2023

Grootschalige gegevensdiefstal na misbruik van kwetsbaarheden in MOVEit, ook Nederlandse organisaties geraakt
Wereldwijd werden organisaties slachtoffer van gegevensdiefstal nadat cybercriminelen van Clop een grootschalige campagne uitvoerden door misbruik te maken van een zeroday-kwetsbaarheid in filetransfer-applicatie MOVEit Transfer.[27] In Nederland maakten o.a. Landal Greenparks en Shell naar aanleiding van deze campagne melding van een datalek. Er zou ten minste een tiental Nederlandse organisaties zijn geraakt.[28] In de maanden na de bekendwording van de aanvallen kwamen er steeds meer slachtoffers naar voren. Beveiligingsbedrijf Emsisoft schat in dat wereldwijd meer dan 2700 bedrijven slachtoffer zijn geworden.[29]

Websites van Nederlandse havens tijdelijk onbereikbaar door DDoS-aanvallen
De websites van de havenbedrijven in Rotterdam, Amsterdam en Den Helder waren een paar uur onbereikbaar door DDoS-aanvallen. De website van de Groningse Zeehavens was twee dagen niet te bereiken. De aanvallen zijn opgeëist door een pro-Russische hacktivistische groepering.[30]

Treinverkeer in en rond Amsterdam plat door IT-storing
Treinverkeer in en rond Amsterdam werd ernstig verstoord doordat de verkeersleidingspost van ProRail kampte met een IT-storing. De storing zorgde ook voor problemen elders op het spoor en gestrande reizigers die de nacht niet thuis konden doorbrengen.[31]

Juli 2023

Gegevens van inwoners vier gemeenten gelekt door softwarefout in burgerportaal
Gegevens van inwoners van vier gemeenten zijn gelekt door een softwarefout in een digitaal burgerportaal. Na de installatie van een software-update was er een foutieve knop zichtbaar in het burgerportaal. Als op die knop werd gedrukt, toonde het systeem in enkele gevallen een document van iemand anders. In geval van de gemeente Apeldoorn zijn gegevens van meer dan 29 inwoners gelekt, van wie naam, adres, geboortedatum en BSN zichtbaar waren. Welke andere gemeenten zijn getroffen is niet bekend.[32]

Augustus 2023

Bereikbaarheid diverse Nederlandse websites aangetast door DDoS-aanvallen
In augustus kampten Nederlandse websites met DDoS-aanvallen waardoor deze tijdelijk niet of slecht bereikbaar waren. Begin augustus waren onder meer Maastricht Airport, de gemeente Vlaardingen en de Bank Nederlandse Gemeenten doelwit.[33] Later in de maand werden er ook aanvallen uitgevoerd op de Luchthavens van Groningen en Schiphol. Alleen de website van Groningen Airport Eelde was tijdelijk onbereikbaar.[34] Pro-Russische hacktivisten claimden de aanvallen. Ook een aantal lokale nieuwswebsites was tijdelijk uit de lucht door DDoS-aanvallen, het was onbekend wie ervoor verantwoordelijk was.[35]

September 2023

Klanten van Lyca Mobile konden tijdelijk niet bellen en opwaarderen door cyberaanval
De provider Lyca Mobile bevestigt het slachtoffer te zijn geworden van een cyberaanval welke wereldwijd impact had, zo ook in Nederland. Door die aanval konden klanten niet opwaarderen. De aanval had ook gevolgen voor nationaal en internationaal bellen. Om wat voor aanval het gaat is niet bekend gemaakt.[36]

Oktober 2023

Gerichte cyberaanval op International Criminal Court (ICC), impact onbekend, mogelijk data buitgemaakt
Het ICC in Den Haag is slachtoffer geworden van een cyberaanval. Om wat voor aanval het gaat en wat de impact is, is niet bekend gemaakt. Bij het ICC bestaat het vermoeden dat het zou gaan om spionage en ondermijning van de werkzaamheden.[37] In media werd gesteld dat er gevoelige documenten zijn buitgemaakt.[38]

Centrum Informatie en Documentatie Israël (CIDI) doelwit van DDoS-aanvallen
In oktober en november was het CIDI mikpunt van voortdurende DDoS-aanvallen. Volgens het online beveiligingsbedrijf dat is ingehuurd door CIDI waren de aanvallen van ongekende omvang. Het is onbekend wie ervoor verantwoordelijk is.[39]

November 2023

Landelijke storing bij noodknopsysteem ouderen en kwetsbaren door ransomware-aanval
De werking van een noodknopsysteem, door ouderen en kwetsbaren in Nederland gebruikt, was tijdelijk verstoord door een ransomware-aanval op Tunstall. Bij deze aanval werden systemen en gegevens versleuteld. De aanval zou zijn begrensd tot de meldkameromgeving van het bedrijf en geen aangrenzende systemen hebben getroffen. Bij de aanval hebben criminelen toegang gehad tot gegevens, om welke gegevens het precies gaat is niet bekend.[40]

December 2023

Systemen en klantenservice Aqualectra niet bereikbaar door ransomware-aanval
Interne systemen en de klantenservice van elektriciteitsbedrijf Aqualectra (Curaçao) waren niet bereikbaar wegens een ransomware-aanval.[41] Door de aanval moest het bedrijf tijdelijk alle online verbindingen uitzetten. Hoewel het bedrijf de schade wist te minimaliseren, hebben hackers wel verouderde data buitgemaakt. Ook zouden de hackers losgeld hebben geëist. Het bedrijf heeft besloten niet te betalen en stelt dat er geen gevoelige klantdata is buitgemaakt. De water- en stroomleverancier benadrukte verder dat recente stroomuitvallen op Curaçao niet veroorzaakt zijn door de aanval.[42]

Opvallende incidenten Nederland 2024

Januari 2024

Hackers van APT Sea Turtle richten zich op telecom- en mediabedrijven in Nederland
Volgens een cybersecuritybedrijf hebben hackers APT Sea Turtle het afgelopen jaar cyberaanvallen uitgevoerd op Nederlandse telecom- en mediabedrijven. Hierbij zouden de hackers het vooral hebben voorzien op persoonsgegevens van specifieke groepen Nederlanders[43]

Actief misbruik van kwetsbaarheden in Ivanti Connect Secure, ook Nederlandse bedrijven gecompromitteerd
Ivanti waarschuwde deze maand voor twee kwetsbaarheden in Ivanti Connect Secure en Ivanti Policy Secure Gateways waardoor een ongeauthenticeerde aanvaller commando's op het VPN-systeem kan uitvoeren. Cybersecurityonderzoekers wisten al snel te melden dat er grootschalig misbruik plaatsvond. Verscheidende aan China gelinkte hackersgroepen zouden de kwetsbaarheden in Ivanti Connect Secure misbruiken voor cyberaanvallen, waaronder op de Energiesector in de VS.[44] Het NCSC constateerde dat ook in Nederland bedrijven via deze kwetsbaarheden zijn gecompromitteerd.

Februari 2024

Computersysteem Nederlandse defensie gecompromitteerd door Chinese hackers
Het ministerie van Defensie heeft in 2023 Chinese spionagesoftware op een ongerubriceerd computersysteem van de krijgsmacht gevonden. Volgens de MIVD ging het om geavanceerde spionage-malware die door Chinese hackers is geplaatst. De malware, COATHANGER genaamd, werd aangetroffen op een losstaand computernetwerk voor Research and Development, dat minder dan 50 gebruikers telde.[45]

April 2024

Cybercriminelen stelen gegevens bij chipmaker Nexperia
Data van Nexperia is gestolen en (deels) gelekt na een aanval door cybercriminelen. In eerste instantie zijn interne e-mails van het bedrijf gelekt, maar de hackers claimden ook te beschikken over handelsgeheimen, chipontwerpen en klantgegevens.[46]

Russische propaganda te zien op kinderzender na opzettelijke verstoring
De uitzending van kinderzender BabyTV werd door signal hijacking onderbroken waarna er een tijdlang Russische propaganda werd getoond op de kinderzender in Nederland, Scandinavië en Portugal.[47] Nadat in maart een incident plaatsvond, volgde in april wederom een onderbreking waarbij Russische propaganda werd getoond op BabyTV. De actie lijkt niet gericht te zijn op BabyTV, maar was nevenschade van een bredere actie gericht op verstoring van uitzendingen van Oekraïense zenders.[48]

Geheime afmeldcodes van duizenden alarmsystemen opvraagbaar door softwarefout
Door een lek in software van Carrier Global was het een jaar lang mogelijk om duizenden alarmsystemen op afstand af te melden. Het lek bevond zich in een app van Carrier Global die installateurs van alarmcentrales gebruiken om toegang te krijgen tot gegevens van hun eigen klantenbestand: MAS Mobile Classic. De software wordt onder meer door de alarmcentrale SMC gebruikt en raakt minstens 26000 actieve Nederlandse beveiligingssystemen. Door een fout in de software van de server waarop de app de data bewaarde, waren de geheime gegevens online toegankelijk. Naast afmeldcodes waren ook de thuisadressen van CEOs, Quote 500-leden, BN'ers en zelfs een voormalig minister opvraagbaar. Prominenten kregen van SMC een aparte aanduiding waardoor zij makkelijker vindbaar waren. Volgens het bedrijf zijn er geen indicaties dat kwaadwillenden misbruik hebben gemaakt van de fout.[49]

Actief misbruik van kwetsbaarheid in Palo Alto product
Het NCSC heeft actief misbruik in Nederland waargenomen van een kwetsbaarheid in Palo Alto PAN-OS. Dit is software die draait op alle Palo Alto Networks® next-generation firewalls.[50]

Mei 2024

Diverse organisaties melden datalek na ransomware-aanval op AddComm
Dienstverlener AddComm is slachtoffer geworden van een ransomware-aanval. Hierbij werden systemen versleuteld en is data ontvreemd.[51] Er werd ook data buitgemaakt van een selecte groep AddComm klanten. Welke klanten dit zijn is niet bekend gemaakt, maar onder meer ABN Amro, de Regionale Belasting Groep, Dunea, Essent en verschillende gemeenten meldden potentiële datalekken. AddComm is een communicatiebedrijf dat klantcommunicatie verzorgt voor verschillende organisaties..[52]

Malware ontdekt bij verschillende scheepvaartbedrijven
ESET heeft malware ontdekt in de systemen van verschillende scheepvaartbedrijven in Noorwegen, Griekenland en Nederland. Dit trof zowel vrachtschepen als kantoorsystemen. In sommige gevallen kwam de malware van een USB-stick. ESET schrijft de aanvallen toe een Chinese APT.[53]

Problemen met pintransacties door grote landelijke pinstoring
Op 16 mei was er een grote landelijke pinstoring, welke problemen veroorzaakte bij 30 tot 40% van de pintransacties. De storing duurde zo'n drie uur en zorgde voor lange rijen in winkels. Het probleem lag bij een van de transactieverwerkers. Er is niet bekend gemaakt of het een menselijke of technische fout betrof.[54]

Juni 2024

Websites politieke partijen tijdelijk niet goed bereikbaar door DDoS-aanvallen
Op de dag van de Europese verkiezingen in Nederland meldden verschillende Nederlandse politieke partijen dat hun websites slecht bereikbaar waren door DDoS-aanvallen. De aanvallen werden opgeëist door pro-Russische hacktivisten.[55]

Webex meta-data inzichtelijk door kwetsbaarheden
Door journalistiek onderzoek werd bekend dat er kwetsbaarheden in de cloudversie van Cisco Webex zaten, waardoor metagegevens van vergaderingen achterhaald konden worden. De journalist wist gegevens te verzamelen van overheden en bedrijven in Duitsland, Nederland, Italië, Oostenrijk, Frankrijk, Zwitserland, Ierland en Denemarken. Daarbij was zij ook in staat om met twee online vergaderingen mee te luisteren. Het NCSC heeft geen aanwijzingen dat er actief misbruik van deze kwetsbaarheid heeft plaatsgevonden.[56]

Storingen van mobiel bankieren-apps zorgen voor problemen bij gebruikers
In juni waren er verschillende keren verstoringen van mobiel bankieren apps. Zo waren op 21 en 24 juni sprake van een urenlange storing bij de bankieren-apps van SNS, ASN en Regiobank, allen onderdeel van de Volksbank. Niet alle klanten werden in gelijke mate getroffen. De oorzaak is niet bekend.[57] Daarnaast kampte die week ook ING met een technische storing. Hierdoor functioneerde de mobielbankieren app niet goed en konden geen overboekingen worden gedaan. De storing zou zijn veroorzaakt door een brandalarm in een datacenter. Daar zorgde een gasblussysteem ervoor dat 'enkele systemen' werden uitgeschakeld.[58]

Gegevens van 60.000 mensen gelekt door slecht beveiligde software
Een ethisch hacker heeft een datalek ontdekt bij DUO, waarbij e-mailadressen van 60.000 mensen met een studieschuld korte tijd online in te zien waren. Het gaat om schuldenaren die zijn benaderd voor een enquête, waarbij de gebruikte software van Survalyzer slecht beveiligd bleek. Omdat veel e-mailadressen een naam bevatten, was vaak duidelijk wie de schuldenaren waren.[59]

Deel online dienstverlening RDW niet continu beschikbaar door storing
Op donderdag 13 juni was er bij de RDW een storing waardoor een deel van de online dienstverlening, zoals de tenaamstelling van voertuigen en het afmelden van APK, niet continu beschikbaar was. De storing ontstond toen een schoningsscript niet tijdig klaar was en voor vertraging/verstoring zorgde op het moment dat de online dienstverlening op gang kwam. Het terugrolmechanisme dat daarna in werking trad, duurde langer dan verwacht. De dag na de storing was de branche nog druk met het inhalen van achterstanden.[60]

Bellen en internetten tijdelijk onmogelijk voor klanten van Odido door problemen met router
Telecomprovider Odido kampte op 30 juni met storingen in verschillende regio's waardoor klanten tijdelijk niet meer konden bellen en internetten. Odido gaf aan dat er een probleem was met een router van het hoofdnetwerk.[61]

Het Jaarbeeld beslaat de periode maart 2023 tot en met juni 2024. Met het oog op de impact zijn twee incidenten opgenomen die na deze periode speelden.

Juli 2024

Onder meer vliegverkeer en gezondheidszorg ontregeld door wereldwijde computerstoring als gevolg van foutieve update
Op 19 juli introduceerde CrowdStrike een software-update die ervoor zorgde dat er wereldwijd zo'n 8,5 miljoen Windowssystemen onbruikbaar werden.[62] De fout zorgde voor 'Blue Screens of Death' op Windowssystemen.[63] Dit zorgde wereldwijd voor grote problemen, zo ook in Nederland. Schiphol annuleerde vluchten en in sommige ziekenhuizen werd de zorg afgeschaald. Ook delen van de overheid werden geraakt. Zo ondervonden het ministerie van Buitenlandse Zaken en het UWV hinder van de storing.[64] Hoewel een deel van de bedrijven na het uitvoeren van de arbeidsintensieve workaround relatief snel weer online was, ondervond een deel van de CrowdStrike klanten ook na een paar dagen nog problemen.

Augustus 2024

Overheidsdiensten en vliegverkeer Eindhoven verstoord door softwarefout op netwerk Defensie
Eind augustus kampten hulpdiensten en diverse overheidsinstellingen met een IT-storing. Hulpdiensten hadden hierdoor problemen met hun communicatie- en alarmeringssysteem, waardoor ze onderling moeilijker konden communiceren. Ambtenaren van diverse ministeries konden niet inloggen op werksystemen. Ook Eindhoven Airport ondervond hinder vanwege het gebruik van datzelfde netwerk. Daar konden vliegtuigen niet opstijgen of landen. Er kwamen ook berichten van diverse gemeenten waarbij de dienstverlening was verstoord. Zo konden er geen rijbewijzen en paspoorten worden afgegeven. Daarnaast kampte DigiD met een storing. [65] De oorzaak van de problemen lag in de toegangsverlening tot het zogenoemde Netherlands Armed Forces Integrated Network (NAFIN). Dat is een zwaarbeveiligd netwerk dat onder meer Defensielocaties met elkaar verbindt en ook wordt gebruikt bij datacenters van verschillende ministeries en politiebureaus. Door een fout in de softwarecode ontstond een probleem in de tijdsynchronisatie op het netwerk. Er is volgens de minister van Defensie vooralsnog geen indicatie dat de storing is veroorzaakt door een kwaadwillende partij. [66]

Opvallende incidenten in buitenland 2023

Maart 2023

Spoedafdeling Brussels ziekenhuis Sint-Pieter tijdelijk gesloten na cyberaanval
De spoedeisende hulp van het Brusselse ziekenhuis Sint-Pieter was op 11 maart tijdelijk gesloten door een cyberaanval. Hierdoor waren onder meer de patiëntendossiers en de telefoonlijnen geblokkeerd, melden Belgische media. Telefoontjes naar 112 werden omgeleid naar andere ziekenhuizen. Patiënten zouden geen hinder hebben ondervonden en ook is er volgens het ziekenhuis geen data gestolen. Uit open bronnen komt niet naar voren om wat voor aanval het precies gaat.[67]

Datadiefstal bij tientallen organisaties door misbruik van zerodaylek in GoAnywhere MFT
Tientallen internationale organisaties meldden dat er gegevens bij hen zijn gestolen door misbruik van een zeroday-kwetsbaarheid in GoAnywhere MFT. Het gaat onder andere om Procter & Gamble, Hitachi Energy, Community Health Systems (CHS), Crown Resorts, de Hatch Bank, het Britse Pension Protection Fund, de stad Toronto en Brightline. Criminelen achter de Clop-ransomware hebben de aanval opgeëist en claimen data te hebben gestolen van tenminste 72 organisaties.[68]

Supplychain-aanval op VoIP bedrijf 3CX van vermoedelijke Noord-Koreaanse hackers
Hackers hebben waarschijnlijk de netwerken van duizenden bedrijven gecompromitteerd als gevolg van een supplychain-aanval op het zakelijke telefoonbedrijf 3CX. In de officiële desktopapplicatie van de populaire VoIP-software 3CX werd malware aangetroffen. De software wordt wereldwijd gebruikt door 600.000 duizend bedrijven. De feitelijke impact van deze grootschalige aanval op organisaties is echter onduidelijk.[69] In Europa zouden op deze manier in ieder geval twee vitale infrastructuurorganisaties zijn geraakt. [70] 3CX en o.a. Symantec stelden dat Noord-Koreaanse hackers hiervoor verantwoordelijk waren.[71]

April 2023

Hackers verstoren websites van de overheid in meer dan de helft van de Duitse deelstaten
In ruim de helft van de Duitse deelstaten waren verschillende websites van overheidsinstanties het doelwit van DDoS-aanvallen. Daardoor waren officiële staatssites, politiewebsites en sites van het ministerie van Binnenlandse Zaken een tijdlang onbereikbaar. Het Duitse Openbaar Ministerie stelde dat er aanwijzingen zijn dat de aanvallers een pro-Russische achtergrond hebben.[72]

Cybercriminelen stalen gegevens van de Belgische gemeente Herselt met behulp van inloggegevens van een softwareleverancier
Cybercriminelen kregen toegang tot de servers van de Belgische gemeente Herselt met behulp van inloggegevens van een softwareleverancier. Met behulp van malware stalen zij vervolgens 180 gigabyte aan gegevens, waaronder persoonsgegevens van inwoners. Om het incident te kunnen onderzoeken werden systemen afgesloten, waardoor een aanzienlijk deel van de gemeentelijke diensten dagenlang waren verstoord.[73]

Bereikbaarheid websites van Eurocontrol aangetast door DDoS-aanvallen
Enkele websites van Eurocontrol, de internationale organisatie die de luchtverkeersleiding in Europa coördineert, zijn getroffen door een DDoS-aanval. Een pro-Russische hackgroep heeft de aanval opgeëist. Eurocontrol stelt dat de aanval onderbrekingen van de websites heeft veroorzaakt, maar dat deze geen enkele impact heeft gehad op de Europese luchtvaart.[74]

Mei 2023

Compromittatie van vitale infrastructuur in de VS
De Verenigde Staten en Microsoft stellen dat hackers de vitale Amerikaanse infrastructuur hebben geïnfiltreerd, mogelijk in voorbereiding op eventuele sabotagehandelingen. De hackers, gevolgd als Volt Typhoon, zouden sinds medio 2021 actief zijn en zich vooral richten op vitale Amerikaanse infrastructuur.[75] Volgens de Amerikaanse autoriteiten is Volt Typhoon een vanuit China opererende groep.[76] Amerikaanse Functionarissen stelden dat China ernaar streeft de toegang die het heeft verkregen tot de Amerikaanse organisaties te benutten in geval van een oorlog of conflict, hierbij met een schuin oog kijkend naar de geopolitieke situatie rondom Taiwan.[77]

Juli 2023

Bedrijfsvoering van Noorse ministeries verstoord, voorstelbaar dat data is gestolen
Twaalf Noorse ministeries zijn gehackt, waarbij de aanvallers gebruik maakten van kwetsbaarheden in Ivanti Endpoint Manager Mobile. De hackers zouden mogelijk toegang hebben verkregen tot gevoelige data en het is voorstelbaar dat deze ook is gestolen. Het is niet bekend wie er achter de aanval zit. Door de cyberaanval konden ambtenaren op twaalf verschillende ministeries niet inloggen op hun e-mailadres en andere applicaties.[78]

Augustus 2023

Poolse treinen tot stilstand gebracht door vervalst radiostopsignaal
Kwaadwillenden hebben met een ongeautoriseerd radiostopsignaal meerdere treinen tot stilstand gebracht. De actor zou hierbij ook het Russische volkslied en een toespraak van de Russische president hebben uitgezonden. [79]

Oktober 2023

Strategische documenten van de NAVO gestolen en online gezet door hackers
Ruim 3.000 NAVO-documenten verschenen online nadat hackers van de hackgroep SiegedSec beweerden de NAVO te hebben gehackt. De hackers zouden mogelijk hebben ingebroken op ten minste vier webportalen, waarbij het gaat om niet-geclassificeerde NAVO-websites.[80]

Database van European Telecommunications Standards Institute gestolen
Het European Telecommunications Standards Institute (ETSI), gevestigd in Frankrijk, heeft laten weten dat hackers een database hebben gestolen die de gebruikers identificeert. ETSI heeft meer dan 900 leden uit meer dan 60 landen, waaronder particuliere bedrijven, onderzoeksinstellingen, de academische wereld, de overheid en publieke organisaties. Het is onduidelijk welke informatie over hen in de gestolen database staat. Het is niet duidelijk of de aanval financieel gemotiveerd was of dat de hackers de bedoeling hadden de lijst met gebruikers te bemachtigen voor bijvoorbeeld spionagedoeleinden.[81]

November 2023

Compromittatie Deense vitale infrastructuur
SektorCERT, een non-profit cyberbeveiligingscentrum voor vitale sectoren in Denemarken, heeft gemeld dat aanvallers in mei 2023 toegang hebben verkregen tot de systemen van 22 bedrijven die toezicht hielden op verschillende componenten van de Deense energie-infrastructuur. De meeste aanvallen zouden mogelijk zijn geweest omdat de bedrijven hun firewalls niet hadden geüpdatet. SektorCERT verwacht dat een statelijke actor verantwoordelijk is. De aanvallen waren volgens de onderzoekers nauwgezet gepland en gecoördineerd, het doel zou het verzamelen van inlichtingen zijn.[82]

Operaties Australische havens verstoord door cyberaanval
In Australië hadden diverse grote havens te kampen met de gevolgen van een cyberaanval. DP World, de op een na grootste havenbeheerder van het land, had uit voorzorg het internetverkeer stilgelegd nadat er een cyberaanval zou zijn ontdekt. Media berichtten dat er hackers in het systeem zouden zitten.[83] Het zou niet gaan om ransomware, wel is er data gestolen. Door de verstoring strandden meer dan 30.000 containers.[84]

Inwoners Iers dorp twee dagen zonder water door cyberaanval op lokale drinkwatervoorziening
In Ierland vond een cyberincident plaats waarbij een lokale watervoorziening kortstondig onderbroken werd. Hackers hadden het hierbij gemunt op digitale apparatuur van Israëlische makelij die de watervoorziening regelde. Er zouden anti-Israëlische boodschappen op de gehackte apparatuur zijn getoond.[85]

Compromittatie meerdere waterfaciliteiten VS, maar geen impact op drinkwatervoorziening
Diverse waterfaciliteiten in de VS zijn gehackt. Zo werd een van de boosterstations van de gemeentelijke waterautoriteit van Aliquippa gehackt door de Cyber Av3ngers.[86] En ook in Pennsylvania werd een waterfaciliteit slachtoffer van een cyberaanval. De cyberaanvallen hebben niet geleid tot enige verstoring van de watervoorzieningen of tot een bedreiging voor de kwaliteit van het drinkwater.[87] De aanvallers richtte zich volgens Amerikaanse autoriteiten op Israëlische apparatuur die in gebruik is bij deze faciliteiten. De aanvallen zijn door de VS gelinkt aan Iraanse hackers en worden in verband gebracht met het conflict tussen Israël en Hamas. Amerikaanse en Israëlische autoriteiten attribueren 'Cyber Av3ngers' aan de Iraanse IRGC.[88]

December 2023

Aan Iran gelinkte hackers claimen cyberaanvallen op parlement en telecombedrijf Albanië
In de laatste week van 2023 zijn het Albanese parlement en het telecombedrijf One Albania het doelwit geworden van cyberaanvallen. De exacte omvang en reikwijdte van de aanvallen zijn niet bekend. Een aan Iran gelinkte hackersgroep, genaamd Homeland Justice, heeft via hun Telegramkanaal de verantwoordelijkheid voor de aanvallen opgeëist. Ze beweerden ook nog een tweede telecombedrijf en de nationale luchtvaartmaatschappij Air Albania te hebben gehackt.[89]

Opvallende incidenten in buitenland 2024

Februari 2024

Tientallen ziekenhuizen Roemenië offline na ransomware-aanval op IT-platform
Tientallen ziekenhuizen in Roemenië werden gedwongen om weer met pen en papier te werken nadat criminelen een ransomware-aanval hadden uitgevoerd op een veelgebruikt IT-platform. Bij een aantal van de ziekenhuizen werden gegevens versleuteld, andere werden losgekoppeld van het internet om verdere problemen te voorkomen.[90]

Apotheken en zorgbetalingen in VS ontregeld door ransomware-aanval op dienstverlener
Apotheken in de Verenigde Staten werden ontregeld door een ransomware-aanval op Change Healthcare en hadden daardoor problemen bij het verwerken van recepten voor patiënten. Hierdoor konden patiënten geen medicatie ophalen bij hun apotheek.[91] Change Healthcare verwerkt naast medicijnrecepten ook declaraties voor apothekers en zorgverzekeraars, hierdoor werden zorgverleners niet uitbetaald en was niet duidelijk of behandelingen werden vergoed.[92] Het herstellen van alle systemen duurde weken.[93] De hackers zouden (bijzondere) persoonsgegevens van een groot deel van de Amerikaanse bevolking hebben bemachtigd.[94] Slechts enkele weken na de aanval en het betalen van het losgeld, werd het bedrijf nogmaals afgeperst.

April 2024

Backdoor ontdekt in veelgebruikte Linux-software
Er is een ernstige kwetsbaarheid (CVE-2024-3094), in de vorm van een backdoor, ontdekt in de software library liblzma van XZ Utils. Dit is een opensource datacompressieapplicatie die in veel distributies van Linux aanwezig is. Via de backdoor kan een aanvaller op afstand toegang tot systemen krijgen. Gezien de complexiteit van de aanval is het beeld ontstaan dat het gaat om de bewuste creatie van een backdoor waar mogelijk jarenlang moeite in is gestoken. In open bronnen wordt geschreven dat er mogelijk een statelijke actor verantwoordelijk is.[95]

Juni 2024

Britse ziekenhuizen annuleren operaties wegens ransomware-aanval op laboratorium
De systemen van het laboratorium Synnovis werden versleuteld waardoor het bedrijf minder aanvragen kon verwerken. Dit had een significante impact op de werkzaamheden van verschillende ziekenhuizen.[96] Britse ziekenhuizen waren genoodzaakt operaties te staken als gevolg van een ransomware-aanval op een serviceprovider.[97]

IT-systeem TeamViewer gecompromitteerd door Russische hackers
Hackers wisten interne IT-systemen van het Duitse TeamViewer binnen te dringen, hierbij maakte het gebruik van inloggegevens van een medewerker. De aanval, welke het bedrijf toeschrijft aan Russische staatshackers, zou geen gevolgen hebben voor klanten. Het aangevallen interne IT-systeem staat volgens TeamViewer volledig los van de productieomgeving en klantgegevens. De hackers zouden wel de directory data van medewerkers hebben gekopieerd en daarbij toegang hebben gekregen tot namen, zakelijke contactinformatie en versleutelde wachtwoorden.[98]

Gevoelige persoonlijke informatie van dienst voor identiteit- en leeftijdsverificatie online toegankelijk
AU10TIX, een bedrijf dat identiteits- en leeftijdsverificatie verzorgt voor onder andere TikTok, Uber en X, heeft gevoelige gebruikersgegevens gelekt. Inloggegevens voor een loggingplatform van AU10TIX stonden meer dan een jaar online, waardoor onbevoegden toegang konden krijgen tot gevoelige persoonlijke informatie en kopieën van identiteitsdocumenten van gebruikers. De gelekte gegevens omvatten namen, geboortedata, nationaliteiten, identificatienummers en afbeeldingen van paspoorten, rijbewijzen en identiteitsbewijzen. Ook resultaten van verificatieprocessen waren zichtbaar.[99]

Internationale acties tegen kwaadwillenden en hun infrastructuur

Internationale operaties van handhavings- en opsporingsinstanties verstoren criminele infrastructuur

Deze rapportageperiode zijn er diverse internationale operaties geweest waarbij opsporingsinstanties criminele infrastructuur verstoorden. In 2023 werd bijvoorbeeld tijdens een internationale actie van politie en justitie een van de grootste wereldwijde botnets, Qakbot, onschadelijk gemaakt. In Nederland werden 22 servers in beslag genomen en ook in Frankrijk en Duitsland werden servers offline gehaald.[100] In 2024 verstoorden Europol en meerdere politiediensten met 'Operatie Cronos' de activiteiten van hackersgroep LockBit. De Nederlandse politie speelde hierbij een belangrijke rol, zij haalde dertien belangrijke servers offline.[101] Later dat jaar volgde een gecoördineerde, internationale operatie van opsporingsautoriteiten waarbij meerdere botnets ontmanteld werden die een sleutelrol hadden bij wereldwijde cybercriminaliteit. Tijdens deze operatie, genaamd Operation Endgame, zijn wereldwijd meer dan 100 computerservers offline gehaald en werden er meer dan 2.000 domeinnamen overgenomen. In Nederlandse datacentra heeft de politie tientallen servers in beslag genomen.[102] Met de door Europol gecoördineerde 'Operation MORPHEUS' werd crimineel gebruik van de legitieme tool Cobalt Strike aangepakt en werden bijna 600 IP-adressen offline gehaald. Bij de operatie werkten diverse politiediensten, waaronder ook de Nederlandse, samen met private bedrijven.[103]

Cybercriminelen gearresteerd en/of op sanctielijst

Deze rapportageperiode werd niet alleen gekenmerkt door de verstoring van criminele infrastructuur, ook zagen we dat er cybercriminelen werden gearresteerd, al dan niet als onderdeel van die verstoring. In Parijs werd in oktober 2023 een malware ontwikkelaar gearresteerd die betrokken zou zijn bij de Ragnar Locker ransomware. De man was afkomstig uit Tsjechië. Ook andere verdachten werden ondervraagd en in Oekraïne vond een huiszoeking plaats.[104] Tijdens een operatie waarbij het ransomwaregroep LockBit in het vizier werd genomen, werd niet alleen de criminele infrastructuur verstoord, maar werden er in Polen en Oekraïne ook twee personen gearresteerd. [105] Daarnaast werden vijf personen aangeklaagd door Amerikaanse en Franse autoriteiten. In relatie tot de eerder benoemde 'Operation Endgame' werd een man gearresteerd. Deze zou werken voor de ransomwaregroepen Conti en LockBit.[106]

Voor het eerst, en op initiatief van Nederland, zijn cybercriminelen door de EU op de sanctielijst geplaatst. In totaal gaat het om zes hackers, waaronder twee cybercrime kopstukken. Zij zijn verantwoordelijk voor cyberoperaties die in de EU en in Oekraïne veel schade hebben veroorzaakt. Als gevolg van de sanctionering worden hun Europese tegoeden bevroren en ze mogen de EU niet meer in. Daarnaast mogen Europese burgers en organisaties deze mensen of groepen geen geld sturen of zaken met hen doen. Volgens het Openbaar Ministerie, de Nationale Politie en Buitenlandse Zaken betekent dit dat partijen die digitale infrastructuur aanbieden dat niet meer kunnen en mogen aanbieden aan deze cybercriminelen en dat er ook een onderzoeksplicht geldt voor deze bedrijven. Daarmee wordt voorkomen dat deze cybercriminelen nog misbruik kunnen maken van digitale infrastructuur binnen de EU.[107] De Verenigde Staten en het Verenigd Koninkrijk hebben vaker cybercriminelen op een sanctielijst geplaatst.[108] De Verenigde Staten sanctioneerde in 2024 bijvoorbeeld vermeende leden van de LockBit-ransomwaregroep.[109]

Nederlandse infrastructuur misbruikt door Russische actoren, diensten en politie grijpen in

De Nederlandse inlichtingendiensten en Nationale Politie hebben samen met de VS een online beïnvloedingscampagne verstoord. Samen met de Amerikaanse en Canadese autoriteiten, hebben de AIVD en MIVD de resultaten van het gezamenlijk onderzoek in de openbaarheid gebracht. De campagne was gericht op het beïnvloeden van het Amerikaanse publieke debat, er is geen indicatie dat deze ook is ingezet om het publieke debat in Nederland of Europa te beïnvloeden. De Nederlandse digitale infrastructuur werd misbruikt voor de campagne, zo stond een gebruikte server in Nederland. De AIVD en de MIVD achten het zeer waarschijnlijk dat de Russische overheid betrokken is bij de ontwikkeling van de software die werd gebruikt in deze campagne.[110]

Digitaal stemmen is een bekend voorbeeld waaruit blijkt dat vertrouwen in digitale veiligheid noodzakelijk is om digitale processen te willen gebruiken. We brengen in Nederland nog steeds onze stem uit met het rode potlood en op papier. De stemcomputers werden in 2009 afgeschaft omdat ze te hackgevoelig waren.

3 Nieuwe uitdagingen voor digitale veiligheid

Als gevolg van ontwikkelingen in het afgelopen jaar zijn meerdere nieuwe uitdagingen voor digitale veiligheid geïdentificeerd. Statelijke actoren intensiveren hun activiteiten en verbreden hun capaciteiten, waarbij zij gebruik maken van verschillende middelen uit een bredere gereedschapskist. Zowel statelijke als criminele actoren zoeken naar nieuwe wegen om aanvallen uit te voeren, om detectie zo lang mogelijk te omzeilen. Verder zijn niet-digitale factoren van invloed op digitale veiligheid. Zo vormt grootschalige concentratie bij de drie grote cloudaanbieders een risico voor digitale veiligheid. Ook zorgt schaarse cybercapaciteit ervoor dat de digitale weerbaarheid in het geding kan komen. Verder vormt de ontwikkeling van een krachtige quantumcomputer nu al een risico voor de nationale veiligheid. De mondiale online datahandel geeft op grote schaal inzage in persoonsgevoelige data en vormt een risico voor de nationale veiligheid. Daarnaast is vertrouwen in digitale processen cruciaal voor gebruikers om daarvan gebruik te willen maken. Wanneer dat vertrouwen verdwijnt, kunnen zich grote problemen voordoen.

Statelijke actoren intensiveren activiteiten en verbreden capaciteiten

Statelijke cyberaanvallen staan niet op zichzelf maar zijn onderdeel bredere gereedschapskist

Cyberaanvallen door statelijke actoren lijken wel het nieuwe normaal, werd gesteld in CSBN 2022.[111] Die cyberaanvallen staan niet op zichzelf, maar zijn onderdeel van een bredere gereedschapskist die staten hanteren om hun belangen te behartigen. Daarbij kunnen cyberaanvallen worden uitgevoerd in combinatie met andere middelen. Ook kunnen verschillende cyberaanvallen in samenhang met elkaar worden uitgevoerd.

Wanneer enkel wordt gekeken naar individuele cyberaanvallen die direct hun weerslag hebben op Nederlandse belangen, gaat dit voorbij aan de bredere dreiging die voortkomt uit het gebruik van een bredere gereedschapskist door statelijke actoren. Het kan verleidelijk zijn om verschillende (fysieke of digitale) incidenten individueel te bekijken en te constateren dat de effecten relatief gezien meevallen. Zo'n smalle focus gaat echter voorbij aan het feit dat de vele acties met elkaar samenhangen, en in combinatie met elkaar wel degelijk impact hebben. Ook een smalle focus op alleen de gevolgen van een individuele cyberaanval is te beperkt; het is juist nuttig om ook die in samenhang te bezien als het gaat om de gevolgen. Het gaat daarbij ook om samenhang tussen een cyberaanval en andere ingezette middelen.

Statelijke actoren intensiveren activiteiten en verbreden capaciteiten

Meerdere statelijke actoren intensiveren hun cybercapaciteiten. Dat geldt in ieder geval voor Rusland en China.[112] Zo was er in 2023, ten opzichte van het eerste jaar van de oorlog in Oekraïne, een toename van cyberoperaties door Russische statelijke actoren tegen Europese en NAVO-bondgenootschappelijke activiteiten. Het is waarschijnlijk dat sommige van deze cyberoperaties zijn uitgevoerd met als doel een positie binnen kritieke infrastructuur te bemachtigen, om deze op een later moment te kunnen saboteren. Daarnaast proberen hackers in te breken op systemen van de Nederlandse overheid en andere EU- en NAVO-landen, om op deze manier informatie te verkrijgen over bijvoorbeeld de steun aan Oekraïne.[113]

Voor China geldt dat het tempo van cyberoperaties op westerse doelwitten hoog ligt en dat Chinese inlichtingendiensten de activiteiten om westerse doelwitten aan te vallen steeds verder opschroeven. Hoewel Chinese statelijke hackersgroepen al geruime tijd grootschalige en persistente cyberspionagecampagnes uitvoeren tegen Nederlandse en bondgenootschappelijke belangen, was er in 2023 een toename van de intensiteit, omvang en het technische niveau van deze cybercampagnes.[114] Illustratief is verder de campagne van de digitale aanvalsgroep 'Volt Typhoon' tegen de militaire en civiele infrastructuur in de VS (zie Jaarbeeld). De Chinese cyberdreiging bestond tot nu toe vooral uit mogelijke spionage, maar opvallend aan de campagne van Volt Typhoon is dat Chinese hackers mogelijk ook voorbereidingen troffen voor sabotage, en niet (enkel) voor spioneren. Vooralsnog zijn geen activiteiten uit dit programma tegen Europa bekend. De Chinese capaciteit op dit gebied groeit echter hard en zou binnen betrekkelijk korte tijd overal ter wereld ingezet kunnen worden. Dit maakt het Chinese cybersabotageprogramma de komende jaren in potentie een dreiging voor onder andere Nederland.[115]

Noord-Korea is ook illustratief, met name vanwege de toenemende hoeveelheden geld die het land binnenhaalt met behulp van cyberaanvallen. Hoewel niet nieuw, kwamen Noord-Koreaanse cyberaanvallen die zijn gericht op het verdienen van geld voor het regime in het nieuws. De resultaten van recent VN-onderzoek onderstrepen dat het Noord-Koreaanse cyberprogramma een wereldwijde dreiging vormt, voor de cryptosector in het bijzonder. Ook Nederland heeft een levendige cryptomarkt, en Noord-Koreaanse cyberaanvallen hierop vallen niet uit te sluiten. Het totaalbedrag van 3 miljard dollar dat Noord-Korea zou hebben verdiend, is op zichzelf al fors, maar wat opvalt is dat het leeuwendeel in 2022 en 2023 buitgemaakt is (resp. 1 miljard en 600 miljoen US-dollar).[116] Deze bedragen kunnen bijdragen aan het financieren van het regime of bijvoorbeeld het nucleaire, cyber of andersoortig wapenprogramma.

Ook nieuwe cybermachten investeren in cyberprogramma's, waardoor zij hun activiteiten kunnen intensiveren. Sommige ontvangen daarbij hulp van bondgenoten.[117] Nieuwe of opkomende statelijke actoren behoren veelal tot landen die groeiende machtsaspiraties hebben of zijdelings betrokken zijn bij (regionale) conflicten. De AIVD en MIVD hebben in 2023 geen aanvallen uit zulke landen onderkend die op Nederland waren gericht.[118] Er zijn ook landen die cybermiddelen inkopen op de vrije markt. Commerciële aanbieders van geavanceerde cybermiddelen zijn in opkomst en de capaciteiten van hun spyware zijn inmiddels zeer geavanceerd.[119] Dit stelt landen zonder eigen cyberprogramma in staat om ook hun activiteiten op te starten of te intensiveren.

Deze nieuwe of opkomende statelijke actoren richten zich voor een deel op landen in de regio of op digitale spionage en monitoring van opposanten of activisten.[120] De intentie om Nederlandse belangen te raken lijkt op dit moment laag te zijn. Toekomstige ontwikkelingen zouden ertoe kunnen leiden dat Nederlandse belangen wel een doelwit worden. Daarnaast is het van belang om rekening te houden met de dreiging die vanuit nieuwe of opkomende staten uitgaat naar dissidenten/opposanten of activisten die zich in Nederland bevinden. Volgens een cybersecuritybedrijf drong een statelijke actor bijvoorbeeld door tot websites toebehorend aan een etnische minderheid die zich uitspreekt tegen het zittende regime.[121] Hierbij werd de Nederlandse digitale infrastructuur geraakt, alhoewel die niet het primaire doelwit was.

Naast intensivering van cyberactiviteiten is voor een aantal landen ook sprake van verbreding van de capaciteiten: ze voegen nieuwe methoden toe aan hun bestaande arsenaal of gebruiken andere middelen. Naast het gebruik van andere middelen uit de bredere gereedschapskist, is ook de inzet of betrokkenheid van niet-statelijke actoren onderdeel van die verbreding. In 2023 werd een groter deel van de digitale spionage-, sabotage- en beïnvloedingsactiviteiten door Rusland uitgevoerd door 'hacktivistische' collectieven. In sommige gevallen gebruiken 'traditionele' Russische cyberactoren deze hacktivistische covers. In andere gevallen gaat het daadwerkelijk om hacktivistische groeperingen die handelen in het verlengde van de Russische staat. Wat betreft China is opvallend hoezeer het Chinese offensieve cyberprogramma mede gestoeld is op samenwerking tussen bedrijfsleven, universiteiten en Chinese inlichtingendiensten. De scheidslijnen tussen organisaties zijn daarbij onduidelijk: personen vervullen soms zowel een wetenschappelijke rol als een rol in het Chinese veiligheidsapparaat en werken daarbij samen met Chinese (staats)bedrijven.[122]

Actoren zoeken nieuwe wegen om cyberaanvallen uit te voeren

Kwaadwillenden kiezen vaak weg van minste weerstand

Kwaadwillenden gaan nog altijd veelal voor aanvalsroutes die relatief eenvoudig en snel toegang bieden. Actoren maken nog altijd veel gebruik van (spear)phishing. Daarbij worden e-mails verstuurd die betrouwbaar en relevant lijken, maar deze bevatten

een besmette link of bijlage. Een voorbeeld van een grootschalige phishingcampagne was de 'DiplomaticOrbiter' campagne die in 2022 werd uitgevoerd door Russische hackers. Hierbij waren diplomaten en denktanks rond de wereld het doelwit.[123] Daarnaast kunnen actoren ook gebruikmaken van eerdere datalekken die bijvoorbeeld gebruikersnamen en wachtwoorden kunnen bevatten.[124] Ook scannen actoren proactief systemen die met het internet zijn verbonden om te zien of organisaties software in gebruik hebben waarvan bekend is dat die een kwetsbaarheid bevat (zie hoofdstuk 4). Als kwetsbaarheden niet (tijdig) gepatcht zijn, kan dit toegang bieden voor kwaadwillenden.

Living-off-the-Land en targeting edge devices kenmerkende modus operandi in 2023

Statelijke en criminele actoren zoeken ook actief naar nieuwe wegen om cyberaanvallen uit te voeren en proberen daarbij steeds geraffineerder detectie te ontwijken. Hierbij wordt onder andere gebruik gemaakt van zogeheten Living-off-the-Land (LOTL) aanvallen.[125] Omdat LOTL aanvallen gebruik maken van legitieme tooling en applicaties die het slachtoffer in gebruik heeft, worden deze door antivirusprogramma's en andere beveiligingsmaatregelen vaak niet automatisch geblokkeerd. Hierdoor wordt het lastiger om aanvallen te detecteren, wat voor zowel statelijke als criminele actoren wenselijk is. Daarnaast laten LOTL-technieken minder 'digitale vingerafdrukken' achter, wat het moeilijker maakt betrokkenheid van specifieke groepen of landen aan te tonen.[126]

Daarnaast zien verschillende overheidsorganisaties een trend dat kwaadwillenden in toenemende mate edge devices aanvallen.[127] Dat zijn systemen die zich aan de rand van een netwerk bevinden, en bestaan uit (beveiligings)producten zoals firewalls, VPN-servers, en routers. Edge devices vormen al geruime tijd een aantrekkelijk doelwit voor kwaadwillenden, mede omdat monitoring en detectie hierop zeer complex is. De MIVD beschrijft dat Chinese actoren zich in toenemende mate richten op edge devices (specifiek VPN-systemen).[128] Het NCSC stelt dat ook Russische actoren en criminele ransomwaregroepen VPN-systemen hebben misbruikt.[129]

Compromittatie van edge devices kan vergaande gevolgen hebben. Zo kan een kwaadwillende een achterdeur inbouwen om zo toegang te blijven behouden. Edge devices worden vaak als toegangspunt voor het achterliggende netwerk gebruikt. Op die manier kunnen kwaadwillenden toegang krijgen tot gevoelige of vertrouwelijke informatie. Verder verwerken edge devices vaak gevoelige gegevens, waaronder inloggegevens van gebruikers. Kwaadwillenden kunnen die inloggegevens gebruiken, waarmee zij na initiële compromittatie onder de radar proberen te blijven.

Niet-digitale ontwikkelingen beïnvloeden digitale veiligheid

Grootschalige concentratie bij grootste cloudaanbieders vormt risico

Steeds meer organisaties maken gebruik van clouddiensten en deze markt is rap gegroeid.[130] Op grote schaal nemen organisaties die diensten af van vooral drie grote cloudaanbieders: Amazon, Microsoft en Google. Zelfs als gebruik wordt gemaakt van Europese of Nederlandse aanbieders, dan nog bestaat een kans dat ook die gebruik maken van diensten van deze cloudaanbieders.[131] Naast voordelen kleven er ook risico's aan grootschalige concentratie van clouddiensten bij de grootste cloudaanbieders.

Toelichting clouddiensten

Clouddiensten zijn IT-diensten die via het internet worden aangeboden. De gebruiker schaft geen hardware en software aan, maar betaalt voor het daadwerkelijke gebruik van één of meerdere diensten die op de infrastructuur van een cloudaanbieder draaien. Clouddiensten worden vaak in drie categorieën verdeeld: Software as a Service (SaaS), Platform as a Service (PaaS) en Infrastructure as a Service (IaaS). De scheidslijnen tussen die drie zijn niet altijd even scherp te trekken. De grootste cloudaanbieders zijn actief op de drie genoemde lagen en zijn dus verticaal geïntegreerd.[132]

Er is een aantal redenen te noemen waarom organisaties gebruik maken van vooral de drie grootste cloudaanbieders. Denk daarbij aan de brede beschikbaarheid van functionaliteiten, integratiemogelijkheden van diensten en de schaalbaarheid.[133] Een andere reden is de kennis bij ICT-deskundigen over het gebruik van de diensten van juist die aanbieders. Naast deze meer inhoudelijke redenen, wordt ook gewezen op regelgeving en procedures voor inkoop.[134] Zo zouden de grootste cloudaanbieders vaak gunstigere aanbiedingen doen bij aanbestedingen ten opzichte van kleinere partijen.[135] Eenmaal gekozen voor een grote cloudaanbieder is het bovendien eenvoudiger om binnen het bestaande contract extra diensten af te nemen, dan een nieuwe inkoopprocedure te starten.[136]

Een ander argument dat wordt genoemd om gebruik te maken van de diensten van juist de grootste cloudaanbieders, is dat er weinig tot geen Europese of Nederlandse alternatieven zouden zijn. De grootste cloudaanbieders hebben een enorm aanbod aan diensten en die kunnen ook als één pakket worden afgenomen door klanten. Een alternatief is om clouddiensten van verschillende cloudaanbieders te combineren. Dit stelt wel extra eisen aan de deskundigheid en het interne beheer van de cloudgebruiker. Een expert vergelijkt in dat kader de grote cloudaanbieders met IKEA, waar je vele producten kunt kopen bij dezelfde winkel.[137]

Maar, als je bijvoorbeeld alleen op zoek bent naar een kamerplant, zijn er vele andere winkels.

Er kleven ook risico's aan grootschalige concentratie bij die grootste cloudaanbieders. Een eerste risico is dat strategische afhankelijkheden worden vergroot. Dit heeft implicaties voor onze digitale open strategische autonomie. Nederland is voor clouddiensten nu al grotendeels afhankelijk van vooral de drie bedrijven uit de VS en de dynamiek in de markt voor clouddiensten versterkt dat nog eens (zie hieronder). Een gevolg hiervan is dat wetgeving in de VS ook in meer of mindere mate van toepassing is op Nederlandse organisaties.[V] Verder kan onder gewijzigde geopolitieke omstandigheden een strategische afhankelijkheid grote gevolgen krijgen. Bovendien bestaan voor Nederland beperkingen aan het toezicht dat op die bedrijven kan worden uitgeoefend. Zo bevinden de hoofdvestigingen van deze bedrijven in de EU zich in andere landen en vindt in die landen toezicht plaats op die bedrijven. Een Nederlandse toezichthouder moet dan in contact treden met de toezichthouder in het andere land om toezicht uit te kunnen oefenen op deze partijen.[138]

Een tweede risico is dat op deze wijze een single point of failure ontstaat. Een storing of cyberaanval kan wereldwijde doorwerking krijgen. De drie grootste aanbieders vormen een heel aantrekkelijk doelwit voor cyberactoren. Dit door de concentratie van clouddiensten en onderliggende data. Een aanval op een cloud serviceprovider is in de Rijksbrede Risicoanalyse dan ook als waarschijnlijk beoordeeld en bovendien als ernstig.[139] Bij de veiligheid van in ieder geval een van die aanbieders zijn vraagtekens geplaatst door de Amerikaanse Cyber Safety Review Board. Die instantie constateerde dat bij die aanbieder een bedrijfscultuur heerst waarin stelselmatig geen prioriteit wordt toegekend aan gedegen risicomanagement en investeringen in veiligheid.[140] Er zijn bovendien al jaren de nodige voorbeelden bekend van misconfiguratie van clouddiensten door klanten met cyberincidenten als gevolg.[141] Er wordt veel van de veiligheid overgelaten aan klanten die daarvoor lang niet altijd over de benodigde kennis beschikken of van de mogelijkheden op de hoogte zijn. Beveiligingsopties moeten continu worden ingeschakeld en onderhouden, of zijn alleen beschikbaar als afzonderlijke service. De technische complexiteit van het configureren en beveiligen van clouddiensten gaat de capaciteit van veel organisaties, zelfs volwassen organisaties, te boven.[142]

Een derde risico is de machtspositie van de grote cloudaanbieders die versterkt wordt vanuit zowel de aanbod- als vraagzijde in de cloudmarkt. Aan de aanbodzijde lijken de drie grootste cloudaanbieders in te zetten op het bouwen van een eigen ecosysteem, waar organisaties na de initiële keuze lastig meer uit kunnen treden. In de cloudmarkt wordt vooral geconcurreerd om nieuwe klanten aan te trekken. Na dat eerste keuzemoment zijn er beperkingen om over te stappen naar een andere aanbieder. Die overstapbeperkingen zijn zowel technisch, organisatorisch/procedureel als financieel van aard. Door de machtspositie ontbreken bovendien potentieel de prikkels bij die bedrijven om te blijven innoveren en reële prijzen te vragen aan klanten.[143] Doordat aan de vraagzijde organisaties veelal kiezen voor de drie grootste aanbieders, wordt ook zo hun machtspositie vergroot. Hierdoor krijgen ook alternatieve aanbieders steeds minder kans om te overleven.[144]

Grootschalige effecten door digitale monocolturen

De wereldwijde computerstoring die cybersecuritybedrijf CrowdStrike in juli 2024 veroorzaakte (zie Jaarbeeld) is een wake-up call voor de mogelijke gevolgen van een digitale monocultuur. Deze computerstoring trof tenminste 8,5 miljoen computers, wat overeenkomt met 1% van het wereldwijde aantal Windows-gebruikers.[145] Incidenten zoals de CrowdStrike-storing zijn door die monoculturen onvermijdelijk geworden, stelt EFF.[146] Ook andere markten voor digitale diensten, hardware en software worden gedomineerd door slechts enkele bedrijven. Door die monoculturen ontstaan single points of failure, zoals eerder is beargumenteerd voor de drie grootste cloudaanbieders.

Weerbaarheid in geding door schaarse cybersecuritycapaciteit

Het tekort aan cybersecuritydeskundigen kan de digitale weerbaarheid van Nederland aantasten. Volgens het UWV kent geen enkele andere beroepsrichting zo'n sterke krapte als de ICT-sector, en met name de vraag naar softwareontwikkelaars en securityspecialisten is toegenomen in de afgelopen vijf jaar.[147] Bovendien is het tekort aan digitale professionals een sectoroverstijgend probleem; in alle sectoren zijn zij nodig om de digitale transitie mogelijk te maken.[148]

Daarnaast is de verwachting dat de vraag naar cybersecurity professionals ook zal toenemen als gevolg van toekomstige wet- en regelgeving. Ook door de verdere ontwikkeling en inzet van AI zullen nieuwe taken ontstaan en nieuwe competenties benodigd zijn, resulterend in een toenemende vraag naar cybersecurity professionals.[149]

Het is niet alleen de toegenomen vraag die tot schaarste heeft geleid, ook het aanbod groeit niet mee. Zo blijkt uit onderzoek dat een groot gedeelte van de vraag naar cybersecurity professionals draait om medior en senior functies. Hiervoor is veelal bij- of omscholing nodig, waarvoor het nodig is om (huidige) cybersecurity professionals aan te houden of aan te trekken. Dit blijkt niet voldoende te gebeuren.[150]

De combinatie van voortschrijdende digitalisering, toenemende vraag, en toekomstige wet- en regelgeving waaraan moet worden voldaan én waar toezicht op moet worden gehouden, maakt het

V Het gaat daarbij lang niet alleen om de zogeheten 'US cloud act' waardoor de overheid – onder juridische waarborgen - toegang kan eisen tot informatie. De overheid in de VS kan ook, bijvoorbeeld in het geval van een grootschalige uitval of aanval, prioriteit eisen voor herstel van diensten in de VS. Ook sanctiewetgeving kan doorwerking krijgen.

aannemelijk dat de tekorten de komende jaren verder toenemen. Ook voor de overheid is het, mede vanwege de competitie op de arbeidsmarkt, complex om arbeidskrachten met expertise aan te trekken en/of te behouden. Dit kan uiteindelijk zijn weerslag hebben op de digitale weerbaarheid van Nederland, zeker omdat overheidsorganisaties een cruciale rol spelen op het gebied van onder andere digitale weerbaarheid en het bestrijden van bijvoorbeeld cybercriminaliteit. Daarnaast kan het voor kwaadwillenden interessant worden om te onderzoeken welke organisaties de grootste tekorten hebben – en daarmee mogelijk de zwakste verdediging.[151]

Toekomstige krachtige quantumcomputer vormt nu al een risico voor de nationale veiligheid

De ontwikkeling van een krachtige quantumcomputer biedt kansen, maar leidt ook tot risico's voor de nationale veiligheid. Een quantumcomputer die over voldoende rekenkracht beschikt is namelijk in staat om veelgebruikte encryptiemethodes te verzwakken of te breken. Cryptografie speelt een sleutelrol als het gaat om het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van digitale processen en data. Voorbeelden hiervan zijn het aansturen van verkeerslichten en bruggen, communicatie in de vorm van e-mail of appberichten en het beschermen van identiteitsgegevens.[152] Daarnaast wordt cryptografie gebruikt om vertrouwelijke, bedrijfsgeheime en staatsgeheime informatie te versleutelen.

Cryptografie maakt een essentieel onderdeel uit van grote delen van de Nederlandse digitale ruimte. Het gebruik van cryptografie beschermt de continuïteit van de vitale infrastructuur, de economische veiligheid en de maatschappelijke veiligheid. Daarmee is cryptografie, zowel nu als in de toekomst, van wezenlijk belang voor het waarborgen van de nationale veiligheid van Nederland.

De ontwikkeling van een krachtige quantumcomputer is de laatste jaren in een stroomversnelling geraakt.[153] Hoewel het onwaarschijnlijk is dat er op dit moment quantumcomputers bestaan die de huidige cryptografie effectief kunnen breken, moet er wel nu al rekening gehouden worden met de mogelijke risico's als gevolg van de komst van een krachtige quantumcomputer. Versleutelde data die nu onderschept en opgeslagen wordt, kan dan namelijk op een later moment ontsleuteld worden.[154] Dit wordt ook wel store now, decrypt later genoemd, en vormt volgens de AIVD en het NCSC op dit moment de meest urgente dreiging voor organisaties in relatie tot de komst van een krachtige quantumcomputer. Met deze dreiging moeten organisaties rekening houden als zij over data beschikken die langere tijd vertrouwelijk moet blijven.[155]

Toekomstige weerbaarheid afhankelijk van huidige voorbereiding

De migratie naar quantumveilige cryptografie kent complexe uitdagingen die veel tijd, planning en voorbereiding zullen vragen. Organisaties die te laat starten met de voorbereidingen om te migreren naar quantumveilige cryptografie, lopen het risico dat ze niet op tijd weerbaar zijn tegen de dreiging van de quantumcomputer.

Grootschalige handel in persoonsgevoelige data vormt dreiging voor nationale veiligheid

Databedrijven handelen wereldwijd in persoonsgevoelige data

Verschillende databedrijven handelen wereldwijd in persoonsgevoelige data van burgers en medewerkers van organisaties (verder datahandel). Veel van die handel hangt samen met het verdienmodel achter vele websites en apps, namelijk geld (terug)verdienen door advertenties aan te bieden. Echter, ook gebruikers van betaalde digitale devices, software of digitale diensten wisselen persoonsgevoelige data uit met de aanbieders. Sommige aanbieders doen dit op hun beurt ook met (soms tientallen of honderden) partners en die mogelijk ook weer met partners.[156]

Databedrijven maken gebruik van geavanceerde advertentietechnologie, ook bekend onder de term real-time bidding (RTB). Onderdeel van RTB is dat sites en apps geautomatiseerd advertentieruimte aanbieden. Adverteerders kunnen op hun beurt advertenties inkopen voor heel specifieke profielen van gebruikers. Om het aanbod van en de vraag naar advertentieruimte bij elkaar te brengen, zijn diverse platforms en partijen actief. Die wisselen daartoe persoonsgevoelige data uit. Denk hierbij aan actuele locatiegegevens, biometrische, financiële en/of psychische en medische data. Sommige daarvan veredelen de verkregen data met andere data, stellen profielen van gebruikers op en verkopen deze.[157] Die data kunnen ook worden gebruikt voor het trainen van generatieve AI-modellen: daarbij is niet duidelijk wat met die data gebeurt en of die op enige wijze ergens kunnen opduiken. Bovendien kunnen statelijke actoren via dekmantelfirma's onderdeel zijn van datahandel en op deze wijze persoonsgevoelige data verzamelen en veredelen.[158]

Datahandel maakt ook gebruik van andere technieken dan de genoemde RTB. Een bekend voorbeeld is de wijze waarop Facebook data verzamelt over online activiteiten van internetgebruikers. Uit een onderzoek van een consumentenorganisatie uit de VS bleek dat van de deelnemers aan het onderzoek hun gegevens door gemiddeld 2.230 bedrijven naar Facebook werden gestuurd.[159] Een ander voorbeeld is dataverzameling door Google. Volgens de Nederlandse Stichting Massaschade & Consument zou Google via Android allerlei gegevens van gebruikers verzamelen en daarbij Nederlandse en Europese regels overtreden. Volgens de stichting wordt een enorme hoeveelheid informatie over smartphonegebruik naar Googleservers doorgesluisd, zelfs als de meest

privacyvriendelijke instellingen zijn ingeschakeld. Uit een onderzoek zou niet alleen blijken dat Google veel meer gegevens verzamelt dan is toegestaan, maar dat het deze gegevens ook aan individuele gebruikers koppelt.[160] Ook slimme apparaten en moderne auto's vergaren veel persoonsgevoelige data en delen die met fabrikanten, die dat op hun beurt ook weer kunnen delen met andere partijen. De vorige minister van Infrastructuur en Waterstaat gaf in een Kamerbrief in januari 2024 aan dat automobilisten zeggenschap moeten hebben over hun voertuigdata en dat die alleen na toestemming met derde partijen mag worden gedeeld.[VI] Ook wees hij in de brief op de risico's van spionage van fabrikanten uit landen met een offensieve cyberstrategie tegen Nederland.[161]

Grootschaligheid en precisie datahandel kunnen veiligheidsbelangen schaden

De grootschaligheid en precisie van de datahandel en de wijze waarop online advertentiemarkten functioneren kan de nationale veiligheid op verschillende manieren schaden. Een eerste is de grootschalige schending van de vertrouwelijkheid van persoonsgevoelige data. 'Ongeautoriseerde inzage in informatie (en/of publicatie daarvan)' wordt niet voor niets al jaren aangemerkt als risico voor de nationale veiligheid. Hoewel er juridisch een onderscheid geldt, is er feitelijk geen verschil tussen illegale schending van vertrouwelijkheid als gevolg van een cyberaanval of schending door de genoemde vormen van datahandel.[VII] Een tweede manier waarop de nationale veiligheid zou kunnen worden geraakt is misbruik van de opgebouwde datasets en/of gedetailleerde persoonsprofielen. Deze zijn niet alleen waardevol voor datahandelaren zelf, maar ook voor talrijke kwaadwillenden, waaronder statelijke actoren, criminelen of extremisten en activisten. De precisie van de opgebouwde profielen stelt groepen of individuen bloot aan een verhoogd risico op digitale spionage of online of fysieke intimidatie en dit kan de nationale veiligheid schaden. Het kan gaan om politici of andere mensen op gevoelige (overheids-)functies, maar ook om bedreigde personen of leden van diaspora-gemeenschappen afkomstig uit autoritaire regimes.[162] Het kabinet Rutte IV schreef in een brief aan de Tweede Kamer zich 'volledig bewust' te zijn van de risico's die de online advertentie-industrie vormt voor de privacy van burgers en de nationale veiligheid.[163] Ook een Amerikaans presidentieel decreet van februari 2024 geeft blijk van bewustzijn over de risico's van online datahandel.[164] Daarbij richt het zich primair op het beschermen van Amerikaans overheidspersoneel (op gevoelige functies) en -processen. Hiermee tracht het te voorkomen dat deze data onbedoeld in handen komt van statelijke actoren zoals Rusland, Iran en Noord-Korea.[165]

Ook criminelen vergaren, veredelen en verkopen data

Ook criminelen vergaren persoonsgevoelige data en veredelen en verkopen die aan andere criminelen. Door verschillende gegevens als woonadressen, telefoonnummers, bankrekeningen, paspoortgegevens en kentekens te combineren, worden waardevolle slachtofferprofielen opgesteld, klaar voor gebruik voor allerlei vormen van criminaliteit.[166] Criminelen kunnen met behulp van deze data en/of profielen politiemedewerkers, bedreigde personen en andere individuen op gevoelige functies blootstellen aan online en/of fysieke intimidatie.

Slachtoffer- en doelwitnotificatie complex vanwege juridische barrières

De politie komt steeds vaker almaar groter wordende datasets met slachtoffergegevens tegen in opsporingsonderzoeken. Door slachtoffers te notificeren, worden zij in staat gesteld om mitigerende acties te ondernemen, zoals het installeren van updates of patches. Daardoor zijn slachtoffers bijvoorbeeld niet langer onderdeel van een botnet waarmee aanvallen op doelwitten in Nederland worden gepleegd. Omdat met regelmaat een groot deel van de slachtoffers in een dataset zich buiten Europa bevindt, kunnen deze slachtoffers wegens juridische onmogelijkheden niet worden genotificeerd. Deze juridische onmogelijkheden komen onder andere voort uit het belang van de bescherming van privacy.

Tot nu toe is het alleen op ad-hoc basis mogelijk gebleken om effectief aan slachtoffer- en doelwitnotificatie te doen, maar het notificeren van (potentiële) slachtoffers gaat in het algemeen gepaard met praktische en juridische problemen. Grootschalige slachtoffer- en doelwitnotificatie is echter van wezenlijk belang voor het duurzaam neerhalen van criminele digitale infrastructuur (op veel grotere schaal dan tot nu toe mogelijk is gebleken) en voor het voorkomen van voortdurend slachtofferschap. Het internationaal delen van data om slachtoffers te kunnen notificeren zou direct bij kunnen dragen aan het verminderen van de digitale dreiging voor de nationale veiligheid van Nederland én andere landen.[167]

VI Het delen (of verhandelen) van data uit slimme apparaten met derden door de datahouder is, zonder dat dit onderdeel is van de overeenkomst met de gebruiker, op basis van de Data Act per september 2025 niet meer toegestaan.

VII Het valt buiten de scope van dit CSBN om een oordeel te vellen over de mate van illegaliteit of legaliteit van deze uitwisseling en handel. De aangehaalde massaclaim is een illustratie dat bepaalde praktijken mogelijk in strijd met de wet zijn. Ook experts in diverse artikelen stellen dat bepaalde praktijken niet conform de wet zijn.

Digitale veiligheid randvoorwaardelijk voor vertrouwen in digitale processen

Dat digitale veiligheid essentieel is in onze sterk gedigitaliseerde maatschappij, is vaak genoemd in de verschillende edities van het CSBN van afgelopen jaren. Daarbij lag de focus vooral op de noodzaak van digitale veiligheid om digitale processen te kunnen gebruiken. Dit om maatschappelijke ontwrichting te voorkomen en als dat zich voordoet zo snel mogelijk te herstellen. Veel minder lag de nadruk op digitale veiligheid als randvoorwaarde voor het vertrouwen in digitale processen.[VIII]

Vertrouwen noodzakelijk om digitale processen te willen gebruiken

Vertrouwen is noodzakelijk om digitale processen te willen gebruiken. Alleen met vertrouwen kunnen organisaties of individuen (verder gebruikers)[IX] omgaan met de vele onzekerheden en de complexiteit die samenhangen met het gebruik ervan. Zonder vertrouwen zouden zij overweldigd worden door de gedachte aan alles wat er mogelijk mis kan gaan.[168]

Voor vertrouwen is meer nodig dan digitale veiligheid alleen. Een webshop kan nog zo veilig zijn, maar als criminelen die shop runnen en het product waarvoor is betaald niet leveren, dan tast dat uiteraard het vertrouwen aan in de webshop. Digitale veiligheid is dus niet de enige randvoorwaarde voor vertrouwen, maar wel een noodzakelijke. Digitaal stemmen is een bekend voorbeeld waaruit blijkt dat vertrouwen in digitale veiligheid noodzakelijk is. We brengen in Nederland nog steeds onze stem uit met het rode potlood en op papier. De stemcomputers werden in 2009 afgeschaft omdat ze te hackgevoelig waren.[169]

Ondanks cyberincidenten toch volop gebruik van digitale processen

Cyberincidenten tonen aan dat garanties voor digitale veiligheid niet bestaan. Desondanks maken gebruikers volop gebruik van digitale processen. Een mogelijke reden daarvoor is dat het is gestoeld op de functionaliteiten en het gebruiksgemak van processen. Gebruikers focussen zich veel minder op schadelijke effecten. Een andere reden is dat het gebruik plaatsvindt binnen een sociale context: als iedereen die processen gebruikt, dan zal het wel goed zijn. En gebruikers hebben ook de verwachting dat wet- en regelgeving en toezicht een vangnet vormt.[170] Een reden kan ook zijn dat er inmiddels nauwelijks nog analoge alternatieven bestaan en/of dat er geen keuzevrijheid is. De drempels om geen gebruik te maken van bepaalde processen is daardoor (te) hoog.

Mogelijk wel zorgen en argwaan

Dat gebruikers volop gebruik maken van digitale processen, hoeft niet te betekenen dat ze volledig vertrouwen hebben in de veiligheid daarvan. Mogelijk bestaan er wel degelijk zorgen en argwaan over de veiligheid van specifieke processen of zelfs digitale processen in het algemeen.

Zoals hierboven beargumenteerd, kan het verdwijnen van vertrouwen ertoe leiden dat gebruikers digitale processen niet meer *willen* gebruiken. Stel dat 1 miljoen burgers niet langer digitaal aangifte zouden *willen* doen omdat ze de veiligheid van processen van de Belastingdienst niet langer vertrouwen. Wanneer burgers op zo'n grote schaal weer analoog aangifte zouden willen doen via de post, zal dat grote consequenties hebben voor de inning van belastingen.

Waar vertrouwen precies op gestoeld is en wat ervoor nodig is om dit te behouden, is lastig te duiden. Wat echter wel helder is, is dat vertrouwen in digitale veiligheid één van de bouwstenen is om digitale processen te willen (blijven) gebruiken. Het behouden en/of versterken van vertrouwen is dan ook van belang om de kansen van digitalisering te benutten.

VIII De voorkeur is gegeven aan vertrouwen in digitale processen in plaats van in de aanbieders daarvan. Allereerst gaat het hier om digitale processen in het algemeen en niet om specifieke processen van een specifieke aanbieder, tenzij expliciet anders is aangegeven. Bovendien zijn in de praktijk vele 'aanbieders' betrokken. Denk aan internetbankieren, waar vele 'aanbieders' direct of indirect een rol spelen, waaronder de eigen bank, de bank van de 'ander', providers, webhosters, cloud leveranciers, en organisaties als iDeal of Google Pay of Apple Pay.

IX Voor *vertrouwen* in digitale veiligheid kan worden gekozen voor diverse invalshoeken, waaronder die van afnemer of aanbieder. Tenzij anders aangegeven, is gekozen voor de invalshoek van gebruiker, mede omdat zowel afnemers als aanbieders gebruik maken van uiteenlopende digitale processen en aanbieders op hun beurt ook afnemer zijn van allerlei processen.

Thuiswonende ouderen gebruiken een draagbare alarmknop om zorgpersoneel te waarschuwen in geval van nood. In november 2023 werkten ruim 3.000 alarmknoppen niet als gevolg van een ransomware-aanval op de dienstverlener. Ook hadden de criminelen toegang tot gegevens.

4 Structurele uitdagingen voor digitale veiligheid

Verschillende factoren vormen al langere tijd een uitdaging voor digitale veiligheid. Statelijke en criminele actoren zijn al jaren verantwoordelijk voor het leeuwendeel van de aanvallen. Daarbij kan de nationale veiligheid worden geraakt. Daarnaast kunnen ontwikkelingen die op het eerste gezicht niets met cybersecurity te maken hebben, toch blijvend van invloed zijn op de dreiging en de weerbaarheid. Dat geldt zeker voor geopolitieke en technologische ontwikkelingen. Verder geldt dat iedere organisatie kan worden geraakt door een cyberincident. Digitale risico's vragen dan ook om een bredere manier van beheersing. De veiligheid van digitale processen is essentieel in onze gedigitaliseerde samenleving, maar het belang van die veiligheid concurreert soms met andere belangen. Wel raakt het belang van digitale veiligheid steeds verder verankerd in wet- en regelgeving.

Geopolitiek en technologische ontwikkelingen beïnvloeden dreiging

De digitale dreiging is complex en wordt beïnvloed door vele niet-digitale ontwikkelingen. Denk hierbij aan geopolitieke spanningen, die ertoe kunnen leiden dat statelijke actoren cybercapaciteiten inzetten om hun belangen te behartigen. Verder kunnen geopolitieke spanningen, conflicten en maatschappelijk controversiële onderwerpen aanleiding zijn voor hacktivisme. Dit is bijvoorbeeld zichtbaar sinds de start van de oorlog tegen Oekraïne. Ook technologische ontwikkelingen, zoals generatieve AI, kunnen van invloed zijn op digitale veiligheid (zie kader).

Generatieve AI van invloed op digitale veiligheid

Het gebruik en de mogelijkheden van generatieve AI zijn zich nog volop aan het ontwikkelen en de impact op de samenleving kent nog vele onduidelijkheden. Er zijn in ieder geval vier relevante invalshoeken. Ontwikkelingen binnen en inzet van generatieve AI valt hier tot nu toe onder:

1. De algoritmen en de data waarmee de algoritmen worden gevoed kunnen doelbewust worden gemanipuleerd. Dat kan bijvoorbeeld 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.
3. Generatieve AI kan worden gebruikt voor cyberaanvallen. Zo kunnen met behulp van AI meer op een ontvanger toegesneden phishing-mails worden gemaakt. Verder kunnen kwaadwillenden generatieve AI gebruiken om snel en automatisch interessante doelwitten te detecteren en informatie daarover te verzamelen. Ook kan laagdrempeliger malware worden ontwikkeld.
4. Generatieve AI kan worden ingezet ter verdediging tegen cyberaanvallen door bijvoorbeeld onregelmatigheden te detecteren in data.

Statelijke en criminele actoren nemen het leeuwendeel van cyberaanvallen voor hun rekening

Al langere tijd nemen statelijke en criminele actoren het leeuwendeel van cyberaanvallen voor hun rekening. Een belangrijke noot hierbij is dat er daartussen een zekere mate van vermenging kan bestaan. Statelijke actoren kunnen namelijk cybercriminelen inhuren, gedogen of onder druk zetten om cyberaanvallen op gewenste doelwitten uit te voeren. Daarnaast kunnen statelijke actoren zich voordoen als criminele organisaties. Hierdoor is de scheidslijn tussen financieel gemotiveerde cybercriminelen en statelijke actoren vaag en lastig te onderscheiden.

Naast statelijke en criminele actoren kunnen hacktivisten, insiders, script kiddies en in mindere mate terroristen, cyberaanvallen uitvoeren.

Statelijke actoren hebben offensief cyberprogramma tegen Nederland

Statelijke actoren gebruiken de digitale ruimte om hun politieke, militaire en/of economische doelen te bereiken. De digitale dreiging die uitgaat van statelijke actoren richting de Nederlandse samenleving is divers.

Nederland is doelwit van een offensief cyberprogramma van landen zoals China, Rusland, Noord-Korea en Iran. Zij voeren cyberaanvallen uit tegen een breed scala aan potentiële doelwitten. Offensieve cyberprogramma's bedreigen dan ook onze nationale veiligheid.

Cyberaanvallen zijn relatief goedkoop, schaalbaar, moeilijk te attribueren en ze kennen een hoge, vaak langdurige opbrengst. Een geslaagde inbreuk kan soms jarenlang onzichtbaar, heimelijk en ongestraft informatie blijven opleveren. Dit kan informatie zijn ten behoeve van spionage, maar het kan ook om informatie van bijvoorbeeld systemen en netwerken gaan. Die informatie kan vervolgens worden gebruikt om (voorbereidingshandelingen voor) sabotage uit te voeren.

In de rapportageperiode kwamen verschillende cyberoperaties van statelijke actoren tegen Nederland aan het licht (zie Jaarbeeld). Hoofdstuk 3 beschrijft inkleuring van en nieuwe inzichten in de statelijke dreiging.

Cybercriminelen kunnen nationale veiligheid raken

Cybercriminelen zijn onverminderd in staat om omvangrijke schade toe te brengen aan digitale processen. Zij handelen vanuit financieel motief en hebben niet de intentie om de maatschappij te ontwrichten. Desondanks kunnen hun aanvallen zoveel impact veroorzaken dat ze nationale veiligheidsbelangen raken. De capaciteit van sommige cybercriminele groepen is van gelijkwaardig hoog niveau als die van statelijke actoren.

De inzet van ransomware vormt een risico voor de nationale veiligheid als het gaat om de continuïteit van vitale processen, het weglekken en/of publiceren van vertrouwelijke of gevoelige informatie en de aantasting van de integriteit van de digitale ruimte. De nationale veiligheid is in het geding wanneer het doelwit van zo'n aanval onderdeel is van de vitale infrastructuur (waaronder de Rijksoverheid en alle vastgestelde vitale processen) en de aanval de continuïteit van vitale processen verstoort. Daarnaast bevinden vitale organisaties zich in een ecosysteem met niet-vitale organisaties. Een aanval op een niet-vitale organisatie kan een opstap zijn naar of doorwerken in vitale organisaties.

In het verleden gaven sommige criminele groepen aan zich niet op vitale infrastructuur te richten. Dat zou niet verstandig zijn omdat zij zich zo in de kijker zouden spelen van inlichtingen- en opsporingsinstanties. Aan de andere kant zou in vitale sectoren de neiging kunnen bestaan om sneller losgeld te betalen vanwege het belang van de bedrijfscontinuïteit. Daardoor zou dit toch een aantrekkelijk doelwit kunnen zijn voor criminelen. Door NCTV geraadpleegde experts geven aan dat criminelen opportunistisch

zijn. Enerzijds betekent dat, dat het doelbewust aanvallen van vitale infrastructuur niet structureel gebeurt. Anderzijds betekent het ook dat criminelen geen ethische standaard hanteren wat betreft het niet aanvallen van de vitale infrastructuur.

Voor cybercriminelen blijft afpersing een aantrekkelijk verdienmodel. Criminelen doen dit onder andere door bestanden of systemen te versleutelen en losgeld te vragen in ruil voor ontsleuteling. Daarnaast kunnen criminelen (ook) dreigen met publicatie van buitgemaakte informatie (zie Jaarbeeld). Soms wordt buitgemaakte informatie verrijkt met andere data en verkocht – zelfs wanneer slachtoffers de criminelen hebben betaald om publicatie te voorkomen.

Cybercriminelen zijn onderdeel van een breder malafide en bonafide digitaal ecosysteem en zijn daarvan afhankelijk. Dit ecosysteem vormt een gelegenheidsstructuur voor hen. Door specialisatie onder cybercriminelen zijn zij afhankelijk 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. Zogeheten resellerconstructies versterken de hostingproblematiek. Hierbij verhuren resellers hostingpakketten door. Dit kan leiden tot onduidelijkheid over de identiteit van degene die verantwoordelijk is als het gaat om het hosten van – in het bijzonder illegale – data en degene die aan een vordering van justitie kan of moet voldoen.

De afhankelijkheid van legale diensten 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. Hierdoor kunnen die principes niet wettelijk worden afgedwongen en ontstaat ruimte voor het niet naleven ervan. Dit biedt cybercriminelen vele kansen om anoniem én schaalbaar te werk te gaan. Kansen die zij niet onbenut laten.

De risico's voor criminelen om gepakt of veroordeeld te worden, zijn relatief laag. Daarbij speelt geopolitiek ook een rol. Wanneer verhoudingen met andere landen (verder) verslechteren, zorgt dit ervoor dat opsporing en vervolging nog complexer is. Zo kunnen criminelen zich in bepaalde landen vrij bewegen of worden ze niet uitgeleverd. Ook wordt opsporing bemoeilijkt door juridische knelpunten om data te kunnen delen tussen de diverse relevante partijen. Desalniettemin laten verschillende gecoördineerde acties van handhavings- en opsporingsinstanties zien dat het wel degelijk mogelijk is om criminele groepen en hun aanvallen te verstoren (zie Jaarbeeld).

Iedere organisatie kan doelwit zijn van kwaadwillenden

Alle digitale processen zijn potentieel kwetsbaar

Alle digitale processen, organisaties en sectoren zijn potentieel kwetsbaar voor cyberaanvallen en zij kunnen hier op verschillende manieren mee te maken krijgen. Ten eerste kan een organisatie een bewust gekozen en direct doelwit zijn van kwaadwillenden. Bijvoorbeeld omdat een organisatie veel persoonsgegevens verwerkt. Ten tweede kan een organisatie binnen het ecosysteem worden aangevallen als opstap naar andere, interessante(re) doelwitten. Ten derde kunnen organisaties 'per toeval' slachtoffer worden. Zo zoeken kwaadwillenden actief naar systemen die kwetsbaarheden bevatten die uitgebuit kunnen worden. Als een organisatie zo'n systeem in gebruik heeft, kan deze worden aangevallen zonder dat kwaadwillenden zich bezighouden met de vraag om wat voor organisatie het gaat.

Of het nu gaat om landen, sectoren of organisaties, weinige kunnen onafhankelijk functioneren van een breder ecosysteem. Binnen het ecosysteem zijn digitale processen, systemen en netwerken in sterke mate verweven met elkaar. 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. 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 op uitval. Legacy systemen zijn bijvoorbeeld vaak in gebruik binnen OT.

Binnen het ecosysteem zijn er knooppunten waar veel informatie of digitale processen geconcentreerd zijn. Dat kan vanuit bedrijfsoverwegingen verklaarbaar en gerechtvaardigd zijn. Deze keuzes gaan echter gepaard met veiligheidsrisico's. Geconcentreerde informatie of processen zijn namelijk aantrekkelijke doelwitten voor kwaadwillenden. Statelijke actoren verzamelen op grote schaal persoonsgegevens, waarbij het verzamelen primair gericht lijkt te zijn op het monitoren en identificeren van relevante personen en bevolkingsgroepen. Ook voor cybercriminelen zijn persoonsgegevens zeer aantrekkelijk. Deze kunnen zij bijvoorbeeld gebruiken voor (spear)phishing aanvallen of om informatie te verrijken en verhandelen. Databases of sectoren die grote hoeveelheden persoonsgegevens verwerken zijn dus bij uitstek aantrekkelijk. Denk daarbij aan cloud-dienstverleners (zie Hoofdstuk 3), of de reis- en luchtvaartsector waarbinnen grote hoeveelheden persoonsgegevens worden verwerkt. Ook de zorgsector en telecomsector zijn interessante doelwitten voor kwaadwillenden vanwege de informatie die daar wordt verwerkt.

Aanvallers zoeken naar zwakste schakel binnen toeleverancierssketens

Toeleverancierssketens binnen het ecosysteem zijn een aantrekkelijk doelwit. Aanvallers zoeken binnen ketens naar organisaties die minder weerbaar zijn. Vervolgens kunnen zij via die organisatie de rest van de keten, of een specifieke organisatie binnen de keten, raken. Een keten is maar zo sterk als de zwakste schakel. Een aanval op de leveranciersketen veroorzaakt niet alleen problemen bij het gecompromitteerde bedrijf, maar ook bij andere organisaties in de keten. Ook in de afgelopen rapportageperiode is dit voorgekomen. Zo werd software van 3CX geïnfecteerd met malware, waarna waarschijnlijk de netwerken van duizenden bedrijven gecompromitteerd zijn (zie Jaarbeeld).

Operationele Technologie van groot belang, én in vizier kwaadwillenden

Operationele Technologie (OT) speelt een centrale rol in het aansturen, monitoren en beheren van fysieke processen binnen (vitale) organisaties. Voorbeelden hiervan zijn toegangssystemen of gebouwautomatiseringssystemen. OT fungeert als motor van vitale processen. Vanwege de belangrijke rol van OT, kunnen grootschalige uitval van en cyberaanvallen tegen OT-systemen grote maatschappelijke gevolgen hebben. Dat kan behalve reputatie- of financiële schade, ook leiden tot schade aan industriele apparatuur en de nabije omgeving. In het uiterste geval is het mogelijk dat er slachtoffers vallen. De digitale veiligheid van OT is dan ook van vitaal belang.

OT raakt steeds meer vervlochten met informatietechnologie (IT). Dat kent vele voordelen, maar het betekent ook dat het aanvalsoppervlak vergroot en daarmee het risico dat OT-systemen gecompromitteerd raken. Gebleken is dat cyberactoren interesse hebben in het compromitteren van OT. Zo zijn er malware-soorten die gebruikt kunnen worden voor de sabotage van OT-systemen. Ook komen aanvallen op industriële omgevingen steeds meer in beeld als verdienmodel van (criminele) actoren. Sinds eind 2023 heeft Microsoft een toename waargenomen in het aantal meldingen van aanvallen gericht op aan internet blootgestelde, slecht beveiligde OT-apparaten (zie Jaarbeeld). Verdere en mogelijk meer gerichte verstoring van OT-systemen kan in deze context niet worden uitgesloten.

Nederland aantrekkelijk doelwit voor aanvallers

Nederland is met haar hoogwaardige kenniseconomie en als voorloper op het gebied van bepaalde technologieën, een aantrekkelijk doelwit voor kwaadwillenden. Zij kunnen kennis daarover (proberen te) ontvreemden. Daarnaast huisvest ons land verschillende internationale organisaties die informatie verwerken die interessant kan zijn voor kwaadwillenden. Zo werd in oktober 2023 het internationaal Strafhof (ICC) in Den Haag slachtoffer van een cyberaanval (zie Jaarbeeld).

Vanwege de internetinfrastructuur in Nederland kan het ook aantrekkelijk zijn voor kwaadwillenden om vanuit Nederland cyberaanvallen te plegen tegen burgers, organisaties of overheden in andere landen. De infrastructuur is namelijk snel, goedkoop en betrouwbaar, wat het aantrekkelijk maakt voor misbruik.

Veiligheid van digitale processen is en blijft essentieel in sterk gedigitaliseerde samenleving

De veiligheid van digitale processen is en blijft essentieel in onze sterk gedigitaliseerde samenleving, en is daarmee onlosmakelijk verbonden met de nationale veiligheid. Er zijn amper nog processen zonder digitale component.

Wanneer digitale processen niet naar behoren werken, heeft dat effect op het functioneren van organisaties. Keteneffecten kunnen sectoren of zelfs de gehele maatschappij raken, zoals werd geïllustreerd door de foutieve software-update van CrowdStrike en de softwarefout op een netwerk van Defensie. Ook kunnen cyberincidenten fysieke consequenties hebben. Zo kan stroomuitval plaatsvinden, onderwijs stil komen te liggen, of patiëntenzorg worden belemmerd.

Digitale risico's vragen om brede manier van beheersing

Digitale risico's hebben verschillende bijzondere kenmerken. Zo hebben digitale risico's betrekking op een uiterst complex systeem, namelijk de digitale ruimte. Er bestaat geen algeheel overzicht van wat de impact zou kunnen zijn van een grootschalige en meerdaagse verstoring van digitale processen in Nederland. Hierdoor is het ook complex om mogelijke risico's in kaart te brengen. Dat komt onder andere door het bredere digitale ecosysteem waarin organisaties zich bevinden. Informatie over cyberincidenten is weliswaar deels beschikbaar, maar is zeker niet volledig en niet altijd toegankelijk voor relevante partijen. 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.

Deze bijzondere kenmerken van digitale risico's vragen om een brede manier van beheersing. Een manier is bijvoorbeeld om niet alleen te kijken naar incidenten die zich al hebben voorgedaan, en niet enkel te voldoen aan eisen waaraan wettelijk moet worden voldaan. Verder geldt nog altijd dat basismaatregelen helpen en dat daarmee een deel van de cyberincidenten kan worden voorkomen. Als laatste is het nuttig om bij het inrichten en beheren van een

netwerk als uitgangspunt te gebruiken dat er al een kwaadwillende in je netwerk zit *(assume breach)*.

Vijf basisprincipes voor digitale weerbaarheid bieden handvatten

Veel digitale incidenten vinden hun oorzaak in het niet op orde hebben van basisbeveiligingsmaatregelen. Denk daarbij aan zwakke wachtwoorden of het niet installeren van patches. Dat is jammer, want vaak is met relatief eenvoudige stappen de organisatie een stuk digitaal weerbaarder te maken. Tegelijkertijd zijn organisaties verschillend, waardoor er geen *one-size-fits-all* set van maatregelen te geven is. Een ZZP'er heeft een andere informatiebehoefte dan een organisatie die binnen de vitale sector valt. Met de vijf basisprincipes voor digitale weerbaarheid geven het NCSC en DTC handvatten voor het op orde krijgen van de basis, zie hiervoor bijlage 3 van dit CSBN.

Belang van digitale veiligheid concurreert met andere belangen

Digitale veiligheid is niet het enige belang dat beschermd moet worden en het concurreert dan ook met andere belangen. Zulke belangentegenstellingen kunnen binnen één organisatie spelen, maar het kan ook zo zijn dat de belangen van organisaties concurreren met belangen op landelijk niveau. Een voorbeeld daarvan is de grootschalige concentratie van clouddiensten bij de drie grootste mondiale cloudproviders. Beslissingen die invloed hebben op digitale veiligheid worden niet alleen gemaakt vanuit veiligheidsoverwegingen; ook bijvoorbeeld politieke, economische of juridische afwegingen worden gemaakt.

Wetgeving consolideert, implementatie onderweg

Een belangrijke ontwikkeling die de digitale weerbaarheid de komende jaren kan vergroten, betreft de extra eisen voor digitale veiligheid. Deze vloeien voort uit nieuwe Europese wet- en regelgeving, de Nederlandse Cybersecuritystrategie 2022-2028 en het daarvan afgeleide actieplan. Door deze ontwikkeling raakt het belang van digitale veiligheid (verder) verankerd in wet- en regelgeving. Deze bevindt zich in verschillende stadia van implementatie. In het onderstaande kader zijn enkele wetten beschreven, inclusief het stadium waarin deze zich bevinden. Hiervoor is een selectie gemaakt, waarbij de focus ligt op wetgeving die sectoroverstijgend is. Wet- en regelgeving met een focus op specifieke sectoren is hier dus niet in opgenomen.

Nieuwe wetgeving digitale veiligheid in verschillende stadia[171]

- **Digital Services Act (DSA):** regelt de verantwoordelijkheid en aansprakelijkheid van internetaanbieders, hostingbedrijven, online platformen, zoekmachines en marktplaatsen. De diensten moeten naar aanleiding van de DSA de rechten van gebruikers beter beschermen, online misleiding en illegale informatie aanpakken en transparantie verbeteren. Vanaf augustus 2023 geldt de wetgeving al voor de 19 grootste platforms. Vanaf februari 2024 geldt deze ook voor overige digitale diensten. EU-lidstaten zijn verantwoordelijk voor toezicht op overige digitale diensten. In Nederland zijn de toezichthouders nog niet wettelijk vastgesteld, waardoor zij slechts beperkt handelingen uit kunnen voeren onder de DSA.[172]
- **Digital Markets Act (DMA):** zorgt voor extra markt- en fusietoezicht op én concurrentieregels voor de wereldwijd grootste online platforms. Sinds maart 2024 moeten deze platforms voldoen aan de DMA. Autoriteit Consument & Markt is de nationale toezichthouder op de DMA. Zij kunnen in Nederland mogelijke overtredingen verzamelen en samen met de Europese Commissie onderzoek doen.[173]
- **Cyber Resilience Act (CRA):** beoogt een veiligere Europese digitale interne markt en een samenleving waarin onveilige producten van de markt kunnen worden geweerd en gehaald. Digitale producten – zowel software, hardware als componenten – moeten naar verwachting vanaf 2027 voldoen aan uitgebreide eisen en standaarden op het gebied van cyberveiligheid.[174]
- **Richtlijn Network and Information Security (NIS2)**: regelt welke entiteiten aan welke verplichte security-eisen moeten voldoen. Als gevolg van de NIS2-richtlijn krijgen veel meer organisaties in Nederland te maken met wettelijke verplichtingen, toezicht en ondersteuning voor hun digitale weerbaarheid. Dit geldt zowel voor overheden, vitale organisaties en andere organisaties die actief zijn in sectoren van maatschappelijk en/of economisch belang.[175] Een uitgangspunt in de NIS2 is dat het bestuurders van deze organisaties nadrukkelijk verantwoordelijk stelt voor cyberbeleid. Als dit beleid niet op orde is, kunnen er sancties volgen. De beoogde implementatie in oktober 2024 is uitgesteld in Nederland en wordt voorzien in 2025. De Cyberbeveiligingswet (Cbw) is het wetsvoorstel om de NIS2 naar nationale wetgeving om te zetten.
- **De verordening tot vaststelling van maatregelen voor een hoog gemeenschappelijk niveau van cyberbeveiliging in de instellingen, organen en instanties van de Unie** (EUIBA's) is in 2023 aangenomen en op 7 januari 2024 in werking getreden. Deze verordening hangt samen met de NIS2. Waar de NIS2 een richtlijn is die naar nationale wetgeving dient te worden omgezet door lidstaten, heeft de verordening doel om het niveau van cyberbeveiliging bij EU-instellingen, organen en agentschappen te waarborgen.[176]
- **Cyber Solidarity Act (CSOA)**: heeft als doel de capaciteiten in de EU te versterken om significante en grootschalige cyberbeveiligingsdreigingen en -aanvallen te detecteren, zich erop voor te bereiden en erop te reageren. De beoogde inwerkingtreding is eind 2024.[177]

Implementatie kost tijd

De implementatie van verschillende wet- en regelgeving is onderweg. Voor sommige wetgeving, zoals de DMA, geldt dat deze al wel is geïmplementeerd en dat toezicht hierop ook is geregeld. Voor andere wetgeving, zoals de DSA en Cbw/NIS2, is dit nog niet het geval.

De uitwerking van en bewustwording over wetgeving kost de nodige doorlooptijd. Het heeft tijd nodig voordat wetgeving daadwerkelijk leidt tot verandering in de digitale weerbaarheid, en invloed heeft op digitale risico's. Dat heeft niet alleen te maken met het vormgeven van wetgeving, maar hangt ook samen met bewustwording en voorbereiding bij bedrijven, uitvoeringsorganisaties, en toezichthouders.

Strategische thema's nog steeds van toepassing, wel enkele extra uitdagingen voor risicobeheersing

Het CSBN 2022 introduceerde zes strategische thema's (zie kader hieronder) die een bouwsteen vormden voor de Nederlandse Cybersecuritystrategie 2022-2028. Deze strategische thema's zijn nog steeds van toepassing en compliceren ieder op zich én in samenhang risicobeheersing.

Strategische thema's genoemd in het CSBN 2022 en geadresseerd in de Nederlandse Cybersecuritystrategie 2022-2028

- 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.

Veel van de bevindingen in dit CSBN vallen onder één of meer van de genoemde thema's en geven daar inkleuring aan. Dat geldt in het bijzonder voor:

1. De constatering dat staten hun activiteiten intensiveren en hun capaciteiten verbreden, en dat statelijke cyberaanvallen niet op zichzelf staan maar onderdeel zijn van een bredere gereedschapskist;
2. De nieuwe wegen die actoren zoeken als start voor cyberaanvallen;
3. Grootschalige concentratie bij drie grootste cloudaanbieders;
4. De mondiale online datahandel;
5. De noodzaak van vertrouwen van gebruikers in digitale processen om gebruik te willen (blijven) maken van digitale processen.

De digitalisering van het spoor maakt openbaar vervoer efficiënter en veiliger, maar ook kwetsbaarder voor cyberaanvallen of uitval.

Bijlagen

1 Verantwoording

Verantwoording wijze van totstandkoming

Het Cybersecuritybeeld Nederland is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Bij de totstandkoming is samengewerkt met het Nationaal Cyber Security Centrum (NCSC). Het CSBN 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 van maart 2023 tot en met juni 2024 in Nederland of in vergelijkbare landen plaatsgevonden en tot welke nieuwe inzichten leiden die?
2. Welke bredere politieke, economische, sociale en technologische ontwikkelingen en factoren hebben naar verwachting de komende jaren invloed op digitale veiligheid? Welke ontwikkelingen kunnen gamechangers zijn?
3. Welke veranderingen zijn te identificeren in digitale dreigingen die de nationale veiligheid aantasten? Denk hierbij aan de aard en omvang van de dreiging, doelwitten, actoren, kwetsbaarheden, vormen van uitval, en werkwijzen actoren.
4. 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?
5. Welke veranderingen zijn te identificeren in de mate waarin Nederland weerbaar is tegen die digitale dreigingen?In hoeverre treden veranderingen op in de grootste risico's voor de nationale veiligheid van Nederland?
6. Welke gebeurtenissen, ontwikkelingen of inzichten zijn van invloed op de strategische thema's zoals geïdentificeerd in CSBN 2022 en welke invloed gaat daarvan uit?

Analisten van de NCTV hebben aan de hand van deze vragen een eerste inventarisatie van 'ingrediënten' voor het CSBN gemaakt. Deze zijn in een drietal sessies besproken met experts van publieke organisaties. Er zijn twee interviews gehouden met hoogleraren over met name het onderwerp vertrouwen.

2 Schrijven en collegiaal toetsen
Na afronding van de analysefase zijn concepthoofdstukken geschreven door afzonderlijke auteurs. Het Jaarbeeld is tussentijds getoetst bij collega's van de NCTV, het NCSC en de AIVD en de MIVD.

3 Valideren
Het CSBN kent een uitgebreid validatietraject, waarbij de concepttekst ter commentaar wordt voorgelegd aan externe partners. 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 primair interne evaluatie plaats. De verzamelde feedback wordt vervolgens verwerkt in het CSBN-traject van het volgende jaar.

2 Methodologische toelichting cijfers ransomware-aanvallen

Genereren totaalbeeld ransomware-aanvallen complex

Ransomware-aanvallen zijn wereldwijd en in Nederland een aanhoudend en hardnekkig fenomeen, dat grote financiële schade aanricht vanwege de noodzakelijke herstelwerkzaamheden en het stilliggen van de bedrijfsvoering. Deze aanvallen tasten veelal ook de vertrouwelijkheid aan van persoons- en/of bedrijfsgevoelige informatie. Dat leidt ook tot schade. Ondanks de impact van en de vele rapporten over deze aanvallen, ontbreekt een totaalbeeld van het aantal ransomware-aanvallen.

Het genereren van zo'n totaalbeeld is verre van eenvoudig, zoals bleek uit een in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum (WODC) uitgevoerd onderzoek. De onderzoekers stellen dat de bestaande databronnen geen eenduidig beeld geven van ransomware-aanvallen op Nederlandse bedrijven en instellingen voor de onderzochte jaren 2020, 2021 en 2022. Veel databronnen zijn te generiek, waardoor het bijvoorbeeld niet mogelijk is om er specifiek informatie voor Nederland uit te halen, of ze beslaan niet de volledige periode. Daarnaast spelen er bij een aantal partijen ook commerciële belangen mee, of is de informatie die partijen publiekelijk beschikbaar maken zeer beperkt. Verder concluderen de onderzoekers dat geen enkele bestudeerde databron vrij is van beperkingen.

- Een eerste beperking is de beschikbaarheid van (relevante) data.
- Een tweede beperking, die voor de meeste databronnen geldt, is dat deze niet specifiek zijn toegespitst op Nederlandse bedrijven en instellingen. De focus van veel databronnen ligt op Noord-Amerika of is wereldwijd. De enige databronnen die specifiek focussen op Nederland zijn de politieaangiftes, de datalekmeldingen bij de Autoriteit Persoonsgegevens en de uitkomsten van de CBS Cybersecuritymonitor.
- Een derde beperking is dat geen enkele databron volledig is.
- Tenslotte is de kwaliteit van de data in sommige gevallen niet toereikend voor het in kaart brengen van ransomware-aanvallen op Nederlandse bedrijven en instellingen.[178]

Genereren totaalbeeld cyberincidenten nog complexer

De geschetste redenen waarom het complex is een totaalbeeld van ransomware-aanvallen te verkrijgen, gelden evenzeer voor een totaalbeeld van cyberincidenten. Het is zelfs nog vele malen complexer om daar een totaalbeeld van te krijgen. Een reden daarvoor is de definitiekwestie. Is het bijvoorbeeld al lastig om een definitie te kiezen voor ransomware-aanvallen, dat geldt in versterkte mate voor cyberincidenten. Is de ontvangst van een phishing e-mail een cyberincident, of moet dat hebben geleid tot bijvoorbeeld plaatsing van malware op het apparaat van de ontvanger? Valt marktplaatsfraude waarbij gebruik is gemaakt van uit een hack afkomstige identiteitsgegevens onder een cyberincident? Is verzending van een gevoelige e-mail, bijvoorbeeld van een psychiatrische instelling, met alle geadresseerden in het aan-veld (in plaats van het BCC-veld) een cyberincident? Een andere reden, die ook geldt voor ransomware-aanvallen, is dat Nederland in de digitale ruimte niet eenduidig is af te bakenen. Denk aan Nederlandse vestigingen in het buitenland, buitenlandse vestigingen in Nederland al dan niet met een hoofdvestiging in een ander Europees land, Nederlandse bedrijven die gegevens verwerken vanuit de hele wereld, buitenlandse bedrijven die gebruik maken van de Nederlandse infrastructuur, bedrijven in andere landen die gegevens verwerken van Nederlandse burgers of organisaties, et cetera.

Toelichting cijfers Jaarbeeld samenwerkingsproject Melissa

Het Jaarbeeld compileert informatie over ransomware-incidenten bij grotere organisaties (vanaf ca. 100 fte). Het is gebaseerd op incidentinformatie van Computest, DataExpert, Deloitte, Fox-IT, NFIR, Northwave, Tesorion, Kennedy Van der Laan, het NCSC en de aangifte cijfers van de Politie. Wat betreft de bedrijven gaat het om bedrijven die aan incidentrespons doen bij ransomware-aanvallen. Incidenten zijn beoordeeld door security-experts die een scherpe afbakening van de definitie ransomware hanteren. Hierdoor kan

dit jaarbeeld afwijken van andere jaarbeelden waarbij uitvraag is gedaan bij burgers en/of kleinere organisaties. Vanwege het anonimiseren van de data is perfect ontdubbelen niet mogelijk. Daarom wordt er gesproken over een schatting van unieke incidenten.[179] Opgemerkt moet worden dat uitgegaan wordt van de initiële ransomware-aanval. Zo telt een aanval op een serviceprovider met tientallen klanten die tevens slachtoffer worden van dezelfde aanval, als één aanval.[180]

Het Jaarbeeld beschrijft dat van de 147 ransomware-aanvallen er 81 alleen bij de politie bekend waren en 40 alleen bij de getroffen bedrijven. 26 aanvallen waren zowel bekend bij de getroffen bedrijven als bij de politie. Hieruit blijkt dat 40 aanvallen niet zijn gemeld bij de politie. Hoewel dat niet verplicht is, is dat wel wenselijk.[181]

Toelichting cijfers Autoriteit Persoonsgegevens (AP)

De cijfers zijn gebaseerd op een analyse van gemelde datalekken bij de AP in 2023.[182] De AP hanteert als definitie voor ransomware: *"... een vorm van malware (kwaadaardige software) die een computer of bestanden gijzelt. Meestal wordt daarna betaling geëist."* Uitsluitend exfiltratie, zonder versleuteling of zonder eis tot betaling van losgeld, valt onder (andere vormen van) malware. Vergelijkbaar met de systematiek van het project Melissa zijn de cijfers van de AP enkel gebaseerd op de eerste aanval, dus als één ransomware-aanval leidt tot tien meldingen bij de AP, wordt dit als één gerekend in de cijfers. De meldingen zelf zijn afkomstig van de verwerkingsverantwoordelijken. Dit kan het bedrijf zijn waar de aanval heeft plaatsgevonden en/of een ander bedrijf als hun verwerker (denk aan een ICT-leverancier) door ransomware is geraakt waarbij data van het bedrijf ook is getroffen. Een ransomware-aanval waarbij persoonsgegevens zijn getroffen, moet worden gemeld tenzij er geen risico is voor personen. Dat kan betekenen dat ook als geen data is ge-exfiltreerd er nog steeds een meldplicht is. Voor versleuteling hebben de hackers immers toegang gehad tot persoonsgegevens.

Het werkelijke aantal kan hoger zijn dan 178 doordat:

- Er ondanks de wettelijke verplichting geen melding is gedaan;
- Er geen toegang is verkregen tot persoonsgegevens: dat lijkt niet heel waarschijnlijk doordat vrijwel altijd wel sprake is van opslag van persoonsgegevens;
- De ransomware aanval vroegtijdig is voorkomen;
- Het gaat om een buitenlandse vestiging van een organisatie met een hoofdvestiging in een ander land. De datalekmelding wordt dan bij een buitenlandse toezichthouder gedaan.

Verschil cijfers project Melissa en die van de AP

Feit is dat het aantal gemelde ransomware-aanvallen bij de AP groter is dan wat er door Melissa is gerapporteerd. Een verklaring daarvoor kan de ondergrens zijn die Melissa hanteert voor de omvang van het bedrijf, namelijk 100 Fte. Die ondergrens geldt niet voor meldingen bij de AP. Een andere verklaring is dat organisaties die geen aangifte doen bij de politie en geen hulp inroepen van de cybersecuritybedrijven die samenwerken in het project Melissa, buiten de cijfers van Melissa blijven. Zij, of hun klanten, moeten daarentegen wel een melding doen bij de AP.

In beginsel mag worden aangenomen dat vrijwel voor alle aanvallen een wettelijke verplichting bestaat om deze te melden bij de AP. Het is immers zeer aannemelijk dat de aanvallers inzage hebben gehad in persoonsgevoelige data. In welke mate ransomware-aanvallen waarover Melissa rapporteert zijn gemeld aan de AP, is niet beken

3 Basisprincipes voor digitale weerbaarheid

Veel digitale incidenten hebben als oorzaak dat organisaties de basisbeveiligingsmaatregelen niet op orde hebben. Denk aan zwakke wachtwoorden of het niet installeren van patches. Dat is jammer, want vaak is met relatief eenvoudige stappen de organisatie een stuk digitaal weerbaarder te maken. Tegelijkertijd zijn organisaties verschillend, waardoor er geen generieke set van maatregelen te geven is. Een ZZP'er heeft een andere informatiebehoefte dan een organisatie die binnen de vitale sector valt. Met de vijf basisprincipes van digitale weerbaarheid geven het NCSC en DTC handvatten voor het op orde krijgen van de basis.

Vijf basisprincipes voor digitale weerbaarheid

1. **Breng risico's in kaart**
   De eerste stap is het in kaart brengen wat er moet worden beschermd. Door afhankelijkheden (inclusief leveranciers), belangen, dreigingen en de huidige weerbaarheid in kaart te brengen, krijgen organisaties zicht op hun risico's en hun te beschermen belangen. Daarmee krijg je zicht op welke beveiligingsmaatregelen nodig zijn om die belangen te beschermen.
2. **Bevorder veilig gedrag**
   Veel cyberincidenten ontstaan als gevolg van interacties tussen mens en techniek. Medewerkers kunnen onbedoeld (maar soms ook bedoeld) grote schade toebrengen aan een organisatie. De mens is in die zin de '*first line of defence*'. Veilig gedrag kan worden bevorderd door mensen bewust te maken van risico's en te trainen hoe deze te adresseren, maar vooral ook door te werken aan een cultuur waar men veilig een melding kan doen als het dan toch misgaat. Ook zijn er verschillende technische hulpmiddelen die kunnen helpen bij het maken van veilige keuzes. Denk bijvoorbeeld aan het gebruik van wachtwoordmanagers.
3. **Bescherm systemen, applicaties en apparaten**
   Systemen, applicaties en apparaten houden organisaties draaiende. Kwetsbaarheden in soft- en hardware kunnen er echter voor zorgen dat deze beschadigen of niet goed functioneren. Daardoor kunnen belangrijke of kritische processen van je organisatie verstoord raken. Het is daarom van belang deze te beschermen door te kiezen voor veilige instellingen (hardening, segmentatie) en dreigingen tijdig te detecteren (detectie en monitoring). Daarmee wordt het aanvalsoppervlak verkleind en kunnen incidenten tijdig worden geadresseerd.
4. **Beheer toegang**
   Als de toegang tot data en systemen niet consequent beheerd wordt, kan dat leiden tot datalekken of ongeautoriseerde toegang. Daarom is het nodig per gebruiker te definiëren welke systemen en data toegankelijk moeten zijn voor het werk dat gedaan dient te worden. Een vuistregel is om niet meer rechten toe te kennen dan nodig voor de werkzaamheden (least privilege). Toegangsrechten moeten worden aangepast als iemand een nieuwe functie krijgt of de organisatie verlaat.
5. **Bereid voor op incidenten**
   Niet alle incidenten kunnen worden voorkomen. Sterker nog: om weerbaar te zijn, is het goed bij het inrichten en beheren van een netwerk als uitgangspunt te gebruiken dat er al een kwaadwillende in je netwerk zit (assume breach). Het is van belang te weten hoe je op cyberincidenten reageert en, als het dan toch misgaat, hoe je daarvan kunt herstellen.

Meer lezen over de basisprincipes en welke maatregelen jij kunt nemen voor het verbeteren van jouw digitale weerbaarheid? Kijk voor meer informatie op: https://www.ncsc.nl/wat-kun-je-zelf-doen/basisprincipes en www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

4 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 Gebruik gemaakt van omschrijving in 'DDoS', NCSC, https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ddos (geraadpleegd op 2024-08-14).

3 Gebruik gemaakt van omschrijving in 'Factsheet Help! Mijn website is beklad', NCSC, 2015-03-04, https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2019/juni/01/factsheet-help-mijn-website-is-beklad/20150304_FS-Help-Mijn-website-is-beklad-archief.pdf.

4 'Hacktivists Stoke Pandemonium Amid Russia's War in Ukraine', WIRED, 03-05-2022, https://www.wired.com/story/hacktivists-pandemonium-russia-war-ukraine/.

5 'Multiple Ukrainian Government Websites Hacked and Defaced', BleepingComputer, 14-01-2022, https://www.bleepingcomputer.com/news/security/multiple-ukrainian-government-websites-hacked-and-defaced/.

6 Gebruik gemaakt van omschrijving in 'Dreigingsbeeld Statelijke Actoren 2021', AIVD, MIVD & NCTV, 03-02-2021, https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren.

7 'Gebruik gemaakt van omschrijving in Cybersecuritybeeld Nederland 2020', NCTV, 2020-06-29, https://www.nctv.nl/documenten/publicaties/2018/06/13/cybersecuritybeeld-nederland-2018.

8 Cijfers Autoriteit Persoonsgegevens verkregen uit bilaterale contacten.

9 Cijfers Autoriteit Persoonsgegevens verkregen uit bilaterale contacten.

10 'Jaarbeeld Ransomware 2023', NCSC, 22-2-2024, https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/22/jaarbeeld-ransomware-2023/Jaarbeeld_Ransomeware_2023_jan_dec.pdf, 20 juni 2024; [gespreksverslag NCTV/AAN – AP, d.d. maart 2024, ongepubliceerd].

11 'Trends on Zero-Days Exploited In-the-Wild in 2023', Google, 27-03-2024, https://cloud.google.com/blog/topics/threat-intelligence/2023-zero-day-trends.

12 'Cybersecurity Dreigingsbeeld voor de zorg 2023', Z-Cert, 27-02-2024, https://z-cert.nl/cybersecurity-dreigingsbeeld-voor-de-zorg-2023/.

13 'Exposed and vulnerable: Recent attacks highlight critical need to protect internet-exposed OT devices', Microsoft, 30-05-2024, https://www.microsoft.com/en-us/security/blog/2024/05/30/exposed-and-vulnerable-recent-attacks-highlight-critical-need-to-protect-internet-exposed-ot-devices/.

14 'het Samenhangend Inspectiebeeld cybersecurity vitale processen', Rijksoverheid.nl, 17-06-2024, https://www.rijksoverheid.nl/documenten/kamerstukken/2024/06/17/tk-samenhangend-inspectiebeeld-cybersecurity-vitale-processen.

15 'Paspoorten van dokters op straat na hack bij oudereninstelling Gelderland', RTL Nieuws, 07-03-2023, https://www.rtlnieuws.nl/nieuws/nederland/artikel/5370082/attent-zorg-behandeling-hack-ransomware-paspoorten-datalek.

16 'Datalek bij waternet: gegevens bezoekers Waterleidingduinen in handen van hackers', AT5, 15-03-2023, https://www.at5.nl/artikelen/219522/datalek-bij-waternet-gegevens-bezoekers-waterleidingduinen-in-handen-van-hackers.

17 'Gevaar op zee na hack bij maritieme dienstverlener', Digital Trust Center, https://www.digitaltrustcenter.nl/gevaar-op-zee-na-hack-bij-maritieme-dienstverlener.

18 'Maritiem dienstverlener Royal Dirkzwager getroffen door ransomware', Security.nl, 20-03-2023, https://www.security.nl/posting/789992/Maritiem+dienstverlener+Royal+Dirkzwager+getroffen+door+ransomware.

19 'Rapportage Datalekken 2023', Autoriteit Persoonsgegevens, april 2024,https://www.autoriteitpersoonsgegevens.nl/uploads/2024-04/Rapportage%20datalekken%202023.pdf.

20 'Uitspraken. ECLI:NL:RBROT:2023:2931', https://uitspraken.rechtspraak.nl/, 06-04-2023, https://uitspraken.rechtspraak.nl/details?id=ECLI:NL:RBROT:2023:2931.

21 'Ransomwaregroep publiceert gegevens cliënten Brabantse zorginstelling', 20-04-2023, Security.nl,https://www.security.nl/posting/793808/Ransomwaregroep+publiceert+gestolen+cli%C3%ABntgegevens+Brabantse+zorginstelling.

22 'Zuid-Hollandse provider kon door ransomware geen internet leveren aan klanten', Tweakers, 24-04-2023,https://tweakers.net/nieuws/209058/zuid-hollandse-provider-kon-door-ransomware-geen-internet-leveren-aan-klanten.html.

23 'Website Rechtspraak.nl door ddos-aanval slecht of niet bereikbaar', Security.nl, 05-05-2023,https://www.security.nl/posting/795318/Website+Rechtspraak_nl+door+ddos-aanval+slecht+of+niet+bereikbaar.

24 'Website Staten-Generaal plat door 'overbelasting', Agconnect.nl, 04-05-2023, https://www.agconnect.nl/business/security/website-staten-generaal-plat-door-overbelasting.

25 'Klantenportaal HVC Energie is tijdelijk ontoegankelijk na cyberaanval', Tweakers, 26-05-2023, https://tweakers.net/nieuws/210142/klantenportaal-hvc-energie-is-tijdelijk-ontoegankelijk-na-cyberaanval.html.

26 'HVC wijst IT-leverancier na hackaanval de deur. Afvalverwerkings- en energiebedrijf heeft klantsysteem na cyberincident op eigen servers ondergebracht', Noordhollands Dagblad, 26-06-2024, https://www.noordhollandsdagblad.nl/regio/alkmaar/hvc-wijst-it-leverancier-na-hackaanval-de-deur.-afvalverwerkings-en-energiebedrijf-heeft-klantsysteem-na-cyberincident-op-eigen-servers-ondergebracht/14465686.html.

27 'Progress Software facing dozens of class action lawsuits, SEC investigation following MOVEit incident', The Record, 12-10-2023, https://therecord.media/progress-facing-lawsuits-sec-action.

28 'Landal GreenParks waarschuwt 12.000 gasten voor mogelijk datalek', Security.nl, 08-07-2023, https://www.security.nl/posting/798904/Landal+GreenParks+waarschuwt+12_000+gasten+voor+mogelijk+datalek 'Clop begins naming alleged MOVEit victims', Computerweekly, 15-07-2023, https://www.computerweekly.com/news/366541817/Clop-begins-naming-alleged-MOVEit-victims.

29 'Unpacking the MOVEit Breach: Statistics and Analysis', Emsisoft, 13-12-2023, https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/.

30 'Pro-Russische groep legt websites Nederlandse havens plat', RTL Nieuws, 14-06-2023, https://www.rtlnieuws.nl/economie/artikel/5390268/pro-russische-cybercriminelen-ddos-aanval-havenbedrijf-rotterdam-amsterdam.

31 'IT-storing legde treinverkeer in en rond Amsterdam plat – update', Tweakers, 05-06-2023, https://tweakers.net/nieuws/210430/it-storing-legde-treinverkeer-in-en-rond-amsterdam-plat.html.

32 'Apeldoorn lekt gegevens inwoners na software-update van burgerportaal', Security.nl, 02-07-2023, https://www.security.nl/posting/801788/Apeldoorn+lekt+gegevens+inwoners+na+software-update+van+burgerportaal.

33 'Nederlandse organisaties doelwit van DDoS-aanvallen', NCSC, 08-08-2023, https://www.ncsc.nl/actueel/nieuws/2023/augustus/8/nederlandse-organisaties-doelwit-van-ddos-aanvallen.

34 'Site luchthaven Groningen plat, pro-Russische hackersgroep claimt ddos-aanval', Algemeen Dagblad, 27-08-2023, https://www.ad.nl/groningen/site-luchthaven-groningen-plat-pro-russische-hackers-groep-claimt-ddos-aanval~af075e19/

35 'Russische hackers weer actief', Rotterdams Dagblad, 22-08-2023.

36 'Cyberattack on British telecom Lyca prevented customers from making calls, topping up', The Record, 04-10-2023, https://therecord.media/cyberattack-on-lyca-stops-calls.

37 'International Criminal Court systems breached for cyber espionage', BleepingComputer, 21-10-2023, https://www.bleepingcomputer.com/news/security/international-criminal-court-systems-breached-for-cyber-espionage/.

38 'Computersystemen van Internationaal Strafhof aangevallen', NOS, 19-09-2023, https://nos.nl/artikel/2491054-computersystemen-van-internationaal-strafhof-aangevallen.

39 'Het CIDI is al wekenlang mikpunt van aanhoudende cyberaanvallen ', EW Magazine, 20-11-2023, https://www.ewmagazine.nl/nederland/achtergrond/2023/11/het-cidi-is-al-wekenlang-mikpunt-van-aanhoudende-cyberaanvallen-1377466/.

40 'Landelijke storing alarmknoppensysteem voor ouderen door cyberaanval', NOS, 13-11-2023, https://nos.nl/artikel/2497671-landelijke-storing-alarmknoppensysteem-voor-ouderen-door-cyberaanval.

41 'Akira Ransomware Strikes Again: Compass Group Italia and Aqualectra Utility Hit by Data Breach', The Cyber Express, 08-12-2023, https://thecyberexpress.com/akira-ransomware-attack.

42 'Aqualectra herstelt na cyberaanval', Curacao.nu, 07-12-2023, https://curacao.nu/aqualectra-herstelt-na-cyberaanval/

43 'Turkish espionage campaigns in the Netherlands', Hunt and Hackett, 05-01-2024, https://www.huntandhackett.com/blog/turkish-espionage-campaigns.

44 'Cutting Edge, Part 4: Ivanti Connect Secure VPN Post-Exploitation Lateral Movement Case Studies', Mandiant, 04-04-2024, https://cloud.google.com/blog/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement.

45 'MIVD onthult werkwijze Chinese spionage in Nederland', Defensie, 06-02-2024, https://www.defensie.nl/actueel/nieuws/2024/02/06/mivd-onthult-werkwijze-chinese-spionage-in-nederland.

46 'Nijmeegse chipmaker gehackt, criminelen dreigen kroonjuwelen te lekken ', RTL, 12-04-2024, https://www.rtl.nl/tech/artikel/5444863/nexperia-gehackt-ransomware-cybercriminelen-dark-web?redirect=rtlnieuws.

47 'Russische propaganda te zien op kinderzender in Nederland na verstoring door hackers', NOS, 06-04-2024, https://nos.nl/artikel/2515707-russische-propaganda-te-zien-op-kinderzender-in-nederland-na-verstoring-door-hackers.

48 'BabyTV wéér overgenomen: kinderen zien gewelddadige Russische propaganda', Nu.nl, 17-04-2024, https://www.nu.nl/tech/6309428/babytv-weer-overgenomen-kinderen-zien-gewelddadige-russische-propaganda.html.

49 'Geheime afmeldcodes van duizenden alarmsystemen opvraagbaar door softwarefout', BNR, 11-04-2024, https://www.bnr.nl/nieuws/tech-innovatie/10544662/geheime-afmeldcodes-van-duizenden-alarmsystemen-opvraagbaar-door-softwarefout.

50 'NCSC meldt actief misbruik van kritiek Palo Alto firewall-lek in Nederland', Security.nl, 19-04-2024,https://www.security.nl/posting/838602/NCSC+meldt+actief+misbruik+van+kritiek+Palo+Alto+firewall-lek+in+Nederland.

51 'AddComm geraakt door ransomware', AddComm, 22-05-2024, https://www.addcomm.nl/addcomm-geraakt-door-ransomware/.

52 'AddComm maakt afspraak met criminelen om gestolen klantdata te verwijderen', Security.nl, 28-05-2024, https://www.security.nl/posting/843180/AddComm+maakt+afspraak+met+criminelen+om+gestolen+klantdata+te+verwijderen.

53 'APT Activity Report' ESET, 14-05-2024, https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2023-q1-2024.pdf.

54 'Grootste landelijke pinstoring in jaren kost supermarkten miljoenen', FD, 18-05-2024, https://fd.nl/bedrijfsleven/1517007/grootste-landelijke-pinstoring-in-jaren-kost-supermarkten-miljoenen.

55 'Hackers leggen websites politieke partijen plat op dag van Europese verkiezingen', Nu.nl, 06-06-2024, https://www.nu.nl/tech/6315777/hackers-leggen-websites-politieke-partijen-plat-op-dag-van-europese-verkiezingen.html.

56 'Meerdere kwetsbaarheden in Cisco Webex', NCSC, 07-06-2024, https://www.ncsc.nl/actueel/nieuws/2024/juni/07/meerdere-kwetsbaarheden-in-cisco-webex.

57 'SNS Bank, ASN Bank en RegioBank hebben opnieuw last van een storing', Tweakers, 24-06-2024, https://tweakers.net/nieuws/223570/sns-bank-asn-bank-en-regiobank-hebben-opnieuw-last-van-een-storing.html.

58 'ING erkent technische storing na problemen met overboekingen', Tweakers, 19-06-2024, https://tweakers.net/nieuws/223410/ing-erkent-technische-storing-na-problemen-met-overboekingen.html.

59 'Gegevens 60.000 terugbetalers op straat na fout bij DUO', BNR, 24-06-2024, https://www.bnr.nl/nieuws/nieuws-politiek/10550815/gegevens-60-000-terugbetalers-op-straat-na-fout-bij-duo.

60 'Storing in online dienstverlening', RDW, 13-06-2024, https://www.rdw.nl/particulier/nieuws/2024/storing-in-online-dienstverlening.

61 'Urenlange storing bij Odido opgelost', NOS, 30-06-2024, https://nos.nl/artikel/2526752-urenlange-storing-bij-odido-opgelost.

62 'Helping our customers through the CrowdStrike outage', Microsoft, 20-07-2024, https://blogs.microsoft.com/blog/2024/07/20/helping-our-customers-through-the-crowdstrike-outage/.

63 'CrowdStrike: logicafout zorgde voor blue screen of death bij computers', Security.nl, 20-07-2024, https://www.security.nl/posting/850698/CrowdStrike%3A+logicafout+zorgde+voor+blue+screen+of+death+bij+computers.

64 'Hoe een softwarefoutje luchthavens, media en ziekenhuizen kon platleggen', NOS, 19-07-2024, https://nos.nl/artikel/2529551-hoe-een-softwarefoutje-luchthavens-media-en-ziekenhuizen-kon-platleggen.

65 'Systemen bij overheidsdiensten plat door storing bij ministerie van Defensie', NOS, 28-08-2024, https://nos.nl/artikel/2534851-systemen-bij-overheidsdiensten-plat-door-storing-bij-ministerie-van-defensie.

66 'Kamerbrief over IT storing bij Defensie en andere overheidsdiensten', Rijksoverheid, 28-08-2024, https://www.rijksoverheid.nl/documenten/kamerstukken/2024/08/29/kamerbrief-it-storing-bij-defensie-en-andere-overheidsdiensten-tk.

67 'Spoedafdeling Brusselse ziekenhuis Sint-Pieter heropend na cyberaanval', VRT, 11-03-2023, https://www.vrt.be/vrtnws/nl/2023/03/11/spoedafdeling-brussels-ziekenhuis-sint-pieter-heropend-na-cybera/.

68 'Explosie aan datalekken door zerodaylek in Fortra GoAnywhere', Security.nl, 29-03-2023, https://www.security.nl/posting/791073/Explosie+aan+datalekken+door+zerodaylek+in+Fortra+GoAnywhere.

69 'Securitybedrijven slaan alarm over malware in desktopapplicatie 3CX', Security.nl, 30-03-2023, https://www.security.nl/posting/791292/Securitybedrijven+slaan+alarm+over+malware+in+desktopapplicatie+3CX+-+update.

70 'Symantec: aanval achter 3CX-hack raakte ook cruciale, Europese infrastructuur', Tweakers, 23-04-2023, https://tweakers.net/nieuws/209026/symantec-aanval-achter-3cx-hack-raakte-ook-cruciale-europese-infrastructuur.html.

71 '3CX: Supply Chain Attack Affects Thousands of Users Worldwide', Symantec, 30-03-2023, https://symantec-enterprise-blogs.security.com/threat-intelligence/3cx-supply-chain-attack.

72 'Hackers leggen websites van overheid plat in meer dan helft van Duitse deelstaten', VRT, 05-04-2023, https://www.vrt.be/vrtnws/nl/2023/04/05/hackers-leggen-websites-van-overheid-plat-in-meer-dan-helft-van/#:~:text=In%20meer%20dan%20de%20helft,verschillende%20delen%20van%20het%20land.

73 'Gemeente Herselt slachtoffer van cyberaanval: gemeentehuis, bibliotheek en OCMW al dagenlang dicht', VRT, 06-04-2023,https://www.vrt.be/vrtnws/nl/2023/04/06/cyberaanval/.

74 'Pro-Russische hackers vallen Europese luchtverkeersleiding aan', FD.nl, 20-04-2023, https://fd.nl/politiek/1474188/pro-russische-hackers-vallen-europese-luchtverkeersleiding-aan.

75 'Volt Typhoon targets US critical infrastructure with living-off-the-land techniques', Microsoft, 24-05-2023, https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.

76 'PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure', CISA, 07-02-2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

77 'US confronts China over Volt Typhoon cyber espionage', Reuters, 08-05-2024, https://www.reuters.com/world/us/us-confronts-china-over-volt-typhoon-cyber-espionage-2024-05-08/.

78 'Noorse overheid erkent gehackt te zijn via zeroday in Ivanti', Tweakers, 26-07-2023, https://tweakers.net/nieuws/212098/noorse-overheid-erkent-gehackt-te-zijn-via-zeroday-in-ivanti.html.

79 'Poland investigates cyber-attack on rail network', BBC, 26-08-2023, https://www.bbc.com/news/world-europe-66630260.

80 'NATO says it is addressing an apparent cyberattack after strategy documents posted online', CNN, 03-10-2023, https://edition.cnn.com/2023/10/03/politics/nato-cyber-attack-strategy/index.html.

81 'Hackers steal user database from European telecommunications standards body', The Record, 02-10-2023, https://therecord.media/etsi-telecommunications-standards-body-hack-database-stolen.

82 'Die Energieversorgung Dänemarks war im Visier von Hackerangriffen. Eine Spur führt nach Russland', Neue Zürcher Zeitung (Internationale Ausgabe), 14-11-2023, https://www.nzz.ch/technologie/mehrere-hackerangriffen-nahmen-die-energieversorgung-daenemarks-ins-visier-eine-spur-fuehrt-nach-russland-ld.1765449.

83 'DP World hack: port operator gradually restarting operations around Australia after cyber-attack', The Guardian, 13-11-2023, https://www.theguardian.com/australia-news/2023/nov/13/australian-port-operator-hit-by-cyber-attack-says-cargo-may-be-stranded-for-days.

84 'DP World confirms data stolen in cyberattack, no ransomware used', Bleeping Computer, 28-11-2023, https://www.bleepingcomputer.com/news/security/dp-world-confirms-data-stolen-in-cyberattack-no-ransomware-used/.

85 'Two-day water outage in remote Irish region caused by pro-Iran hackers', The Record, 11-12-2023, https://therecord.media/water-outage-in-ireland-county-mayo.

86 'Municipal Water Authority of Aliquippa hacked by Iranian-backed cyber group ', CBS News, 26-11-2023, https://www.cbsnews.com/pittsburgh/news/municipal-water-authority-of-aliquippa-hacked-iranian-backed-cyber-group/.

87 'Federal investigators confirm multiple US water utilities hit by hackers', CNN, 01-12-2023, https://edition.cnn.com/2023/12/01/politics/us-water-utilities-hack/index.html.

88 'IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities', CISA, 01-12-2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

89 'Albanian parliament, telecom company hit by cyberattacks', The Record, 27-12-2023, https://therecord.media/albanian-parliament-telecom-company-hit-by-cyberattacks.

90 'Hospitals offline across Romania following ransomware attack on IT platform', The Record, 13-02-2024, https://therecord.media/romanian-hospitals-offline-after-ransomware-attack.

91 'Prescriptions nationwide impacted by cyber incident at Change Healthcare ', The Record, 22-02-2024, https://therecord.media/prescriptions-nationwide-impacted-by-change-healthcare-incident.

92 'Change Healthcare incident drags on as report pins it on ransomware group', The Record, 27-02-2024, https://therecord.media/change-healthcare-blackcat-alphv-incident-drags-on.

93 'Change Healthcare brings some systems back online after cyberattack', The Record, 08-03-2024, https://therecord.media/change-healthcare-brings-some-systems-online.

94 'UnitedHealth says Change hackers stole health data on 'substantial proportion of people in America'', 23-04-2024, https://techcrunch.com/2024/04/22/unitedhealth-change-healthcare-hackers-substantial-proportion-americans/.

95 'The XZ Backdoor: Everything You Need to Know', WIRED, 02-04-2024, https://www.wired.com/story/xz-backdoor-everything-you-need-to-know/.

96 'NHS London statement on Synnovis ransomware cyber attack – Tuesday 4 June 2024 ', NHS England, 04-06-2024, https://www.england.nhs.uk/london/2024/06/04/nhs-london-statement-on-synnovis-ransomware-cyber-attack/.

97 'Hospitals cyber attack impacts 800 operations', BBC, 14-06-2024, https://www.bbc.com/news/articles/cd11v377eywo.

98 'TeamViewer: Hackers copied employee directory and encrypted passwords', The Record, 01-07-2024, https://therecord.media/teamviewer-cyberattack-employee-directory-encrypted-passwords.

99 'Identiteitsverificatiebedrijf TikTok, Uber en X lekte kopieën van id-documenten', Security.nl, 27-06-2024.

100 'Cybercrimebeeld Nederland', Openbaar Ministerie en Politie, 28-06-2024, https://fts.politie.nl/cybercrimebeeld/.

101 'Servers neergehaald van 's werelds grootste ransomware groepering', Politie, 20-02-2024, https://www.politie.nl/nieuws/2024/februari/20/09-servers-neergehaald-van-s-werelds-grootste-ransomware-groepering.html.

102 'Meerdere botnets ontmanteld in grootste internationale operatie tegen ransomware ooit, Politie, 30-05-2024, https://www.politie.nl/nieuws/2024/mei/30/11-meerdere-botnets-ontmanteld-in-grootste-internationale-operatie-tegen-ransomware-ooit.html.

103 'Europol coordinates global action against criminal abuse of Cobalt Strike', Europol, 03-07-2024, https://www.europol.europa.eu/media-press/newsroom/news/europol-coordinates-global-action-against-criminal-abuse-of-cobalt-strike.

104 'Ragnar Locker ransomware developer arrested in France', Bleepingcomputer, 20-10-2023, https://www.bleepingcomputer.com/news/security/ragnar-locker-ransomware-developer-arrested-in-france/

105 'Ransomware group LockBit is disrupted by a global police operation that includes 2 arrests', AP, 20-02-2024, https://apnews.com/article/lockbit-ransomware-website-police-disrupt-0297653ddfc245fcdf7d-9308c6c1e6fe.

106 'Police arrest Conti and LockBit ransomware crypter specialist' Bleepingcomputer, 12-06-2024, https://www.bleepingcomputer.com/news/security/police-arrest-conti-and-lockbit-ransomware-crypter-specialist/.

107 'Russian hackers sanctioned by European Council for attacks on EU and Ukraine', The Record, 24-06-2024, https://therecord.media/six-russian-hackers-sanctioned-european-council-eu-ukraine; 'EU-sancties tegen zes Russische hackers', NOS.nl, 24-06-2024, https://nos.nl/artikel/2525962-eu-sancties-tegen-zes-russische-hackers.

108 'VS en VK zetten nog eens elf verdachten achter Trickbot-malware op sanctielijst', Security.nl, 07-09-2023, https://www.security.nl/posting/809408/VS+en+VK+zetten+nog+eens+elf+verdachten+achter+Trickbot-malware+op+sanctielijst.

109 'VS legt sancties op aan vermeende leden LockBit-ransomwaregroep', Security.nl, 20-02-2024, https://www.security.nl/posting/830419/VS+legt+sancties+op+aan+vermeende+leden+LockBit-ransomwaregroep.

110 'Nederland en VS verstoren Russische digitale beïnvloedingsoperatie', AIVD, 09-07-2024, https://www.aivd.nl/actueel/nieuws/2024/07/09/nederland-en-vs-verstoren-russische-digitale-beinvloedingsoperatie.

111 ' Cybersecuritybeeld Nederland. CSBN 2022', NCTV, juli 2022.

112 'AIVD Jaarverslag 2023', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf; 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministerie van Defensie, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf; Microsoft Digital Defense Report 2023, Microsoft, oktober 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023; 'M-Trends 2024 Special Report', Google, 13-5-2024, https://services.google.com/fh/files/misc/m-trends-2024.pdf.

113 AIVD Jaarverslag 2023', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

114 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministerie van Defensie, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf.

115 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministerie van Defensie, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf.

116 'Exclusive: UN experts investigate 58 cyberattacks worth $3 bln by North Korea', Reuters, 8-2-2024, https://www.reuters.com/technology/cybersecurity/un-experts-investigate-58-cyberattacks-worth-3-bln-by-north-korea-2024-02-08/; 'Final report of the Panel of Experts submitted pursuant to resolution 2680 (2023)', United Nations Security Council, 7 maart 2024, https://undocs.org/en/S/2024/215; 'Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises', Chainanalysis, 24-1-2024, https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/.

117 'Microsoft Digital Defense Report 2023', Microsoft, oktober 2023, https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023; 'Microsoft shifts to a new threat actor naming taxonomy', Microsoft, 18-4-2023, https://www.microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/; 'AIVD Jaarverslag 2023', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

118 'AIVD Jaarverslag 2023', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf

119 'The most notorious instances of commercial spyware', Kaspersky, 21-3-2024, https://www.kaspersky.com/blog/commercial-spyware/50813/.

120 Marczak, Scott-Railton, McKune, Abdul Razzak, Deibert, 'Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries', 18-9-2018, https://tspace.library.utoronto.ca/bitstream/1807/95391/1/Report%23113--hide%20and%20seek.pdf.

121 'Turkish espionage campaigns in the Netherlands', Hunt and Hackett, 5-1-2024, https://www.huntandhackett.com/blog/turkish-espionage-campaigns.

122 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministerie van Defensie, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf.

123 'AIVD Jaarverslag 2023', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

124 'Cybercrimebeeld Nederland 2024', Openbaar Ministerie & Politie, 11-6-2024, https://www.om.nl/onderwerpen/cybercrime/cybercrimebeeld-cybercrimebeeld-ccbn.

125 'AIVD Jaarverslag 2023', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

126 'AIVD Jaarverslag 2023', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 23-4-2024, https://www.aivd.nl/binaries/aivd_nl/documenten/jaarverslagen/2024/04/22/jaarverslag-2023/AIVD+Jaarverslag+2023.pdf.

127 'Factsheet omgaan met edge devices', NCSC, 10-6-2024, https://www.ncsc.nl/documenten/factsheets/2024/juni/10/kennisproduct-omgaan-met-edge-devices.

128 'Openbaar jaarverslag 2023 Militaire Inlichtingen- en Veiligheidsdienst', Ministerie van Defensie, 18-04-2024, https://www.defensie.nl/binaries/defensie/documenten/jaarverslagen/2024/04/18/jaarverslag-mivd-2023/MIVD_Openbaar+jaarverslag+2023+_18april.pdf .

129 'Factsheet omgaan met edge devices', NCSC, 10-6-2024, https://www.ncsc.nl/documenten/factsheets/2024/juni/10/kennisproduct-omgaan-met-edge-devices.

130 'Marktstudie Clouddiensten', Autoriteit Consument & Markt, 2022-09-20, https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf.

131 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem.

132 'Marktstudie Clouddiensten', Autoriteit Consument & Markt, 2022-09-20, https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf.

133 Onder andere gebaseerd op: 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem; 'Baas in eigen cloud – het kan, maar Europa doet het niet', de Correspondent, 7-5-2024, https://decorrespondent.nl/15295/baas-in-eigen-cloud-het-kan-maar-europa-doet-het-niet/a6fda854-11c2-0676-355c-129f8a76bf4d.

134 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem; feedback op concepttekst van een groot overheidsonderdeel.

135 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem.

136 Feedback op concepttekst van een groot overheidsonderdeel.

137 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem; 'Baas in eigen cloud – het kan, maar Europa doet het niet', de Correspondent, 7-5-2024,https://decorrespondent.nl/15295/baas-in-eigen-cloud-het-kan-maar-europa-doet-het-niet/a6fda854-11c2-0676-355c-129f8a76bf4d.

138 Genoemd door partner tijdens expertmeeting in het kader van CSBN voorbereidingen.

139 'Rijksbrede Risicoanalyse Nationale Veiligheid', Analistennetwerk Nationale Veiligheid, 31-07-2022, https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2022/07/31/rijksbrede-risicoanalyse-nationale-veiligheid-2022/Rijksbrede+Risicoanalyse+Nationale+Veiligheid+2022.pdf.

140 'Review of the Summer 2023 Microsoft Exchange Online Intrusion', Cyber Safety Review Board, 20-03-2024, https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf.

141 'NSA Releases Top Ten Cloud Security Mitigation Strategies',NSA, 7-03-2024,https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies/.

142 'Majority of CIOs concerned that cloud complexity exceeds human ability', ITpro.com, 15-9-2022, https://www.itpro.com/cloud/cloud-management/369086/majority-cios-concerned-cloud-complexity-exceeds-human-ability; 'Rush to cloud computing is outpacing organizations' ability to adapt', ZDnet, 5-3-2022, https://www.zdnet.com/article/rush-to-cloud-computing-is-outpacing-organizations-ability-to-adapt/

143 'Marktstudie Clouddiensten', Autoriteit Consument & Markt, 2022-09-20, https://www.acm.nl/system/files/documents/marktstudie-clouddiensten.pdf.

144 'Europa is (bijna) volledig afhankelijk van de VS en China en dat is een probleem', De Technoloog, 30-1-2024, https://www.bnr.nl/podcast/de-technoloog/10538713/europa-is-bijna-volledig-afhankelijk-van-de-vs-en-china-en-dat-is-een-probleem.

145 'Helping our customers through the CrowdStrike outage', Microsoft, 2027-07-20, Helping our customers through the CrowdStrike outage - The Official Microsoft Blog.

146 'CrowdStrike, Antitrust, and the Digital Monoculture',Electronic Frontier Foundation, 2024-08-01,https://www.eff.org/deeplinks/2024/07/crowdstrike-antitrust-and-digital-monoculture.

147 'ICT in beeld', UWV, 10-8-2023, https://www.werk.nl/arbeidsmarktinformatie/sector/ict/personeelstekort-in-ict-blijft-ondanks-toename-aantal-ict-ers.

148 'Lijst van vragen en antwoorden over de Jaarverslagen van de ministeries van Justitie en Veiligheid 2023 (Kamerstuk 36560-VI-1), Binnenlandse Zaken en Koninkrijksrelaties 2023 (Kamerstuk 36560-VII-1 en Economische Zaken en Klimaat 2023 (Kamerstuk 36560-XIII)', Tweede Kamer, 4-6-2024, https://www.tweedekamer.nl/kamerstukken/detail?id=2024Z09679&did=2024D22834.

149 'Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity', Platform Talent voor Technologie en Dialogic, april 2024, https://www.cybersecurityraad.nl/documenten/brieven/2024/07/04/csr-signaal-brief-cybersecurity-arbeidsmarkt.

150 'Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity', Platform Talent voor Technologie en Dialogic, april 2024, https://www.cybersecurityraad.nl/documenten/brieven/2024/07/04/csr-signaal-brief-cybersecurity-arbeidsmarkt.

151 'Foresight 2030 Threats', ENISA, maart 2024, https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024.

152 'Antwoorden op aanvullende kennisvragen inzake Kwantumtechnologie en de gevolgen voor encryptie', Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 7-11-2023, https://open.overheid.nl/documenten/7cc21d78-75bb-4778-9615-cccb2b79b613/file.

153 'Maak je organisatie quantumveilig', NCSC & AIVD, 18-09-2023, https://www.ncsc.nl/documenten/publicaties/2023/september/18/maak-je-organisatie-quantumveilig.

154 'Bereid je voor op de dreiging van quantumcomputers', AIVD, 23-09-2021, https://www.aivd.nl/documenten/publicaties/2021/09/23/bereid-je-voor-op-de-dreiging-van-quantumcomputers.

155 'The PQC Migration Handbook', TNO, 4-4-2023, https://www.tno.nl/en/newsroom/2023/04-0/pqc-migration-handbook/

V 'Quantumveilige cryptografie', Digitale Overheid, 7-11-2023 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/quantumveilige-cryptografie/.

156 Voor een onderbouwing: zie de verdere alinea's.

157 'Europe's hidden security crisis', Irish Council for Civil Liberties and the Open Markets Institute, 2023, https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf; 'Hoe datahandelaren adressen van jou én van bedreigde personen te koop aanbieden', RTL, 5-1-2024,https://www.rtl.nl/boulevard/crime/artikel/5425259/geheime-adressen-bedreigde-journalisten-politici-en-advocaten-te; 'Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico'', BNR, 10-01-2024,https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico.

158 'Europe's hidden security crisis', Irish Council for Civil Liberties and the Open Markets Institute, 2023, https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf; 'Biden order will limit how much data can be sold to Russia and China', The Record, 28-02-2024,https://therecord.media/biden-executive-order-data-sales-adversaries-russia-china.

159 'Each Facebook User Is Monitored by Thousands of Companies', Consumer Reports, 17-01-2024, https://www.consumerreports.org/electronics/privacy/each-facebook-user-is-monitored-by-thousands-of-companies-a5824207467/.

160 'Stichting start massaclaim tegen Google wegens dataverzamelen Android', Security.nl, 8-04-2024,https://www.security.nl/posting/837020/Stichting+start+massaclaim+tegen+Google+wegens+dataverzamelen+Android.

161 'Minister: automobilist moet zeggenschap over voertuigdata hebben', Security.nl, 18-01-2024,https://www.security.nl/posting/825979/Minister%3A+automobilist+moet+zeggenschap+over+voertuigdata+hebben.

162 'Europe's hidden security crisis', Irish Council for Civil Liberties and the Open Markets Institute, 2023,https://www.iccl.ie/wp-content/uploads/2023/11/Europes-hidden-security-crisis.pdf; 'Hoe datahandelaren adressen van jou én van bedreigde personen te koop aanbieden', RTL, 5-1-2024,https://www.rtl.nl/boulevard/crime/artikel/5425259/geheime-adressen-bedreigde-journalisten-politici-en-advocaten-te; 'Nederlandse telefoons online stiekem te volgen: 'Extreem veiligheidsrisico'', BNR, 10-01-2024,https://www.bnr.nl/nieuws/technologie/10537256/nederlandse-telefoons-online-stiekem-te-volgen-extreem-veiligheidsrisico; 'Kabinet wil bewustzijn burgers over dataverzameling apps en sites vergroten', Security.nl, 26-06-2024,https://www.security.nl/posting/847721/Kabinet+wil+bewustzijn+burgers+over+dataverzamelin-g+apps+en+sites+vergroten.

163 'Kabinet wil bewustzijn burgers over dataverzameling apps en sites vergroten', Security.nl, 26-06-2024,https://www.security.nl/posting/847721/Kabinet+wil+bewustzijn+burgers+over+dataverzamelin-g+apps+en+sites+vergroten.

164 'ACT SHEET: President Biden Issues Executive Order to Protect Americans' Sensitive Personal Data', The White House, 28-02-2024,https://www.whitehouse.gov/briefing-room/statements-releases/2024/02/28/fact-sheet-president-biden-issues-sweeping-executive-order-to-protect-americans-sensitive-personal-data/.

165 'Biden order will limit how much data can be sold to Russia and China', The Record, 28-02-2024,https://therecord.media/biden-executive-order-data-sales-adversaries-russia-china.

166 'Cybercrimebeeld Nederland 2024', Openbaar Ministerie & Politie, 11-6-2024, https://www.om.nl/onderwerpen/cybercrime/cybercrimebeeld-cybercrimebeeld-ccbn

167 Interne informatie, afkomstig van Openbaar Ministerie.

168 Vrij naar diverse artikelen van en een presentatie door Keymolen, w.o. 'Trust and trustworthiness in a data-driven context', E. Keymolen, 27-03-2020, https://www.youtube.com/watch?v=oqr39l7sjyU; 'Regulating security on the Internet: control versus trust', Bibi van den Berg & Esther Keymolen,International Review of Law, Computers & Technology, 31:2.; 'Can we trust trust-based data governance models?', Bart van der Sloot, Esther Keymolen, in Data & Policy (2022); 'Trustworthy tech companies: talking the talk or walking the walk?', Esther Keymolen, AI Ethics (2023). Keymolen behandelt het concept van vertrouwen breder dan digitale veiligheid. De link met digitale veiligheid is de eigen interpretatie van de auteurs.

169 'Digitalisering van het verkiezingsproces? Bij twijfel niet doen', 16-3-2023, https://www.nederlandrechtsstaat.nl/digitalisering-van-het-verkiezingsproces-bij-twijfel-niet-doen/.

170 'Trust and trustworthiness in a data-driven context', E. Keymolen, 27-03-2020, https://www.youtube.com/watch?v=oqr39l7sjyU.

171 In het CSBN2023 werden zowel de DMA als DSA beschreven. Vanwege deze reden zijn deze ook dit jaar opgenomen, om zo de voortgang te kunnen weergeven.

172 'Eerste bedrijven onder Digital Services Act', Digitale Overheid, 8-5-2023, https://www.digitaleoverheid.nl/nieuws/europese-dsa-verscherpt-online-toezicht/ ; ' DSA voor alle digitale diensten van kracht', Digitale Overheid, 19-2-2024, https://www.digitaleoverheid.nl/nieuws/dsa-voor-alle-digitale-diensten-van-kracht/.

173 'Overzicht wetten en regels voor online platforms', Autoriteit Consument & Markt, n.d., https://www.acm.nl/nl/online-platforms/overzicht-wetten-en-regels-voor-online-platforms.

174 'Europees akkoord: veiligheidseisen en standaarden voor alle digitale producten', Rijksoverheid, 1-12-2023, https://www.rijksoverheid.nl/actueel/nieuws/2023/12/01/europees-akkoord-veiligheid-seisen-en-standaarden-voor-alle-digitale-producten.

175 'Voortgangsrapportage Nederlandse Cybersecuritystrategie', Rijksoverheid, 9-10-2023, https://www.rijksoverheid.nl/documenten/rapporten/2023/10/09/tk-bijlage-1-voortgangsrapportage-nederlandse-cybersecuritystrategie-2023.

176 'VERORDENING (EU, Euratom) 2023/2841 VAN HET EUROPEES PARLEMENT EN DE RAAD', Publicatieblad van de Europese Unie, 18-12-2023, https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=OJ:L_202302841

177 'The EU Cyber Solidarity Act', Europese Commissie, n.d., https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity.

178 'Ransomware-aanvallen op instellingen en bedrijven in Nederland',Dialogic Innovatie en Interactie, 12-09-2023, https://repository.wodc.nl/handle/20.500.12832/3292.

179 'Jaarbeeld Ransomware 2023', Project Melissa, 22-02-2024,https://cyberveilignederland.nl/upload/userfiles/files/Jaarbeeld_Ransomeware_2023_jan_dec.pdf.

180 Toelichting medewerker project Melissa tijdens interview.

181 'Jaarbeeld Ransomware 2023', Project Melissa, 22-02-2024,https://cyberveilignederland.nl/upload/userfiles/files/Jaarbeeld_Ransomeware_2023_jan_dec.pdf.

182 Gegevens Autoriteit Persoonsgegevens verkregen uit bilaterale contacten.

Colofon

Het Cybersecuritybeeld Nederland 2024 (CSBN 2024) 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 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. Het CSBN 2024 vormt een inhoudelijke basis voor de evaluatie van het daarvan afgeleide actieplan. De focus van het CSBN ligt op de nationale veiligheid.

Het CSBN is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). In de totstandbrenging is samengewerkt met het Nationaal Cyber Security Centrum (NCSC). De NCTV heeft dankbaar gebruikt gemaakt van de informatie, de inzichten en de expertise van overheidsdiensten, aanbieders van vitale processen, wetenschappers en andere partijen. 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 draagt bij aan het digitaal weerbaar maken van Nederland en, daarbij, aan het creëren van een gunstig digitaal klimaat voor organisaties en de samenleving. Dat doet het NCSC door in samenwerking met andere publieke en private partners in binnen- en buitenland de digitale weerbaarheid van organisaties te bevorderen. Ook helpt het NCSC cyberincidenten en -crises met een ontwrichtend karakter te voorkomen en de impact ervan 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

Oktober 2024