Digitalisering is allang niet meer een geïsoleerd of op zichzelf staand proces dat gestart is om 'papieren' middelen om te zetten in techniek. Digitalisering is bovendien al veel meer dan het gebruik en de werking van IT. De gigantische ontwikkelingen en de diverse informatiesystemen, telecommunicatie(middelen), digitale informatie, data, informatie- en computersystemen hebben ook een steeds verdergaande en toenemende invloed op de economie, op de samenleving en op de menselijke gedragingen. Nee, het is zelfs veel sterker dan dat: veel beter kan worden gesproken over een doorgaande digitale transitie; de verdergaande intense verwevenheid en verknoping van IT in steeds meer aspecten van het dagelijks leven en de economische processen die vervolgens op hun beurt in steeds meer netwerken opgenomen zijn met allerlei verbindingen en afhankelijkheden.

Digitalisering biedt oplossingen voor maatschappelijke problemen, maar brengt ook risico's met zich mee. Strategische punten bij de verdere ontwikkeling van digitalisering zijn de informatiebeveiliging, de interoperabiliteit van data/gegevens en binnen organisaties de rollen en verantwoordelijkheden van de verschillende stakeholders: professionele medewerkers en management. Voldoende goed gekwalificeerd personeel zal beschikbaar en het 'IT-budget' zal toereikend moeten zijn voor – ook – die andere aandachtsgebieden. Voor informatiebeveiliging zal bijzonder aandacht moeten zijn binnen de organisatiestructuur om recht te doen aan de toegenomen digitale dreigingen en de noodzaak om hier een goed gefundeerde besturing voor in te richten. Daar komen ook nog de afhankelijkheden bij in een 'digitale monocultuur': een kwetsbaarheid in één product raakt vele andere informatietechnologieën, dat een groot deel van de publieke sector en het bedrijfsleven kan raken.

Op nationaal niveau zijn de afgelopen jaren enkele belangrijke onderzoeken gedaan en is er gerapporteerd over het thema digitale veiligheid. Adviezen zijn gegeven over hoe 'verstoring van de digitale infrastructuur' dan wel een 'digitale ontwrichting' en 'cyberrampen' voorkomen kunnen worden alsook hoe 'cyberincidenten' zo spoedig mogelijk bestreden dan wel beheersbaar kunnen worden gemaakt.
De aanbevelingen uit al die rapporten geven vaak een eenduidige tendens aan: het Nederlandse digitale poldermodel is niet goed toegesneden, er dreigen digitale ontwrichtingen, de instanties reageren te traag én zowel aanbiedende fabrikanten, consumenten c.q. burgers, ondernemingen die gebruik maken van IoT-apparaten en andere IT-middelen kunnen en moeten veel meer doen aan cybersecure en cybersafe handelen. Nederlandse overheidsorganisaties en bedrijven zijn zeer kwetsbaar voor cyberaanvallen en er bestaat geen nationale structuur waarlangs alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd.

Dit artikel voorziet in een zeer beknopt overzicht van die rapporten.

AR: al meer dan tien jaar onderzoek

De Algemene Rekenkamer (AR) doet al meer dan tien jaar onderzoek naar informatiebeveiliging en heeft deze recent weer geanalyseerd. 'Hieruit blijkt herhaaldelijk dat de gestelde ambities op het gebied van digitalisering niet goed in balans zijn met de mensen, middelen en organisatie', zo valt op rekenkamer.nl/onderwerpen/ICT-en-digitalisering te lezen. De AR vraagt regelmatig aandacht voor het eenduidig beleggen van taken en een adequate invulling van verantwoordelijkheden, bijvoorbeeld rondom cybersecurity, informatiebeveiliging, het e-ID stelsel en het stelsel van basisregistraties. Zo wordt ook gevraagd om een (meer) coördinerende rol voor de verantwoordelijke bewindspersoon in het kabinet. 'Dat kan een uitbreiding van bevoegdheden van de minister inhouden, zoals bij informatiebeveiliging, waar resultaten achterblijven', zo schrijft de AR (1).

WRR: voorbereiden op digitale ontwrichting

De Wetenschappelijke Raad voor het Regeringsbeleid (WRR) startte in 2018 een adviestraject over hoe Nederland kan omgaan met een mogelijke cyberramp. De overheid en aanbieders van vitale processen hebben beperkt zicht op de partijen van wie zij afhankelijk zijn. Op het terrein van cybersecurity krijgt de voorbereiding op ontwrichting echter weinig aandacht. Dit maakt het lastig om de ernst van incidenten te kunnen vaststellen en het hoofd te bieden aan een digitale ontwrichting. Bij de bestrijding hiervan ontbeert de overheid bovendien een duidelijk omschreven bevoegdheid om in te grijpen. In het rapport Voorbereiden op digitale ontwrichting (2) pleit de WRR voor een betere voorbereiding op een digitale ontwrichting door o.a. adequate bevoegdheden om escalatie te voorkomen en inspanningen op het terrein van cyberverzekeringen te verrichten.

Van 'digitale maatschappelijke ontwrichting', of kortweg 'digitale ontwrichting' is volgens de WRR sprake als - door de groeiende verwevenheid van de digitale wereld met de fysieke en de sociale wereld - verstoringen van het maatschappelijke leven steeds vaker samenhangen met een ernstige verstoring of uitval van digitale processen. Van digitale ontwrichting is sprake wanneer het normale leven ernstig is verstoord.
De WRR stelt dat incidenten – door onderlinge afhankelijkheden en door de complexiteit en diversiteit van netwerk- en informatiesystemen – sneller grootschalige en grensoverschrijdende effecten

bezitten. Volgens de WRR moeten zowel de overheid als het bedrijfsleven samenwerken ten einde voorbereid te zijn op incidenten in de digitale ruimte.

De WRR deed een aantal aanbevelingen, waaronder de volgende:

- besteed bij het beleid voor vitale infrastructuur meer aandacht aan de ketens en netwerken die vitale processen ondersteunen;
- onderzoek bovendien of digitalisering het nodig maakt de prioritering van die processen aan te passen; en
- benut nationale en internationale incidentdata beter, om lessen te trekken met het oog op toekomstige verstoringen.

CSR: integrale aanpak cyberweerbaarheid

Ook de Cyber Security Raad (CSR) liet in april 2021 op een vergelijkbare wijze van zich horen. In het rapport Integrale aanpak cyberweerbaarheid (3) stelde de CSR dat digitale veiligheid op het hoogst bestuurlijke niveau moet worden belegd. Op dit moment is de cyberweerbaarheidsketen in Nederland niet op alle punten even sterk. Hierdoor ontstaan er lacunes en gebreken waardoor de cyberweerbaarheid van Nederland op diverse onderdelen zwakheden vertoont. De CSR adviseert voor de langere termijn te verkennen hoe het besturingsmodel zo kan worden ingericht dat overheden, inclusief de decentrale overheden, bedrijfsleven en wetenschap gezamenlijk kunnen werken aan één nationale cyberweerbaarheidsstrategie. "Wij gaan hier echt stevig werk van maken. Niet omdat het kan, maar omdat het moet", zei de demissionair minister van JenV bij de inontvangstneming.

RvS: precisie, standaardisatie en centralisatie

In mei 2021 bracht de Raad van State (RvS) een publicatie uit waarin het zijn visie ontvouwt op het gebied van digitalisering. Natuurlijk adviseert de RvS dat de wetgever waarborgen moet bieden voor de bescherming van de rechten van burgers en bedrijven bij algoritmische besluitvorming. Algoritmische besluitvorming is complex en vaak lastig uit te leggen. De bestuursrechter moet burgers rechtsbescherming bieden bij algoritmische besluitvorming. Er is een verscheidenheid in situaties en van complicaties waarmee men bij de uitvoering geconfronteerd zal worden. De RvS geeft na deze beschouwing aan op welke wijze dat beter kan: 'Dat wordt dan op de klassieke manier opgelost: door de bepalingen vaag te formuleren en in de toelichting alle mogelijkheden open te laten. Juristen en beleidsmakers gaan er doorgaans vanuit dat een gedigitaliseerde uitvoering de ruimte voor flexibiliteit, variëteit en oneindige mogelijkheden biedt. Het is echter precies omgekeerd: gedigitaliseerde uitvoering vraagt om precisie, standaardisatie en centralisatie, want alleen zo heeft men de voordelen van digitalisering' (4).

IvhO: meer sturing op cyberveiligheid

Naar aanleiding van de cyberaanval op de Universiteit Maastricht besteedde ook de Inspectie van het Onderwijs (IvhO) aandacht aan het thema cyberveiligheid in haar rapport met het heldere adagium 'Binnen zonder kloppen' (5). Onderwijsinstellingen zijn voor een groot deel zelf verantwoordelijk en daardoor onvoldoende beschermd. De IvhO vindt dat de overheid meer verantwoordelijkheid en regie moet nemen. 'Want de kennis en kunde blijkt in het veld zeker aanwezig, maar de sturing ontbreekt', aldus de IvhO. 'Het verhogen van de digitale weerbaarheid van de onderwijssector is niettemin noodzakelijk', maar 'ook moet het duidelijk zijn welke verantwoordelijkheden individuele instellingen zelf kunnen invullen, waar ze in gezamenlijkheid kunnen optreden om de kennis en expertise van alle ketenpartners optimaal te benutten en waar aanvullende coördinatie of ondersteuning vanuit de overheid nodig is', schrijft de demissionaire minister van OCW (6).

OvV: 'Kwetsbaar door software': fundamenteel ingrijpen

Het meest recente rapport over dit thema komt van de Onderzoeksraad voor Veiligheid (OvV). De OvV is duidelijk en zeer helder. De Nederlandse aanpak van digitale veiligheid moet snel en fundamenteel veranderen om te voorkomen dat de maatschappij ontwricht raakt door cyberaanvallen. Tot deze stevige conclusie kwam de OvV in het rapport Kwetsbaar door software (7). De OvV onderzocht beveiligingslekken die ontstonden bij duizenden organisaties door kwetsbaarheden in de software van Citrix. De OvV-voorzitter stelde duidelijk: 'Uit dit voorval blijkt dat Nederlandse overheidsorganisaties en bedrijven zeer kwetsbaar zijn voor cyberaanvallen en dat er geen nationale structuur is waarbinnen alle potentiële slachtoffers van cyberaanvallen tijdig worden gewaarschuwd.' De OvV merkt in het bijbehorend persbericht op dat aanvallers 'tot op de dag van vandaag' illegale toegang hebben 'tot systemen en data in bedrijven en organisaties die zij op elk moment kunnen activeren met disruptieve effecten op bedrijfsprocessen, dienstverlening, privacy en veiligheid.'

De OvV ziet 'opvallende overeenkomsten' tussen de onderzochte voorvallen. Organisaties, mensen die afhankelijk zijn van organisaties en ketenpartners waren digitaal onveilig omdat zij kwetsbare software gebruikten. De OvV geeft ook aan dat 'incidentbestrijding nog geen sluitende, vanzelfsprekende, systematische ingebouwde reflex is.'

Vanwege de doorgaande digitale transitie verkrijgen we steeds meer mogelijkheden, maar daarmee creëren we ook een steeds grotere afhankelijkheid van de digitale systemen. Fabrikanten, overheden en organisaties zullen samen tot een effectieve aanpak moeten komen om Nederland weerbaarder te maken tegen cybercriminaliteit; dus voorbereiden van een organisatie om

repressief te kunnen reageren. 'Fabrikanten overstelpen softwaregebruikers nu met patches en updates om gebreken in hun software te verhelpen zonder met structurele oplossingen te komen'. 'Er zijn geen instrumenten die afnemers van software onafhankelijk inzicht bieden in de veiligheid van de software. Ook schiet de eigen kennis en positie van afnemers vaak tekort om zelf eisen te stellen aan fabrikanten en veiligere software af te dwingen, of zien zij daar het belang niet van in', aldus de OvV. Dit vraagt van fabrikanten dat zij de veiligheid van hun software voortdurend en fundamenteel verbeteren. Door samen te werken kunnen afnemers hun positie richting softwarefabrikanten versterken en hun schaarse expertise beter benutten.

Dat vergt dat er één bewindspersoon en één centrale dienst komt die hierop toeziet, zo nodig kan ingrijpen en verantwoording aflegt. Ook beveelt de OvV aan dat grotere bedrijven en organisaties wettelijk worden verplicht om verantwoording af te leggen over de wijze waarop zij hun digitale veiligheid beheersen.

Korte beschouwingen

De inhoud van deze rapporten komen grosso modo overeen, al dan niet soms anders geformuleerd.

– De publieke sector en het bedrijfsleven zijn onvoldoende voorbereid om mogelijke, digitale ontwrichtingen te voorkomen en te bestrijden. De digitale polder functioneert onvoldoende of te traag door de vele lagen om de toenemende bedreiging goed het hoofd te kunnen bieden;

– De onderzoeken geven aan dat de kennis en kunde aanwezig is, maar overheden en het bedrijfsleven moeten hun krachten bundelen, meer regie, meer centralisatie, meer (en aanvullende) coördinatie tot stand brengen;

– De wens is om te komen tot één nationale cyberweerbaarheidsstrategie;

– Er wordt steeds meer geadviseerd een nationale 'instanz- und behördenübergreifende' structuur te laten ontstaan waarbij een effectieve vorm van regie met betrekking tot samenwerking vorm moet krijgen. Deze centrale dienst zal de informatiedeling sneller moeten verspreiden zodat alle belanghebbende organisaties tijdiger geworden gewaarschuwd om zodoende snel mitigerende maatregelen te nemen;

– Een aardige gedachte is om grotere bedrijven en organisaties wettelijk te verplichten om verantwoording af te leggen over de wijze waarop zij hun digitale veiligheid beheersen; dit naar analogie van de verplichte accountabilityverplichtingen uit de AVG/GDPR;

– Fabrikanten zullen de veiligheid van hun software voortdurend en fundamenteel moeten verbeteren. Dit zijn eigenlijk de alom bekende vereisten van 'privacy/security by design' en verbeteringen die worden doorgevoerd na toepassing van die ontwikkelprincipes! Inkopende organisaties kunnen dat uiteraard zelf afdwingen. In het bestek van aanbestedingsprocedures en bij andere inkoopprocedures kunnen eisen worden gesteld alvorens die IT-middelen daadwerkelijk aan te schaffen. Wellicht dat als IT-middelen door een virus getroffen worden, zouden achteraf de leveranciers aansprakelijk kunnen worden gesteld. Dan is het leed echter al geschied. Een zorgplicht voor fabrikanten – voor levering van veilige hard- en software aan burgers, bedrijven en overheid – kan leiden tot een vooraf beschermen alsook tijdig en snel leveren van eventuele updates en patches.

De zwakste schakel

De rapporten en de aanbevelingen zijn er. Nu is het te bezien hoe de CEO's en de bestuurders dit gaan oppakken hoe deze aanbevelingen georganiseerd worden. De sterke schakel is dat er voldoende kennis en kunde aanwezig is om Nederland voldoende cyberveilig te houden en nog cyberveiliger te krijgen. Fabrikanten kunnen meer doen om cybersecure en cybersafe producten te ontwikkelen. 'De zwakste schakel in de cyberketen is de mens. Maar dat is niet per se de gebruiker. Het kan ook de ontwerper van de beveiliging van het informatiesysteem zijn' (8). Het op peil houden van de cyberawareness voor burgers c.q. consumenten c.q. werknemers is van groot belang. Er zal maar dat ene mailtje met malware binnenkomen; hopelijk wordt dat niet geopend.
De soft controls goed realiseren blijft altijd het lastigst en probeer de boodschap positief over te brengen. En, o ja, denk niet aan de smaak van citroen.

Referenties

(1) AR (2019), https://www.rekenkamer.nl/onderwerpen/ict-en-digitalisering

(2) WRR (2019), Voorbereiden op digitale ontwrichting (rapport nr. 101, 2019) Den Haag; wrr.nl/adviesprojecten/digitale-ontwrichting

(3) CSR (2021), Integrale aanpak cyberweerbaarheid, Advies 2021, nr. 2, Den Haag; cybersecurityraad.nl/documenten/adviezen/2021/04/06/csr-adviesrapport-integrale-aanpak-cyberweerbaarheid

(4) RvS (2021), Digitalisering - wetgeving en bestuursrechtspraak, Den Haag, p. 116-117; raadvanstate.nl/publicaties/studies-onderzoeken/

(5) IvhO (2021), Binnen zonder kloppen - digitale weerbaarheid in het hoger onderwijs, Utrecht

(6) Kamerstukken II, 2021/22, 31 288, 31 524 en 26 643, nr. 922

(7) OvV (2021), Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix, Den Haag; onderzoeksraad.nl/nl/page/17171/kwetsbaar-door-software-lessen-naar-aanleiding-van

(8) Kok, T. de (2021), De zwakste schakel in de cyberketen kan ook de ontwerper zijn! agconnect.nl/blog/de-zwakste-schakel-de-cyberketen

Lexicon

Informatiebeveiliging is het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit en ook het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen (1).
Cybersecurity alle beveiligingsmaatregelen die men neemt om schade te voorkomen door een storing, uitval of misbruik van een informatiesysteem of computer. Ook worden maatregelen genomen om schade te beperken en/of te herstellen als die toch is ontstaan. Voorbeelden van schade zijn dat men niet meer in een computersysteem kan komen wanneer men dat wil. Of dat de opgeslagen informatie bij anderen terecht komt of niet meer klopt. De maatregelen hebben te maken met processen in de organisatie, technologie en gedrag van mensen.
Datasecurity gaat over de bescherming gedurende de gehele lifecycle van digitale informatie tegen bedoelde of onbedoelde aanpassing, verwijdering, diefstal of openbaarmaking van data door ongeautoriseerde personen.
Cybersafety kent twee betekenissen:

1. De veiligheid en betrouwbaarheid van het geautomatiseerde systeem: dat componenten betrouwbaar werken en hun functies kunnen vervullen om, bijvoorbeeld, beschermd te zijn tegen oververhitting (2) en
2. Cybersafety is kort gezegd online veilig zijn. Cybersafety helpt je met het ontwijken van gevaren, maar helpt je ook je te beschermen tegen de gevolgen ervan. Je kunt namelijk niet alles ontwijken. Sommige aanvallen overkomen je, hoewel je aan alle gangbare beveiligingseisen voldoet (3).

Referenties

(1) Art. 1 onder k Besluit CIO-stelsel Rijksdienst 2021

(2) Fraunhofer magazine 3, 2021, p. 44: fraunhofer.de/s/ePaper/magazine/2021/03/index.html

(3) https://www.utwente.nl/nl/cyber-safety/cybersafety/

Kleine catalogus van cyberrisico's [1,2]

Cybercriminaliteit in enge zin
Het gebruik van informatiesystemen en computers niet alleen als middel, maar ook als doel. Bijvoorbeeld computers beschadigen, spamaanvallen, DDoS-aanvallen, virussen verspreiden.
Cybercriminaliteit in brede zin
Dit zijn alle strafbare activiteiten waarbij iemand een informatiesysteem of computer gebruikt. Denk aan diefstal en vervalsing van betaalpassen, oplichting, afpersing, kinderporno, racisme en belediging.
Georganiseerde cybercriminaliteit
Criminele netwerken die gebruik maken van IT, waarbij dat gebruik invloed heeft op hun criminele bedrijfsprocessen, maar meestal zonder enige ideologische achtergrond.
Dit kan theoretisch worden onderscheiden in: (3, 4)

– Traditionele georganiseerde criminaliteit, dat wil zeggen zaken zonder een sterke IT-component. Het gaat dan om gevallen van offline drugshandel, mensenhandel/-smokkel en andere (combinaties van) misdrijven;
– Traditionele georganiseerde criminaliteit met IT als belangrijk vernieuwend element in de modus operandi, zoals zaken van door IT gefaciliteerde drugshandel/-smokkel en een zaak waarin het witwassen van Bitcoins centraal staat.
– Georganiseerde low-tech cybercriminaliteit, waartoe skimming en phising wordt gerekend bij de low-tech cybercriminaliteit; hierbij maken daders gebruik van contacten die ze hebben in het criminele milieu;
– Georganiseerde hightech cybercriminaliteit: zaken als banking malware; kernleden van het criminele samenwerkingsverband de benodigde technische expertise verschaffen door het gebruik van forums.

Cyberterrorisme
Terroristische activiteiten die digitaal worden uitgevoerd, met (enige) ideologische achtergrond. Bijvoorbeeld het beschadigen of uitschakelen van belangrijke informatienetwerken via internet.
Cyberspionage
Het binnendringen van digitale systemen voor het verkrijgen van vertrouwelijke informatie, vaak strategisch, economisch of militair van aard, veelal door staten of (staats)bedrijven.
Cyberoorlog/cyberwar(fare)
Digitale (genetwerkte) technieken die gebruikt worden om de systemen van staten of organisaties aan te vallen. Vaak met een militair of strategisch doel.

Referenties

(1, 2) Verder ontwikkeld en geïnspireerd op:
Gaycken, S. (2015) Cybersecurity – Kleiner Katalog der Cyberrisiken. In: Jäger, T. (eds) (2015) Handbuch Sicherheitsgefahren. Globale Gesellschaft und internationale Beziehungen, Wiesbaden Springer, p. 230 en het Cyberveilig Nederland i.s.m. Cybersecurity Alliantie (2021). Cybersecurity Woordenboek : van cybersecurity naar Nederlands, 3e druk
(3) Kruisbergen, E. W., Leukfeldt, R., Kleemans, E. R., & Roks, R. (2018). Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit. (Cahier; Vol. 2018, No. 8). WODC.
(4) Kruisbergen, E. W., Leukfeldt, R., Kleemans, E. R., & Roks, R. (2018). Criminele geldstromen en ICT: over innovatieve werkwijzen, oude zekerheden en nieuwe flessenhalzen. WODC: Justitiële Verkenningen 44(5), 23-39.

Enkele kwetsbaarheden

DigiNotar (2011)
DigiNotar was een publicly trusted Certificate Authority (CA)en verzorgde de beveiliging van de elektronische communicatie door en tussen overheden (de zgn. Public Key Infrastructure of PKI). In 2011 werd dit bedrijf gehackt. Hierdoor kreeg een externe partij de mogelijkheid valse SSL-certificaten uit te geven en werden de certificaten onbruikbaar.

WannaCry (2017)
WannaCry (ook WannaCrypt, WanaCrypt0r 2.0 of Wanna Decryptor) is een ransomware ontwikkeld voor het Microsoft Windows besturingssysteem. WannaCry bestaat uit twee componenten: een ransomwarecomponent en een worm. Een uitbraak van dit ransomware heeft plaatsgevonden en het besmette daarbij meer dan 230.000 computers in 150 landen. Door de cyberaanval WannaCry viel een deel van de Britse gezondheidszorg uit.

NotPetya (2017)
NotPetya legde de productie van belangrijke medicijnen plat en kostte één van de grootste containerrederijen ter wereld honderden miljoen euro's.

Universiteit Maastricht (2019)
Cyberaanval waardoor de goede voortgang van het onderwijs en onderzoek tijdelijk in gevaar was. Tien dagen was de universiteit digitaal op slot waardoor medewerkers en studenten geen gebruik konden maken van het netwerk en de ICT-diensten van de universiteit.

Citrix (2020)
Ernstige kwetsbaarheid in 2 Citrix-servers: Citrix ADC en Citrix Gateway. Door deze kwetsbaarheid in het Citrix-systeem kunnen hackers toegang krijgen tot het computersysteem van uw organisatie.

Hof van Twente (2020)
Criminelen kwamen de systemen van de gemeente Hof van Twente binnen via een openstaande RDP-poort die kan worden gebruikt voor beheer op afstand. Door middel van een bruteforceaanval ofwel het proberen van grote hoeveelheden gebruikersnaam/wachtwoord-combinaties, kregen de aanvallers toegang tot een van de servers met een testbeheerdersaccount.

SolarWinds Orion (2021).
Volgens SolarWinds is de kwetsbaarheid opzettelijk gecreëerd door een actor, met als achterliggend doel om de systemen te compromitteren van de afnemers van de betreffende versie van SolarWinds Orion. Deze kwetsbaarheid kan door kwaadwillenden worden misbruikt om toegang te krijgen tot bijvoorbeeld informatie of beheersfuncties van organisaties.

Log4J (2021)
Een Denial-of-Service-kwetsbaarheid van in Apache Log4j. Dit is software die veel gebruikt wordt in webapplicaties en allerlei andere systemen. Het is een Log4Shell-gat in Java-tool Log4j. Ontwikkelaars gebruiken die logbestanden om te kijken of hun programma's naar behoren functioneren. Door de registraties te manipuleren kunnen hackers Log4J hun eigen, kwaadaardige code laten downloaden en uitvoeren.

Rode Kruis (2022)
Het Internationale Comité van het Rode Kruis (ICRC) in Genève (Zwitserland) werd slachtoffer van een geavanceerde cybersecurityaanval. Daarbij werden van zeker 515.000, vaak kwetsbare mensen de privégegevens weggenomen. De data is over de hele wereld gestolen, ook bij lokale verenigingen van het Rode Kruis.

Nederlandse securitycentra

NCSC
Het Nationaal Cyber Security Centrum (NCSC) is, met het oog op het voorkomen en beperken van maatschappelijke ontwrichting door cyberdreigingen en -incidenten en het versterken van de digitale weerbaarheid van de samenleving, belast met:

a. het informeren, adviseren en bijstaan van de rijksoverheid en vitale aanbieders in geval van dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen;
b. het informeren van anderen;
c. het verrichten van analyses en technisch onderzoek naar aanleiding van cyberdreigingen en -incidenten;
d. het aan anderen verstrekken van analyses verkregen informatie over dreigingen en incidenten betreffende andere netwerk- en informatiesystemen;
e. de taken van het centraal contactpunt, bedoeld in de Wet beveiliging netwerk- en informatiesystemen;
f. het bevorderen en voeren van het secretariaat van de publiek-private samenwerking op het gebied van cybersecurity.

DTC
Het DTC waarschuwt niet-vitale bedrijven wanneer er sprake is van specifieke, ernstige cyberdreigingen. Dit zijn actuele cyberaanvallen of kwetsbaarheden in bedrijfsapplicaties die een grote kans op misbruik hebben en potentieel veel schade kunnen aanrichten.

Het DTC en NCSC vormen samen met verschillende sectorale computercrisisteams en schakelorganisaties het groeiende Landelijk Dekkend Stelsel (LDS) van cybersecurity- samenwerkingsverbanden

CSIRT

De taken van een Computer Security Incident Response Teams zijn onder andere:

- reageren op incidenten die vrijwillig of verplicht worden gemeld;
- incidenten op nationaal niveau monitoren, aanbieders vroegtijdig waarschuwen en informatie over risico's en incidenten verspreiden;
- deelnemen aan het internationale netwerk van CSIRT's en
- op samenwerking gerichte contacten onderhouden met de particuliere sector.

Het CSIRT-DSP is het nationale Cyber Security Incident Response Team voor digitale dienstverleners.

CERT

Een Computer Emergency Response Team (CERT) is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen. Naast reactie op incidenten richt een CERT zich ook op preventie en preparatie.

Er is een aantal sectorale CERT's: Z-CERT voor zorginstellingen, SURFcert voor onderwijsinstellingen, IBD voor gemeenten en WM-CERT voor waterschappen.
Daarnaast bestaan er Organisaties die Kenbaar Tot Taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten (OKTT's)

SOC

Een Security Operations Center (SOC) is een eenheid, die binnen de organisatie monitort om inzicht en grip te hebben op de digitale infrastructuur binnen uw organisatie en op wat daarbinnen allemaal gebeurt. Vanuit applicaties en apparaten wordt loginformatie verzameld en onderzocht op mogelijke aanvallen. Door correlatie van gegevens wordt bepaald of er afgeweken wordt van de standaard. De loginformatie is afkomstig van verschillende bronnen zoals servers, firewalls, (web)applicaties, infrastructurele componenten en endpoint-protectiesystemen.

SIEM

Een hulpmiddel dat onlosmakelijk verbonden is met een SOC is een Security Information & Event Management (SIEM) systeem. Het betreft software die in staat is om loginformatie vanuit verschillende bronnen te interpreteren en te correleren naar wat zich binnen en rondom het netwerk afspeelt op gebied van cyberaanvallen en andere beveiligingsincidenten.