Nationaal Cyber Security Centrum
*Ministerie van Veiligheid en Justitie*

# Cybersecuritybeeld Nederland

## CSBN-4

# Cybersecuritybeeld Nederland

CSBN-4

## Nationaal Cyber Security Centrum

Het Nationaal Cyber Security Centrum (NCSC) draagt via samenwerking tussen bedrijfsleven, overheid en wetenschap bij aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein.

Het NCSC ondersteunt de Rijksoverheid en organisaties met een vitale functie in de samenleving met het geven van expertise en advies, response op dreigingen en het versterken van de crisisbeheersing. Daarnaast biedt het NCSC informatie en advies voor burger, overheid en bedrijfsleven ten behoeve van bewustwording en preventie. Het NCSC is daarmee het centrale meld- en informatiepunt voor ICT-dreigingen en -veiligheidsincidenten.

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

## Samenwerking en bronnen

Bij het opstellen van dit rapport heeft het NCSC dankbaar gebruik gemaakt van informatie die de volgende partijen beschikbaar hebben gesteld:

- De ministeries
- MIVD
- DefCERT
- AIVD
- politie (THTC)
- OM
- Belastingdienst
- leden van de ISAC's
- NCTV
- wetenschappelijke instellingen
- universiteiten
- experts uit het cybersecuritywerkveld

Hun bijdragen, inhoudelijke reviews, openbaar toegankelijke bronnen, een enquête, informatie van de vitale sectoren en analyses van het NCSC hebben samen bijgedragen aan de inhoudelijke kwaliteit van het beeld.


1

# INHOUD

# KERNBEVINDINGEN

1 POTENTIËLE IMPACT VAN CYBERAANVALLEN EN VERSTORINGEN NEEMT TOE DOOR VERDERGAANDE DIGITALISERING

2 GEBREK AAN ICT DUURZAAMHEID EN TOENEMENDE KOPPELING VORMEN RISICO VOOR MAATSCHAPPELIJKE VEILIGHEID

3 CYBERCRIMINELEN EN STATEN BLIJVEN GROOTSTE DREIGING

4 PRIVACY ONDER DRUK DOOR DATAVERZAMELING

# SAMENVATTING

**Het Cybersecuritybeeld Nederland (CSBN) wordt jaarlijks door het Nationaal Cyber Security Centrum (NCSC) gepubliceerd en komt tot stand in nauwe samenwerking met publieke en private partijen. Doel is het bieden van inzicht in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity over de periode april 2013 tot en met maart 2014.**

De focus van het CSBN ligt op de ontwikkelingen in Nederland. Ook belangwekkende ontwikkelingen in het buitenland zijn meegenomen. Het CSBN is een feitelijke beschrijving, met duiding op basis van inzicht en expertise vanuit overheidsdiensten, vitale sectoren en wetenschap. Voor dit CSBN is opnieuw samengewerkt met een groot aantal partijen, zowel publieke (bijvoorbeeld politie, inlichtingen- en veiligheidsdiensten en het openbaar ministerie), wetenschappelijke, als private (vitale sectoren) partijen.

Het aantal toepassingen van ICT en internet neemt in Nederland nog altijd drastisch toe. Anno 2014 zijn de Nederlandse burger, de overheid en het bedrijfsleven meer dan ooit afhankelijk van ICT en internet. Het aantal apparaten (waaronder computers, telefoons, tablets, medische apparatuur en vervoermiddelen) dat gebruik maakt van internet neemt nog altijd toe, net als het aantal functies dat (aan internet of met elkaar) verbonden apparaten vervullen.

Als de afgelopen periode iets duidelijk heeft gemaakt, is het dat de afhankelijkheid van ICT grote risico's met zich meebrengt. Tot voor kort werden deze risico's vooral gezien in termen van bescherming tegen digitale verstoring, maar ook grip op informatie wordt steeds belangrijker. Gebruik en misbruik van informatie als persoonsgegevens of informatie over gedrag en interesses wordt een steeds belangrijker aspect van cybersecurity.

## Kernbevindingen

1 Potentiële impact van cyberaanvallen en verstoringen neemt toe door verdergaande digitalisering De belangen zijn de afgelopen periode weer substantieel toegenomen. Het gebruik en daarmee de afhankelijkheid van ICT nemen nog altijd toe. ICT is een drijvende kracht achter onze maatschappij en steeds meer processen zijn hiervan volledig afhankelijk. Dreigingen blijven onverminderd hoog, en ook de zichtbaarheid van hulpmiddelen van statelijke actoren en cybercriminelen is gegroeid. De maatregelen houden geen gelijke tred met de belangen en kwetsbaarheden.

Omdat de belangen substantieel toenemen, stijgt automatisch ook de potentiële impact van cyberaanvallen. Deze groeiende impact wordt onderstreept door de verstoringen die vorig voorjaar optraden door DDoS-aanvallen op Nederlandse banken en overheidsdiensten zoals DigiD. De grote afhankelijkheid van ICT voor onze maatschappelijke en persoonlijke veiligheid betekent dat een cyberverstoring of cyberaanval (in potentie) grote impact heeft op zowel de maatschappelijke als de persoonlijke veiligheid.

2 Gebrek aan ICT duurzaamheid en toenemende koppeling vormen risico voor maatschappelijke veiligheid De ontwikkeling dat steeds meer apparatuur (waaronder medische apparatuur, voertuigen, televisies en huishoudelijke apparaten) aan internet verbonden is, zal doorzetten. De software in deze apparatuur zal altijd beveiligingslekken bevatten. Veel apparatuur kan niet eenvoudig worden geüpdatet. Ook zal niet alle software gedurende langere tijd door de leverancier (kunnen) worden onderhouden. De apparatuur wordt kwetsbaar, waardoor een (potentieel) probleem ontstaat met het waarborgen van de maatschappelijke veiligheid. Dit is een gebrek aan duurzaamheid van ICT. De kwetsbaarheden die het afgelopen jaar in OpenSSL en Java zijn ontdekt zijn hiervoor illustratief. Updaten van alle apparatuur blijkt problematisch.

Daarnaast registreren steeds meer apparaten gegevens over hun omgeving en hun eigenaren. Zij verzamelen en delen deze informatie via internet (het fenomeen Internet der Dingen). Dit biedt grote kansen, maar ook grote uitdagingen op het gebied van cybersecurity en de grip op informatie.

3 Cybercriminelen en staten blijven grootste dreiging De grootste dreiging gaat uit van beroepscriminelen (vanwege diverse vormen van cybercriminaliteit) en van statelijke actoren (vanwege digitale spionage).

Criminele organisaties worden steeds professioneler. De contouren van een zeer professionele criminele dienstensector op het gebied van cybercrime worden steeds duidelijker. Dit werd in de afgelopen jaren al voorzien. Deze dienstensector is geen incident, maar een structureel onderdeel van cybercrime. Met behulp van deze diensten kunnen ook minder ervaren of geëquipeerde criminelen (complexe) cyberaanvallen uitvoeren of daarmee dreigen. Illustratief voor de professionalisering is de opkomst van CryptoLocker, een variant van ransomware waarbij het betalen van losgeld lijkt te helpen. Hiermee lijkt een winstgevend businessmodel te zijn ontstaan.

De dreiging van digitale spionage door statelijke actoren is onverminderd groot. Het aantal digitale spionageaanvallen is toegenomen, net als de complexiteit en impact. Bijna elke buitenlandse inlichtingendienst heeft de afgelopen jaren geïnvesteerd in digitale

capaciteiten. Digitale spionage is hierdoor niet langer voorbehouden aan grote en geavanceerde inlichtingendiensten.

4 Privacy onder druk door dataverzameling De trends van datificatie, het direct en indirect vastleggen van het dagelijks leven, en grootschalige dataverzameling zullen zich de komende jaren voortzetten. Dit leidt enerzijds tot maatschappelijke vooruitgang en meer mogelijkheden op veiligheidsgebied. Anderzijds brengt dit risico's met zich mee voor het individuele privacybelang en het belang van vertrouwelijkheid van informatie voor private organisaties en overheden.

Mondiale cases hebben het afgelopen jaar laten zien dat deze risico's reëel zijn en dat de belangen geschaad kunnen worden. Op het gebied van dataverzameling en data-exploitatie zijn gebruikers afhankelijk geworden van de intenties van statelijke en commerciële actoren. Hiermee zijn gebruikers tevens kwetsbaar voor een verandering in deze intenties.

**Wearables**
Het Internet der Dingen begint zichtbaar te worden in zogenaamde wearables zoals 'slimme brillen'. Een dergelijke bril hee de rekenkracht van een smartphone, kan beeld tonen aan de drager en bevat een camera. Langzamerhand komen zulke apparaten op de markt. Critici maken zich zorgen om hun privacy. Het is voor omstanders bijvoorbeeld niet duidelijk of de drager op dat moment aan het lmen is. Er kunnen bijvoorbeeld apps voor worden ontwikkeld die gezichtsherkenning gebruiken, en zo de drager informatie tonen over de mensen om hem heen, zonder dat zij dit in de gaten hebben. Tegenstanders vrezen zich bespioneerd te gaan voelen, omdat onbekend is wat er met de camerabeelden gebeurt en wie er meekijken.

## Hoofdvragen

In dit vierde Cybersecuritybeeld Nederland (CSBN-4) gelden opnieuw de onderstaande hoofdvragen:

» Welke Nederlandse belangen worden in welke mate geschaad door beperkingen van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie en welke ontwikkelingen doen zich daarbij voor? (**belangen**)
» Welke gebeurtenissen of welke activiteiten van welke actoren kunnen ICT-belangen aantasten, welke hulpmiddelen gebruiken zij en welke ontwikkelingen doen zich daarbij voor? (**dreigingen**)In hoeverre is Nederland weerbaar tegen kwetsbaarheden in ICT, kunnen die leiden tot aantasting van ICT-belangen en welke ontwikkelingen doen zich daarbij voor? (**weerbaarheid**)

## Inzicht in dreigingen en actoren

Tabel 1 geeft inzicht in de dreigingen die de verschillende actoren over de periode april 2013 tot en met maart 2014 hebben gebruikt om de doelwitten 'overheden', 'private organisaties' en 'burgers' aan te vallen.

## Belangen

Belangen en a ankelijkheid blijven toenemen, (potentiele) impact aanvallen en verstoringen neemt daarmee toe Net als in voorgaande jaren neemt de afhankelijkheid van ICT toe. Het gevolg is dat het niet-functioneren van ICT of inbreuk op de vertrouwelijkheid en integriteit van informatie steeds meer impact heeft op het leven van mensen, de manier van werken van Nederlandse organisaties en de continuïteit van de maatschappij. Deze toenemende afhankelijkheid is in versterkte mate van toepassing op de vitale sectoren. Cyberaanvallen en cyberverstoringen hebben in potentie grote impact op de persoonlijke en maatschappelijke veiligheid.

Uitdagingen door Internet der Dingen De ontwikkeling die bekend staat als Internet der Dingen(het fenomeen dat steeds meer apparaten gegevens verzamelen over hun omgeving en deze gegevens onderling of via het internet uitwisselen) heeft een positieve invloed, maar brengt ook grote uitdagingen op het gebied van cybersecurity met zich mee. Mensen gaan inventief om met de hierbij verzamelde gegevens en gebruiken deze voor andere doeleinden dan waar ze oorspronkelijk voor dienden. Hiermee ontstaan uitdagingen op het gebied van beveiliging en privacy.

Ketene ecten in de vitale sectoren Vitale sectoren merken steeds meer van keteneffecten in de omgang met cybersecurityrisico's. Andere opvallende zaken in de vitale sectoren zijn het grote, onderkende belang van het beschermen van persoonsgegevens, de impact van meer Customer Self Care (klantportalen) en het vergrote risico door steeds verdergaande uitbesteding van systeemkennis.

**DDoS-aanvallen**
De DDoS-aanvallen op DigiD zijn illustratief voor de impact die een aanval op een belangrijke schakel onder invloed van verdergaande digitalisering kan hebben op een volledige keten. De beperkte beschikbaarheid van DigiD als gevolg van enkele DDoS-aanvallen medio 2013 zorgde er niet alleen voor dat (semi-)overheidsdiensten voor burgers minder toegankelijk waren. Ook zorginstellingen en zorgverzekeraars maken steeds meer gebruik meer van DigiD als vertrouwd middel om toegang te verlenen tot hun klantportalen. Hierdoor kan het verstoren van één enkele schakel leiden tot ernstige verstoringen in meer dan één vitaal proces. Dit kan in potentie leiden tot ernstige schade aan de maatschappelijke groei.

## Dreigingen: actoren en hun intenties

De grootste dreiging gaat uit van statelijke actoren (vanwege digitale spionage) en van beroepscriminelen (vanwege diverse vormen van cybercriminaliteit).

**Doelwi□en**

| *Bron van Dreiging* | *Overheden* | *Private organisaties* | *Burgers* |
|---|---|---|---|
| **Staten** | Digitale Spionage | Digitale Spionage | Digitale Spionage |
| | O□ensieve cybercapaciteiten | O□ensieve cybercapaciteiten | |
| **Terroristen** | Verstoring/overname ICT | Verstoring/overname ICT | |
| **Beroepscriminelen** | Diefstal en publicatie of verkoop van informatie Q | Diefstal en publicatie of verkoop van informatie | Diefstal en publicatie of verkoop van informatie n |
| | Manipulatie van informatie Q | Manipulatie van informatie Q | Manipulatie van informatie |
| | Verstoring ICT n | Verstoring ICT n | Verstoring ICT 2 |
| | Overname ICT Q | Overname ICT n | Overname ICT |
| **Cybervandalen en scriptkiddies** | Diefstal informatie Q | Diefstal informatie Q | Diefstal informatie |
| | Verstoring ICT Q | Verstoring ICT | |
| **Hacktivisten** | Diefstal en publicatie verkregen informatie | Diefstal en publicatie verkregen informatie | Diefstal en publicatie verkregen informatie |
| | Defacement | Defacement | |
| | Verstoring ICT | Verstoring ICT | |
| | Overname ICT 2 | Overname ICT | |
| **Interne actoren** | Diefstal en publicatie of verkoop verkregen informatie | Diefstal en publicatie of verkoop verkregen informatie | |
| | Verstoring ICT | Verstoring ICT | |
| **Cyberonderzoekers** | Verkrijging en publicatie van informatie | Verkrijging en publicatie van informatie | |
| **Private Organisaties** | | Diefstal informatie (bedrijfsspionage) Q | Commercieel ge-/misbruik of 'doorverkopen' gegevens 2 |
| **Geen actor** | Uitval ICT | Uitval ICT | Uitval ICT |

**Legenda relevantie**

| *Laag* | *Midden* | *Hoog* |
|---|---|---|
| Er worden geen nieuwe trends of fenomenen waargenomen waarvan dreiging uitgaat.<br>OF Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen.<br>OF Er hebben zich geen noemenswaardige incidenten voorgedaan in de rapportageperiode | Er worden nieuwe trends en fenomenen waargenomen waarvan dreiging uitgaat.<br>OF Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen.<br>OF Incidenten hebben zich (op enkele kleine na) vooral voorgedaan buiten Nederland. | Er zijn duidelijke ontwikkelingen die de dreiging opportuun maken.<br>OF Maatregelen hebben beperkt e□ect, zodat de dreiging aanzienlijk blij□.<br>OF Incidenten hebben zich voorgedaan in Nederland. |

n dreiging is toegenomen Q dreiging is afgenomen 2 dreiging is nieuw

*Tabel 1. Dreigingsmatrix*

Verdere professionalisering criminele organisaties Criminele organisaties worden steeds professioneler. De contouren van een zeer professionele criminele dienstensector worden steeds duidelijker. Dit werd in de afgelopen jaren al voorzien. Cybercrime-as-a-service is geen incident, maar een structureel onderdeel van cybercrime. Hiermee kunnen ook minder ervaren of geëquipeerde criminelen (complexe) cyberaanvallen uitvoeren of daarmee dreigen.

Onverminderde dreiging digitale spionage Digitale spionage vormt net als voorgaande jaren een grote dreiging voor de overheid en de topsectoren in Nederland. De aanvallen winnen aan complexiteit, omvang en impact. Bijna elke inlichtingendienst heeft de afgelopen jaren geïnvesteerd in zijn digitale capaciteiten. Digitale spionage is hierdoor niet langer voorbehouden aan grote en geavanceerde inlichtingendiensten. Hoewel er nog weinig precedenten zijn, is de potentiële impact van de militaire inzet van offensieve cyberoperaties groot. Diverse landen hebben de afgelopen jaren dergelijke capaciteiten ontwikkeld.

A□ankelijkheid van intentie actoren De trends van dataficatie en dataverzameling zullen zich de komende jaren voortzetten. Dit leidt enerzijds tot maatschappelijke vooruitgang en meer mogelijkheden op veiligheidsgebied. Anderzijds brengt dit risico's met zich mee voor het individuele privacybelang en het belang van vertrouwelijkheid van informatie voor private organisaties en overheden.

Mondiale cases hebben de afgelopen jaren laten zien dat deze risico's reëel zijn en dat de belangen geschaad kunnen worden. Het verlies van grip op informatie blijft een reële dreiging. De inlichtingendiensten hebben geen indicaties dat bondgenoten het afgelopen jaar digitale spionageactiviteiten tegen de Nederlandse belangen hebben ontplooid. Vanuit niet-bondgenoten wordt de dreiging echter aanwezig en toenemend geacht.

Commerciële partijen nemen een steeds centralere rol in binnen de informatie-infrastructuur van individuen, bedrijven en overheden. De belangen zijn groot, de weerbaarheid laag en er zijn hulpmiddelen om de belangen te bedreigen. Eindgebruikers kunnen maar moeilijk vormgeven aan maatregelen om de kwetsbaarheden af te wenden. Op het gebied van dataverzameling en data-exploitatie zijn gebruikers afhankelijk geworden van de intenties van statelijke en commerciële actoren. Als deze intenties veranderen, kunnen Nederlandse belangen geschaad worden.

## Dreigingen: hulpmiddelen

Minder exploits of commercialisering exploits? Actoren maken gebruik van hulpmiddelen om kwetsbaarheden te misbruiken of te vergroten. Het kan zowel om technische hulpmiddelen als om aanvalsmethoden gaan. Het jaarlijks aantal publiek gemaakte exploits daalt. Mogelijk wordt het lastiger goede exploits voor kwetsbaarheden te ontwikkelen en is er een verband met de stijgende prijzen voor zero-day exploits. Er is een groeiende (grijze en zwarte) markt voor exploits, waarin ieder jaar meer geld omgaat. Het is onduidelijk of er simpelweg minder exploits zijn, of dat het aantrekkelijker is geworden om exploits te commercialiseren.

Hoeveelheid malware blij□ stijgen De hoeveelheid malware blijft ieder jaar hard stijgen. Het betreft vaak varianten op bestaande malware. Deze varianten kennen slechts een kort bestaan. Dit roept steeds meer de vraag op of traditionele antivirusproducten op basis van signature-herkenning nog wel effectief zijn, of dat er daarnaast moet worden ingezet op andere vormen van bescherming tegen malware.

Hulpmiddelen complexer en winstgevender Botnets worden steeds beter verhuld en verdedigd en kunnen dus ingezet worden bij meer en zwaardere DDoS-aanvallen. Mobiele malware neemt wereldwijd aanzienlijk toe, maar tot op heden zijn grootschalige besmettingen in Nederland nog niet vastgesteld. Gerichte spearphishing draagt bij aan de toename van deze besmettingen. Ransomware is steeds innovatiever en agressiever. In Nederland zijn veel ransomware-besmettingen en nog maar weinig cryptoware-besmettingen bekend. De opkomst van varianten waar betalen lijkt te helpen is zorgelijk omdat daarmee een innovatief en lucratief business model lijkt te ontstaan.

Professionalisering criminele dienstensector Hulpmiddelen om kwetsbaarheden te benutten worden professioneler, uitgebreider en eenvoudiger om toe te passen. Door de ontwikkeling van cybercrime-as-a-service neemt de beschikbaarheid van deze hoogwaardige aanvalsmiddelen toe, ook voor technisch minder onderlegde gebruikers. Op die manier wordt het steeds eenvoudiger om aanzienlijke schade toe te brengen.

**FritzBox**
In februari 2014 bleken verschillende Nederlandse internetgebruikers de dupe te zijn geworden van telefoniefraude. Bij deze gebruikers werd, zonder dat ze het zelf wisten, gebeld naar dure buitenlandse telefoonnummers, waarna zij met hoge rekeningen werden geconfronteerd. Dit bleek mogelijk door een kwetsbaarheid in de FritzBox-modem die zij gebruikten. Dit voorbeeld illustreert de kwetsbaarheid van apparaten die verbonden zijn met internet. In dit geval was het mogelijk de modems te patchen, waarmee de kwetsbaarheid werd verholpen.

## Weerbaarheid: kwetsbaarheden

Kwetsbaarheden blijven achilleshiel De kwetsbaarheid van software en systemen blijft onverminderd groot. Dit is de technische achilleshiel voor het waarborgen van cybersecurity. Er is nog onvoldoende antwoord op dit probleem. De mate waarin systemen kwetsbaar zijn is afhankelijk van de wijze waarop de gebruikte software tot stand is gekomen. De omvang van het probleem kan worden teruggedrongen, bijvoorbeeld door aandacht te besteden aan concepten als security-by-design.

Risico voor veiligheid door gebrek ICT-duurzaamheid De ontwikkeling dat steeds meer apparatuur (waaronder medische apparatuur, voertuigen, televisies en huishoudelijke apparaten) aan internet verbonden is, zal doorzetten. De software in deze apparatuur zal altijd beveiligingslekken bevatten. Veel apparatuur kan niet eenvoudig worden geüpdatet. Ook zal niet alle software gedurende langere tijd door de leverancier (kunnen) worden onderhouden. De apparatuur wordt kwetsbaar, waardoor een potentieel probleem ontstaat met het waarborgen van de maatschappelijke veiligheid. Dit is een gebrek aan duurzaamheid van ICT. De kwetsbaarheden die het afgelopen jaar in OpenSSL en Java zijn ontdekt, zijn hiervoor illustratief. Updaten van alle apparatuur blijkt problematisch.

## Weerbaarheid: maatregelen

Weerbaarheidsinitiatieven in uitvoering, implementatie blijft complex Maatregelen hebben tot doel de digitale weerbaarheid van individuen, organisaties en de samenleving te versterken. Veel weerbaarheidsinitiatieven die in de vorige editie van het CSBN werden genoemd, zijn inmiddels gestart of al in volle uitvoering. Denk hierbij aan het Nationaal Respons Netwerk, een publiek-privaat samenwerkingsverband met als doel de weerbaarheid van onze samenleving te versterken door gezamenlijke respons op cybersecurity-incidenten. Het afgelopen jaar is de aandacht voor cybersecurity opnieuw toegenomen, vaak door incidenten of nieuw ontdekte, ernstige kwetsbaarheden. Overheid en bedrijfsleven besteden meer aandacht aan maatregelen en pakken dit steeds vaker in gezamenlijkheid op. Voor thuisgebruikers blijft het lastig om zich adequaat tegen bestaande en nieuwe dreigingen te beveiligen.

Toenemend bewustzijn en nieuwe initiatieven Cybersecurity wordt steeds meer bezien binnen de bredere context van veiligheid, vrijheid en maatschappelijke groei. Het – mede door uitgebreide aandacht in reguliere media – toegenomen bewustzijn resulteerde de afgelopen periode in nieuwe initiatieven en aanvullende maatregelen, op nationaal niveau én bij afzonderlijke organisaties. Voorbeelden hiervan zijn samenwerking in nationale netwerken, inrichting van technische maatregelen om DDoS-aanvallen tegen te gaan en gebruik van veiliger standaarden en oplossingen op organisatorisch niveau. Ook wordt steeds meer aandacht besteed aan de noodzaak om de eindgebruiker voldoende toe te rusten op verantwoord gebruik van internet en zijn apparatuur.

## Manifestaties

Een manifestatie is een daadwerkelijke aantasting van cybersecurity. In de periode april 2013 tot en met maart 2014 vielen onderstaande zaken op.

Manifestaties zijn grensoverschrijdend De impact van cyberaanvallen stopt niet bij de landsgrenzen. Dit geldt bijvoorbeeld voor de verspreiding van malware (waaronder ransomware). Van sommige manifestaties die impact hebben gehad in het buitenland, is het voorstelbaar dat ze ook in Nederland plaats (zullen) vinden. In andere gevallen, zoals bij mobiele malware, lijkt de dreiging wereldwijd juist toe te nemen, terwijl er in Nederland nog weinig wordt opgemerkt. Het gebruik van malware komt overigens bij veel verschillende manifestaties terug en kan dan ook worden ingezet om informatie te achterhalen of om systemen te verstoren.

Grote datadiefstallen en datalekken In de afgelopen rapportageperiode vonden opvallend veel grote datadiefstallen en datalekken plaats. Vaak werden hier botnets voor ingezet, maar actoren gingen ook gerichter te werk en maakten gebruik van specifieke kwetsbaarheden om zich toegang tot informatie te verschaffen. Misbruik van, maar ook door interne medewerkers of ondernemers is een zeer reële dreiging geworden.

Impact natuurlijke gebeurenissen en menselijk fouten Ook technische en natuurlijke gebeurtenissen en menselijke fouten leiden tot manifestaties. Verstoringen en uitval van ICT en het lekken van gegevens zijn helaas niet te voorkomen, ook niet wanneer zorgvuldig en professioneel wordt gehandeld en er aandacht is voor preventieve maatregelen.

Substantiele stijging incidentmeldingen Het NCSC handelde in de periode van dit CSBN beduidend meer incidentenmeldingen af dan in het vorige CSBN. Denk hierbij aan hulpverzoeken en notice-and-takedowns. Het NCSC verwerkt per kwartaal steeds meer incidentmeldingen. Exclusief de geautomatiseerde controles is het aantal in de rapportageperiode van dit CSBN opgelopen van 89 in het tweede kwartaal van 2013 tot 163 in het eerste kwartaal van 2014. Opvallend is dat het aandeel incidentenmeldingen uit de private sector langzaam begint toe te nemen. Terwijl in de periode van het CSBN-3 37 procent van alle incidentmeldingen betrekking had op de private sector, is dit in de periode van dit CSBN gegroeid naar 46 procent van alle meldingen. «

**Heartbleed**
De Heartbleed-kwetsbaarheid is een voorbeeld waarmee de ICT duurzaamheidsproblematiek zichtbaar wordt gemaakt. Deze kwetsbaarheid zat al jaren in de OpenSSL-library. Deze software draait op bijna alle aan internet gekoppelde apparaten, zoals webservers en smartphones, maar ook smart-tv's en industriële apparatuur. Het updaten van alle apparatuur is problematisch, waardoor een deel van de apparatuur kwetsbaar blijft. Hiervan kan misbruik worden gemaakt met mogelijk ernstige gevolgen voor de maatschappelijke veiligheid.

# INLEIDING

**“Grootste DDoS-aanval ooit uitgevoerd in Europa”, “Zeer geavanceerde malware richt zich op overheden”, “Ruim 200 duizend slachto□ers van skimming of phishing”, “Hackers maakten naast creditcardgegevens ook pincodes buit”, “Criminelen dol op verspreiden malware via advertenties”. Dit zijn slechts enkele koppen van nieuwsberichten uit het afgelopen jaar. Het onderwerp cybersecurity is urgent en weet zich verzekerd van permanente aandacht.**

Het aantal toepassingen van ICT en internet neemt in Nederland nog altijd drastisch toe. Anno 2014 zijn de Nederlandse burger, de overheid en het bedrijfsleven meer dan ooit afhankelijk van ICT en internet. Het aantal apparaten (computers, telefoons, tablets, maar ook medische apparatuur, vervoermiddelen, enzovoort) dat gebruik maakt van internet neemt nog altijd toe, net als het aantal functies dat door (aan internet of met elkaar) verbonden apparaten wordt vervuld. Essentiële processen als identificatie, financiële transacties, klimaatregeling, rampenbestrijding, navigatie of verkeersbegeleiding zijn intussen ondenkbaar zonder hulp van (aan internet verbonden) ICT.

Als de afgelopen periode iets duidelijk heeft gemaakt, is het wel dat deze afhankelijkheid grote risico’s met zich mee brengt. Tot voor kort werden deze risico’s vooral gezien in termen van bescherming tegen digitale verstoring, maar ook grip op informatie wordt steeds belangrijker. Gebruik en misbruik van bijvoorbeeld persoonsgegevens of informatie over gedrag en interesses wordt een steeds belangrijker aspect van cybersecurity, en heeft dan ook een prominente plaats in deze rapportage.

Het Cybersecuritybeeld Nederland (CSBN) wordt jaarlijks door het Nationaal Cyber Security Centrum (NCSC) gepubliceerd en komt tot stand in nauwe samenwerking met een groot aantal partijen, zowel publieke (bijvoorbeeld politie, inlichtingen- en veiligheidsdiensten en het openbaar ministerie), wetenschappelijke, als private (vitale sectoren) partijen.

Het CSBN biedt inzicht in ontwikkelingen, belangen, dreigingen en weerbaarheid op het gebied van cybersecurity over de periode april 2013 tot en met maart 2014. Het is bedoeld voor beleidsmakers van de overheid en de vitale sectoren om de digitale weerbaarheid van Nederland te versterken of lopende cybersecurityprogramma’s te verbeteren.

In dit vierde Cybersecuritybeeld Nederland (CSBN-4) gelden opnieuw de onderstaande hoofdvragen:

- Welke Nederlandse belangen worden in welke mate geschaad door beperkingen van de beschikbaarheid en betrouwbaarheid van ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie en welke ontwikkelingen doen zich daarbij voor? (**belangen**)
- Welke gebeurtenissen of welke activiteiten van welke actoren kunnen ICT-belangen aantasten, welke hulpmiddelen gebruiken zij en welke ontwikkelingen doen zich daarbij voor? (**dreigingen**)
- In hoeverre is Nederland weerbaar tegen kwetsbaarheden in ICT, kunnen die leiden tot aantasting van ICT-belangen en welke ontwikkelingen doen zich daarbij voor? (**weerbaarheid**)

Verder wordt aandacht besteed aan de verschillende manieren waarop dreigingen zich manifesteren in de maatschappij en wordt een aantal onderwerpen verdiept, zoals de duurzaamheidsproblematiek van ICT.

In het afgelopen jaar heeft de Rijksoverheid een tweede editie van de Nationale Cyber Security Strategie gepubliceerd. In deze strategie wordt een afwegingskader geschetst tussen vrijheid, veiligheid en maatschappelijke groei. Dit vormt een referentiekader voor de geschetste ontwikkelingen en is een belangrijke toetssteen voor de verschillende belangen.

Dit CSBN bouwt voort op eerdere beelden en verwijst daar ook naar. Toch is het rapport een zelfstandig document. De rapportageperiode van het CSBN-4 loopt van april 2013 tot en met maart 2014. De focus ligt op de ontwikkelingen in Nederland, waarbij ook belangwekkende ontwikkelingen in het buitenland zijn meegenomen. Het CSBN is een feitelijke beschrijving met een duiding op basis van inzicht en expertise van overheidsdiensten en de vitale sectoren zelf. Het beschrijft ontwikkelingen in kwalitatieve vorm en geeft, daar waar in betrouwbare vorm beschikbaar, een kwantitatieve onderbouwing en/of een verwijzing naar bronnen. De totstandkoming is een continuproces met het CSBN als één van de jaarlijkse resultanten. Zaken die ten opzichte van de vorige edities niet of nauwelijks zijn veranderd, zijn niet of beknopt beschreven.

## Leeswijzer

Het CSBN-4 bestaat uit een kernbeeld en een aantal verdiepende katernen. In het kernbeeld staan de belangrijkste trends en verschuivingen in de rapportageperiode.

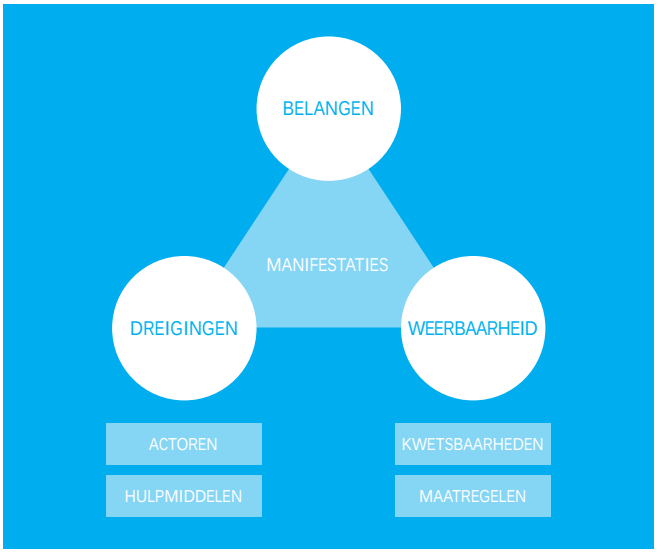
Bij **Belangen** (hoofdstuk 1) wordt ingegaan op de Nederlandse belangen. Hierbij wordt gekeken naar de manier waarop deze belangen geordend kunnen worden: individuele, organisatorische, keten- en maatschappelijke belangen.

De **Dreigingen** vallen uiteen in hoofdstukken over actoren en hulpmiddelen. De opzettelijke activiteiten van **actoren** en hun intenties worden in hoofdstuk 2 beschreven. De mate waarin die actoren over de intentie en vaardigheden beschikken om zich van technische en andere **hulpmiddelen** (hoofdstuk 3) te voorzien, bepaalt in hoge mate hun potentiële impact en de kans van slagen.

De **Weerbaarheid** van eindgebruikers, organisaties en de samenleving kan de kans dat een dreiging zich manifesteert en de impact ervan beperken. De weerbaarheid bestaat uit de af- of aanwezigheid van **kwetsbaarheden** bij mensen, organisaties of technologie (hoofdstuk 4) en **maatregelen** om weerstand en veerkracht te versterken en kwetsbaarheden te beperken (hoofdstuk 5).

In hoofdstuk 6 is beschreven welke zaken zich hebben **gemanifesteerd** binnen de driehoek belangen, dreigingen en weerbaarheid. Ook wordt in dit hoofdstuk een overzicht gegeven van de dreigingen die van de verschillende actoren uitgaan.

In de verdiepingskaternen is ruimte voor onderwerpen die speciale aandacht verdienen. Ofwel omdat er belangrijke nieuwe ontwikkelingen zijn te melden, ofwel omdat een trend uit de afgelopen jaren zo belangrijk is geworden dat deze speciale aandacht verdient. Op het gebied van belangen heeft de ontwikkeling in datagroei een steeds duidelijker impact, zowel positief als negatief. Dit onderwerp vindt een plaats in het verdiepingskatern **Mondiale datagroei**. In de verdiepingskaternen **Internet der Dingen** en **Duurzaamheid ICT** worden de kwetsbaarheden die samenhangen met integreren van internet in steeds meer apparaten, en de vragen die dit oproept over wenselijkheid en onderhoud hiervan, behandeld.




*Figuur 1. Samenhang belangen, dreigingen en weerbaarheid*

Het onderwerp **Digitale dreiging door statelijke actoren** verdient specifieke aandacht. Staten zijn immers al enige jaren de belangrijkste actoren die een bedreiging vormen voor Nederlandse belangen. In dit katern wordt ook specifiek aandacht besteed aan de inzichten vanuit de Nederlandse inlichtingen- en veiligheidsdiensten. Het hulpmiddel **Ransomware**, met als bijzondere variant **Cryptoware**, heeft in de afgelopen periode meer aandacht gekregen van opsporingsdiensten. Cryptoware is een agressieve en winstgevende variant en is aan populariteit aan het winnen onder beroepscriminelen. Steeds meer consumenten hebben last van deze vorm van diefstal.

In de **bijlagen** is een overzicht opgenomen van de door het NCSC afgehandelde incidenten, gebruikte afkortingen en een referentielijst. Dit jaar zijn voor het eerst met een aantal vitale sectoren analyses uitgevoerd met als doel een completer en beter gedifferentieerd cyberbeeld te krijgen. De resultaten van de sectoranalyses die het NCSC met medewerking van de Information Sharing and Analysis Centres (ISAC's) heeft uitgevoerd worden beschreven.

In dit kernbeeld wordt geprobeerd zo min mogelijk uitvoerige definities en technische terminologie te gebruiken, er is echter een **begrippenlijst** opgenomen met definities van veelgebruikte termen en afkortingen. «

# KERNBEELD

“SOMMIGE BELANGEN OVERSTIJGEN HET BELANG VAN HET INDIVIDU OF ORGANISATIE EN RAKEN DE NEDERLANDSE SAMENLEVING ALS GEHEEL”

# HOOFDSTUK 1 » BELANGEN

**De Nationale Cyber Security Strategie 2 omschrijft cybersecurity als volgt:**

*"Cybersecurity is het streven naar het voorkomen van schade door verstoring, uitval of misbruik van ICT en, indien er toch schade is ontstaan, het herstellen hiervan."*

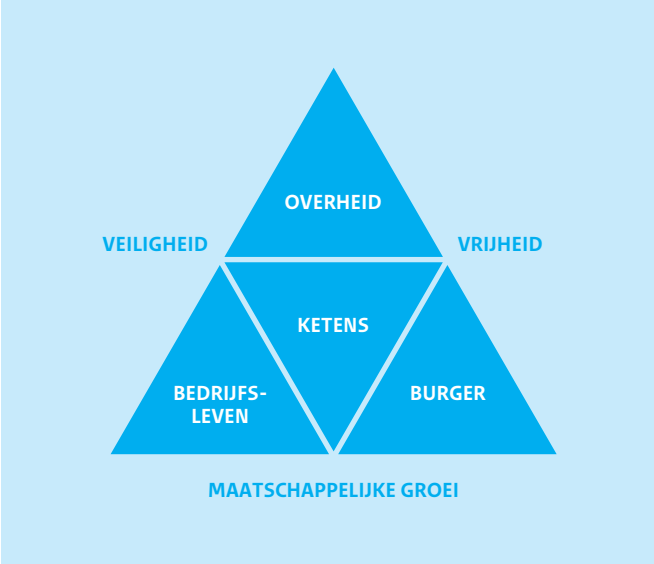
**Het voorkomen van schade is in het belang van de Nederlandse samenleving in het algemeen, maar ook in het belang van individuele burgers, bedrijven en overheidsorganisaties. Wanneer ICT niet (naar behoren) functioneert of informatie niet kan worden vertrouwd, raken belangen in de samenleving geschaad. Dit hoofdstuk gaat in op de relatie tussen cybersecurity en die belangen.**

## De noodzaak van cybersecurity[1]

Het cyberdomein is steeds meer verweven met ons dagelijks leven. Burgers, overheden en bedrijven gebruiken digitale toepassingen voor online interactie en transacties, efficiënter (samen)werken, communicatie en vermaak. De wereld digitaliseert steeds verder. Dit dient niet alleen gemak, efficiëntie en plezier, maar is ook een belangrijke drijfveer voor innovatie en economische groei. Uiteraard zijn aan deze verdergaande digitalisering ook risico's verbonden. Cybersecurity is er op gericht deze risico's te beheersen. Maatregelen in dit kader vergen maatwerk:

- door maatregelen toe te snijden op het probleem dat ze moeten oplossen (risicogebaseerd);
- door cybersecurity steeds in samenhang te bezien met maatschappelijke groei;
- door fundamentele rechten en waarden te waarborgen.

Deze samenhang tussen veiligheid, vrijheid en maatschappelijke groei is een dynamische balans.




*Figuur 2. Driehoek Veiligheid, Vrijheid en Maatschappelijke groei*

Veiligheid Cybersecurity gaat zowel over de veiligheid van ICT als over de veiligheid van de daarin opgeslagen informatie. Uitval van op ICT-gebaseerde diensten en processen kan grote maatschappelijke gevolgen hebben. Het waarborgen van de veiligheid is essentieel voor het vertrouwen in het cyberdomein.

Vrijheid In de transformatie van de samenleving naar een informatiemaatschappij heeft ICT een centrale rol gekregen. Hierdoor kunnen fundamentele waarden en rechten niet meer los gezien worden van de technische omgeving waarin deze tot uiting komen. Fundamentele rechten en waarden moeten dan ook in het cyberdomein gewaarborgd worden.

Maatschappelijke groei De ontwikkeling van ICT en de innoverende kracht die uitgaat van verdergaande digitalisering is een belangrijke stimulans voor groei.[2] De opkomst van ICT heeft hele nieuwe bedrijfssectoren in het leven geroepen.[3] Daarnaast heeft de innovatieve inzet van ICT in bestaande bedrijven een positieve invloed op productiviteit en concurrentiepositie – volgens het CBS is 60 procent van de economische groei in de periode 1985-2005 gekoppeld aan ICT.[4] Behalve economische groei gaat het ook om maatschappelijke groei. Digitalisering biedt aan de samenleving nieuwe mogelijkheden, bijvoorbeeld in de vorm van

1 Nationale Cyber Security Strategie 2, 26643-291 d.d. 28 oktober 2013

2 Online winkelen groeit met zo'n 10 procent per jaar, zie http://www.thuiswinkel.org/groei-online-winkelen (geraadpleegd 27 mei 2014)

3 Zie http://www.nederlandict.nl/Files/TER/ICT_en_TOPSECTOREN_ICT_als_Innovatie_As.pdf

4 Zie http://www.rijksoverheid.nl/onderwerpen/ict/ict-en-economie


onderwijstoepassingen,[5] mogelijkheden tot het onderhouden van sociale contacten en verbeterde overheidsvoorzieningen.

## Verschillende vormen van belangen

De toenemende digitalisering van onze samenleving is voor bijna iedereen merkbaar. Aantasting van de ICT-veiligheid kan daardoor een steeds grotere impact hebben op de belangen van die samenleving. We onderscheiden op het gebied van cybersecurity vier soorten belangen:

Vanuit cybersecurity moet rekening worden gehouden met elk van deze belangen. Deze belangen zullen voor eenieder een ander gewicht hebben en kunnen tegenstrijdig zijn.

Individuele belangen Dit zijn onderwerpen die (individuele) personen van belang achten en beschermen. Denk hierbij aan grondrechten als privacy, vrijheid van meningsuiting, veiligheid van digitale identiteit en de toegang tot onlinedienstverlening. Burgers willen steeds meer zaken online zelf regelen. De groei van het aantal klantportalen laat dit ook zien.

Organisatorische belangen Organisatorische belangen zijn belangen waarvan een organisatie voor het bereiken van haar doelstellingen of zelfs haar voortbestaan afhankelijk is. Een door een DDoS-aanval getroffen organisatie heeft niet alleen bij haar werkzaamheden last van een verstoring in het betalingsverkeer, maar kan hierdoor ook financiële en reputatieschade lijden. Over een langere periode kan dit ernstige gevolgen hebben voor de continuïteit van de onderneming. Daarnaast beschikken veel organisaties over eigendommen die interessant kunnen zijn voor buitenstaanders, zoals geld, klantgegevens, intellectueel eigendom of onderzoeksgegevens. De beveiliging van klant- en persoonsgegevens wordt in vitale sectoren dan ook een steeds belangrijker thema, zeker nu steeds meer informatie in 'Customer Self Care'-portalen opgeslagen en aangepast kan worden (zie bijlage 2).

Ketenbelangen Belangen beperken zich niet tot individuele organisaties. Er zijn ook organisatie-overstijgende belangen, zoals:
» de verantwoordelijkheid voor informatie van burgers of klanten en leveranciers;
» de beschikbaarheid van digitale diensten;
» het belang van basisvoorzieningen, zoals die voor online betalen.

Het belang van een keten komt in het geding wanneer cyberaanvallen belangen van derden raken. Bijvoorbeeld wanneer persoonsgegevens worden gelekt of wanneer onlinediensten, waarvan andere organisaties afhankelijk zijn, niet meer beschikbaar zijn. Ten tijde van de DDoS-aanvallen op de DigiD-infrastructuur in augustus 2013 was toegang tot de persoonlijke omgeving op de site van zorgverzekeraars grotendeels niet mogelijk. De vitale sectoren hebben specifiek aangegeven veel belang te hechten aan ketenintegratie en het waarborgen van cybersecurity in ketens van informatiesystemen (zie bijlage 2). Ook fysieke productieketens zijn in veel sectoren verweven. Het aanbod van 'veilige' IT-oplossingen lijkt achter te blijven bij de vraag.

Maatschappelijke belangen Sommige belangen overstijgen het belang van het individu of organisatie en raken de Nederlandse samenleving als geheel. Denk aan de beschikbaarheid van vitale diensten zoals elektriciteit. Cyberaanvallen gericht tegen een bedrijf of sector kunnen uiteindelijk ook de maatschappij als geheel raken. Zo kan langdurige uitval van het betalingsverkeer of de elektriciteitsvoorziening het economisch belang van Nederland treffen en leiden tot maatschappelijke ontwrichting.

5 Zie bijvoorbeeld h□ps://www.coursera.org en h□ps://www.edx.org

## Ontwikkelingen

De ontwikkelingen zoals geschetst in voorgaande edities van het CSBN hebben nog steeds grote invloed op de belangen. Denk hierbij aan:

» het omvangrijk gebruik van sociale media en mobiele media;
» het toenemende gebruik van de cloud;
» de verder gaande hyperconnectiviteit (alle apparatuur is continu met elkaar en het internet verbonden).

Daarnaast zijn de onderstaande ontwikkelingen relevant voor de digitale veiligheid.

A□ankelijkheid blij□ toenemen De afhankelijkheid van ICT blijft toenemen. Deze conclusie, uit alle voorgaande edities van het CSBN, blijft gelden. De efficiency- en effectiviteitsverbeteringen die de intensievere inzet van ICT in het vooruitzicht stelt, blijven bedrijven en overheden uitnodigen om processen in te richten met nieuwe ICT-oplossingen. Ook eindgebruikers gebruiken in toenemende mate ICT-toepassingen in de contacten met hun omgeving. Zo stijgt het aantal smartphonegebruikers nog altijd.[6] Dat geldt ook voor het aantal diensten dat op dergelijke mobiele platforms wordt aangeboden.[7] Deze aandachtsgebieden hebben met elkaar gemeen dat zij steeds meer worden ingezet als middel om informatieverzameling en -uitwisseling mogelijk te maken. De aard van de technieken leent zich daarbij om steeds dieper door te dringen in de haarvaten van de samenleving.

> *"De impact van verstoringen en aanvallen neemt toe door de verdergaande digitalisering."*

Door deze ontwikkelingen neemt het belang van cybersecurity toe. Steeds vaker biedt het digitale kanaal de enige mogelijkheid tot informatie-uitwisseling. Hierdoor heeft tekortschietende beveiliging of robuustheid van de gekozen oplossing onmiddellijke effecten op de beschikbaarheid en betrouwbaarheid van de dienstverlening. Cyberaanvallen hebben een toenemende impact op het functioneren van en het vertrouwen in de infrastructuur waarop Nederland draait. De afgelopen periode hebben we een aantal ontwikkelingen gezien, die van invloed zijn op de belangen van individuen, organisaties en de maatschappij als geheel.

Ten slotte zien we dat de oorspronkelijke oplossingen, die naast de digitale oplossingen in stand werden gehouden, verouderd raken en worden afgebouwd. Vaak verdwijnen ze uit kostenoverwegingen. Het is te duur om een parallelle 'oude' structuur in stand te houden naast een nieuwe digitale oplossing. Ook zien steeds meer nieuwe digitale producten en processen het licht waarvoor nooit een analoog alternatief heeft bestaan. Het belang van cybersecurity neemt hiermee toe, doordat de potentiële schade van aanvallen steeds groter wordt.

Verdergaande ketena□ankelijkheid Een belangrijke ontwikkeling is de invloed van de voortgaande koppeling van voorheen losse stappen in informatieverwerkingsprocessen op de belangen van de betrokken actoren. Verdere organisatie in procesketens vergroot de ketenafhankelijkheid van deelnemende partijen. Als het belang van één van de partijen in het geding is, heeft dit onmiddellijk invloed op de overige partijen in de keten. Individuele- of organisatiebelangen groeien zo uit tot gedeelde belangen. Bij het beschermen van belangen moet dus ook rekening gehouden worden met de invloed van (het wegvallen van) andere schakels in de keten. De keten is immers zo sterk als de zwakste schakel. Een verstoring krijgt daarmee in potentie een grotere impact: het raken van de belangen van één deel van de keten kan consequenties hebben voor de keten als geheel (zie de sectorale analyse in bijlage 2).

Internet der Dingen Steeds meer apparaten verzamelen gegevens over hun omgeving, en wisselen deze gegevens onderling of via het internet uit. Gartner schat dat er in 2020 ruim 25 miljard apparaten verbonden zijn met het internet.[8] Dit concept, dat bekendstaat als het Internet der Dingen, biedt veel toepassingen om ons leven gemakkelijker, veiliger en vrijer te maken. In de komende jaren bevatten steeds meer huishoudelijke, medische en industriële apparaten allerlei sensoren. Met een internetverbinding wisselen ze voortdurend gegevens uit. De ontwikkeling staat nu nog in de kinderschoenen, maar heeft zeker impact op cybersecurity: apparaten die online zijn, lopen risico's en zijn in potentie kwetsbaar. In het verdiepingskatern Internet der Dingen wordt dit nader uitgewerkt.

Mondiale datagroei Steeds meer aspecten van ons dagelijks leven worden vastgelegd: een ontwikkeling die wordt aangeduid als dataficatie. De data-explosie en de daarop gebaseerde diensten hebben een positieve invloed op maatschappelijke groei. Nieuw ontwikkelde toepassingen hebben niet alleen grote economische effecten, maar brengen ook op sociaal-maatschappelijk gebied een verandering teweeg. De toegenomen analysemogelijkheden van de steeds grotere hoeveelheid beschikbare informatie kunnen ten behoeve van de veiligheid worden ingezet.

6 In 2013 nog 30 procent, zie h□p://www.telecompaper.com/nieuws/smartphonemarkt-groeit-met-bijna-30-procent-in-q1--1011185 (geraadpleegd 1 mei 2014).
7 In 2013 waren er 1,5 miljoen apps beschikbaar voor Apple en Android, h□p://www.□urry.com/bid/103601/Mobile-Use-Grows-115-in-2013-Propelled-by-Messaging-Apps (geraadpleegd 11 juni 2014). Het gebruik van apps neemt nog altijd □ink toe.
8 h□p://www.gartner.com/newsroom/id/2684915 (geraadpleegd op 11 juni 2014)

Aan de andere kant brengt de dataexplosie ook risico's met zich mee. De schade en potentiële impact die ontstaat door verstoring, uitval of misbruik van deze informatie is veel groter dan voorheen. Het is zeer waarschijnlijk dat allerlei partijen de trends van datificatie en dataverzameling de komende jaren zullen doorzetten. Dit leidt enerzijds tot maatschappelijke vooruitgang en meer mogelijkheden op veiligheidsgebied. Aan de andere kant brengt dit risico's met zich mee voor het individuele privacybelang en het belang van vertrouwelijkheid van informatie voor private organisaties en overheden.

Afgelopen jaar bleek uit mondiale cases dat deze risico's reëel zijn en dat de belangen geschaad kunnen worden. Het verlies van grip op informatie, een risico dat vorig jaar al in het CSBN is geconstateerd, is een reële dreiging. In de media en maatschappij is het afgelopen jaar veel aandacht geweest voor activiteiten van inlichtingendiensten. Die inlichtingendiensten achten de dreiging vanuit niet-bondgenoten echter aanwezig en toenemend. Ook commerciële partijen nemen een steeds centralere rol in binnen de informatie-infrastructuur van individuen, bedrijven en overheden. Dit brengt risico´s met zich mee, vanwege de afhankelijkheid van deze bedrijven en de grote hoeveelheid data. Het vergroten van de weerbaarheid blijkt problematisch omdat eindgebruiker nauwelijks gerichte maatregelen kunnen treffen tegen de aanwezige kwetsbaarheden. In het verdiepingskatern Mondiale datagroei in context wordt dit nader uitgewerkt.

> *"De data-explosie en de daarop gebaseerde diensten hebben een positieve invloed op maatschappelijke groei."*

## Conclusie

Belangen in het kader van cybersecurity kennen verschillende niveaus:

- persoonlijke belangen;
- organisatiebelangen;
- ketenbelangen;
- maatschappelijke belangen.

Cybersecurity vereist bescherming van al die belangen. De belangen zullen altijd moeten worden beschouwd in onderlinge samenhang en worden bezien in de cybersecurity-driehoek van veiligheid, vrijheid en maatschappelijke groei.

Evenals in voorgaande jaren neemt de afhankelijkheid van ICT toe. Het gevolg daarvan is dat het niet-functioneren van ICT of inbreuk op de vertrouwelijkheid en de integriteit van informatie steeds meer impact heeft op het leven van mensen, het functioneren van Nederlandse organisaties en de continuïteit van de maatschappij. Deze toenemende afhankelijkheid is in versterkte mate van toepassing op de vitale sectoren. Cyberaanvallen en cyberverstoringen hebben in potentie grote impact op de persoonlijke en maatschappelijke veiligheid.

De ontwikkelingen die bekend staan als *Internet der Dingen* (het fenomeen dat steeds meer apparaten gegevens verzamelen over hun omgeving en deze gegevens onderling of via het internet uitwisselen) hebben enerzijds een positieve invloed, maar brengen anderzijds ook grote uitdagingen op het gebied van cybersecurity met zich mee. Mensen gaan inventief om met de hierbij verzamelde gegevens en willen deze voor andere doeleinden gebruiken dan waar ze oorspronkelijk voor dienen. Hiermee ontstaan uitdagingen op het gebied van beveiliging en privacy. «

“RELATIEF VEEL CYBERCRIMINALITEIT IS AFKOMSTIG UIT LANDEN WAAR DE AUTORITEITEN ER BEPERKT TEGEN OPTREDEN”

# HOOFDSTUK 2 » DREIGINGEN: ACTOREN

**Dit hoofdstuk gaat in op actoren die de betrouwbaarheid en de beveiliging van informatie(systemen) aantasten, hun intenties, de doelwi□en waarop zij zich richten en de vaardigheden waarover zij beschikken. De grootste dreiging voor overheid en bedrijfsleven gaat uit van statelijke actoren en criminelen. Door het aanbod van hulpmiddelen komen grotere en complexere cyberaanvallen binnen het bereik van meer partijen.**

## Staten

De AIVD en MIVD hebben vastgesteld dat de dreiging van digitale spionage door statelijke actoren tussen april 2013 en maart 2014 onverminderd groot was. Het aantal digitale spionageaanvallen nam toe, net als de complexiteit en impact. In Nederland zijn overheidsinstellingen, de defensie-industrie en bedrijven binnen topsectoren het slachtoffer. Daarnaast misbruiken statelijke actoren de Nederlandse ICT-infrastructuur op grote schaal voor digitale aanvallen op andere landen. Bijna elke buitenlandse inlichtingendienst heeft de afgelopen jaren geïnvesteerd in digitale capaciteiten. Hierdoor is digitale spionage niet langer voorbehouden aan grote en geavanceerde inlichtingendiensten.[1]

Als het gaat om schending van de vertrouwelijkheid en integriteit van informatie(systemen), dan waren gedurende de rapportageperiode de 'onthullingen' van Edward Snowden in het nieuws. Vanaf juni 2013 verschenen onthullingen over de activiteiten van de Amerikaanse Nationale Security Agency (NSA) in de wereldpers op basis van informatie gelekt door de voormalige werknemer van die dienst Edward Snowden. De aandacht in media werd gericht op vormen van data-exploitatie die normaliter minder in de schijnwerpers staan. In de media wordt de schaal van de activiteiten en de geavanceerde technische capaciteiten benadrukt.[2]

Diverse landen ontwikkelen het vermogen om offensieve digitale operaties uit te voeren en hebben militair optreden in het digitale domein opgenomen in hun militaire doctrines. Deze kunnen zij bijvoorbeeld inzetten tijdens conflicten met andere staten of oppositionele groepen. Hoewel er internationaal nog weinig precedenten zijn van de inzet van computer network attack (CNA) operaties,[3] kan de impact hiervan groot zijn.[4]

Staten kunnen ook diensten inhuren of producten kopen van anderen of opereren onder andermans vlag, bijvoorbeeld door zich voor te doen als hacktivisten.[5] Staten beschikken ten opzichte van andere actoren over relatief veel vaardigheden en middelen voor aanvallen gericht op informatie en ICT.[6] Hierdoor ontstaat een afhankelijkheid van de intenties van deze actoren en tevens een kwetsbaarheid voor de verandering van de intenties van deze actoren.

## Terroristen

Het beeld over cyberaanvallen door terroristen is ten opzichte van CSBN-3 niet veranderd. Het doel van terroristen is maatschappelijke veranderingen te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden. Terroristen beschikken (nog) niet over voldoende vaardigheden en middelen om daadwerkelijk maatschappijontwrichtende schade aan te richten. Jihadisten, een categorie terroristen waarvan een grote dreiging uitgaat, hebben in het buitenland en in Nederland wel kleinschalige en eenvoudige cyberaanvallen (defacements en DDoS-aanvallen) uitgevoerd. Wraak voor gepercipieerde islamvijandigheden lijkt een voornaam motief. Terroristen en zeker jihadisten benutten verder soms hackvaardigheden ter ondersteuning van hun activiteiten, bijvoorbeeld voor propaganda. De kennis die terroristen met dit type hackvaardigheden hebben opgedaan, kunnen zij in de toekomst benutten voor het uitvoeren van grotere of meer geavanceerde cyberaanvallen.

## Beroepscriminelen

Cybercriminaliteit wordt beter georganiseerd en de mogelijkheden van het internet worden vaker gebruikt om andere vormen van criminaliteit mogelijk te maken. De intentie van beroepscriminelen is het verdienen van geld. Dat kan op uiteenlopende manieren:

- Het zelf uitvoeren van aanvallen op informatie of ICT (bijvoorbeeld een DDoS-aanval) of afpersing door te dreigen met cyberaanvallen of een malwarebesmetting.
- Diensten aanbieden waarmee anderen aanvallen kunnen uitvoeren. In 2013 zijn deze markten in omvang, complexiteit en professionaliteit gegroeid. Wel dalen de prijzen van bijvoorbeeld de inzet van botnets en DDoS vanwege de vele andere opties die

1 Zie het verdiepingskatern Digitale dreiging door statelijke actoren.
2 Zie het verdiepingskatern Mondiale datagroei in context en vele artikelen van The Guardian, The New York Times en Der Spiegel. Ook Luke Harding, 'De Snowden Files', 2014.
3 CNA-operaties of o□ensieve cybercapaciteiten zijn digitale middelen die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Deze capaciteiten kunnen in een militaire operatie worden ingezet ter ondersteuning van conventionele militaire capaciteiten.
4 Zie het verdiepingskatern Digitale dreiging door statelijke actoren
5 'CrowdStrike global threat report 2013 year in review', Crowdstrike, 2014, 'Government spying tools will worsen Internet security: experts', Reuters, 3-3-2014 (h□p://www.reuters.com/assets/print?aid=USBREA2228K20140303), 'The digital arms trade. The market for so□ware that helps hackers penetrate computer systems', The Economist, 30 maart 2013.
6 Zie hoofdstuk 6 voor een toelichting op aanvallen gericht op informatie en ICT.

ook beschikbaar zijn. Daarnaast is de prijs voor nieuw ontdekte kwetsbaarheden is gestegen.[7]

» Handel in of dienstverlening voor gestolen informatie. De informatie die criminelen buitmaken door middel bijvoorbeeld botnets en malware heeft voor de aanvaller zelfstandige waarde. Die gebruikt hij bijvoorbeeld om fraude mee te plegen of om te verhandelen. Symantec stelt dat er een zeer professioneel team van hackers bestaat dat ingehuurd kan worden om aan informatie te komen.[8]

» De inzet van cyberaanvallen voor andere vormen van criminaliteit. In 2013 signaleerde de politie dat drugscriminelen diensten van hackers 'inhuurden'. Door manipulatie van systemen van twee grote containerterminals in de haven van Antwerpen konden de drugscriminelen de locaties en verplaatsingen van containers zelf aanpassen. Op die manier konden zij de container waarin de drugs waren verstopt eerder ophalen dan de geplande transporteur.[9]

Cybercriminelen zijn zich in de afgelopen periode meer gaan richten op misbruik van de infrastructuur van het internet in plaats van misbruik van individuele computers of sites.[10] De schaalvoordelen van het misbruiken van een dienstverlener zoals een hostingpartij, een domeinnaamserver[11] of populaire website, bieden bijvoorbeeld veel meer mogelijkheden dan een gecompromitteerde individuele website.

Het niveau van kennis en vaardigheden van cybercriminelen varieert sterk. Er zijn (groepen van) criminelen die beschikken over geavanceerde cybervaardigheden en professionele middelen. Op enig moment kunnen zij die vaardigheden tegen betaling aanbieden aan anderen. Daardoor kunnen ook minder ervaren of geëquipeerde criminelen (complexe) cyberaanvallen uitvoeren of daarmee dreigen.

Relatief veel cybercriminaliteit komt uit landen waar de autoriteiten er beperkt tegen optreden. Cybercriminelen kunnen de grensoverschrijdende mogelijkheden van het internet benutten en de autoriteiten ontlopen. Daarnaast zijn er dienstverleners actief, zoals hostingproviders, die criminelen bewust of onbewust anonimiteit en veiligheid garanderen. Ook de jurisdictieproblematiek bij de opslag van gegevens in de cloud is een extra uitdaging voor de opsporing en werkt in het voordeel van verdachten.

## Cybervandalen en scriptkiddies

Cybervandalen hebben veel kennis, ontwikkelen hun eigen hulpmiddelen of breiden die van anderen uit. Zij voeren hacks uit omdat het kan of om aan te tonen dat zij ertoe in staat zijn. Scriptkiddies zijn hackers met beperkte kennis. Zij maken gebruik van technieken en hulpmiddelen die anderen hebben ontwikkeld en die voor iedereen toegankelijk zijn. Vaak zijn het jongeren die zich nauwelijks bewust zijn van de gevolgen van hun handelen. Hun motieven zijn vaak baldadigheid en het zoeken van een uitdaging. De gevolgen van hun acties kunnen echter groot zijn. Er zijn geen aanwijzingen dat zich veranderingen hebben voorgedaan wat betreft het beeld van cybervandalen en scriptkiddies.

**Vier Nederlandse hackers maakten een miljoen euro buit**
Het OM meldde op 24 oktober 2013 dat vier Nederlandse hackers bankrekeningen hebben geplunderd en daarbij vermoedelijk een miljoen euro hebben buitgemaakt. Ze stuurden e-mails met een link naar malware. Zo werden computers van Nederlandse rekeninghouders geïnfecteerd, waardoor ze nieuwe betalingsopdrachten konden aanmaken of bestaande opdrachten konden wijzigen. Het geld boekten ze op rekeningen van zogeheten moneymules, mensen die hun bankrekening beschikbaar stelden voor het gestolen geld. Ook verstuurden ze tweets over actuele onderwerpen met daarin links naar hun malware.[12]

Het feit dat er een markt bestaat voor criminele cyberdienstverlening zorgt er samen met de ruime beschikbaarheid van kennis en tools voor dat cybervandalen en scriptkiddies over ruime mogelijkheden beschikken. Ondanks dat scriptkiddies geen bijzondere vaardigheden of middelen hebben, kunnen zij cyberaanvallen met een grote impact lanceren. Simpelweg omdat het uitvoeren van bepaalde cyberaanvallen zeer eenvoudig is. Denk bijvoorbeeld aan het uitvoeren van zogenaamde DNS-amplification-aanvallen.[13]

## Hacktivisten

Hacktivisten zijn mensen die met hun cyberaanvallen ideologische doelen willen realiseren of dichterbij willen brengen. De doelen variëren tussen en binnen groepen van hacktivisten en in de loop van de tijd. In het verleden hebben hacktivisten veelvuldig cyberaanvallen uitgevoerd als protest tegen maatregelen die in hun ogen de vrijheid van het internet aantasten. Ideologisch gemotiveerde cyberaanvallen zijn, ondanks specifieke claims, lastig toe te wijzen. Zo valt er soms weinig samenhang te ontdekken in claims. Ook beweren sommigen een actie uit naam van een groep, om die later weer te ontkennen. De trend dat hackerscollectieven zich opwerpen als verdedigers van de belangen van staten, heeft zich volgens de AIVD en MIVD het afgelopen jaar doorgezet. Het afgelopen jaar zijn geen aanvallen tegen Nederland waargenomen van dergelijke hackerscollectieven die belangen van staten behartigen.[14]

In zowel het buitenland als in Nederland doken regelmatig oproepen op tot cyberaanvallen. Lang niet alle oproepen tot cyberaanvallen resulteren in geslaagde aanvallen. In 2013 viel op dat menigmaal

7 'Internet Security Threat Report 2014', Symantec, 2014, 'Markets for Cybercrime Tools and Stolen Data. Hackers' Bazaar', Rand Corporation, 2014, "Cybercrime shopping list study points to falling prices', BBC news technology, 17 december 2013.
8 'Hidden Lynx – Professional Hackers for Hire', Symantec, September 17 2013 (h□p://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire en h□p://www.wired.com/images_blogs/threatlevel/2013/09/hidden_lynx_□nal.pdf).
9 'Cyber Security Perspectives 2013', KPN, Politie, NCSC, TNO, 2014, ''Hackers geven drugssmokkelaars vrij baan', NOS.nl, 17 juni 2013 (h□p://nos.nl/op3/artikel/519270-hackers-geven-drugssmokkelaars-vrij-baan.html).
10 'Cisco 2014 annual security report, CISCO, 2014.
11 Zie voor een uitgebreide beschrijving van kwetsbaarheden in protocollen zoals DNS ook H4 Kwetsbaarheden
12 'OM: Nederlandse hackers plunderden bankrekeningen', de Volkskrant, 24-10-2013.
13 Zie het hoofdstuk Hulpmiddelen
14 Katern Digitale dreiging door statelijke actoren.

accounts van nieuwsorganisaties werden overgenomen, bijvoorbeeld van Reuters, of websites zijn gedefacet, bijvoorbeeld van de BBC.[15] Er zijn geen cijfers voorhanden om te beoordelen of het aantal hacktivistische cyberaanvallen in 2013 is veranderd.

Vaardigheden van hacktivisten verschillen sterk binnen en tussen groepen en zijn afhankelijk van tal van factoren. Zo is in CSBN-3 aangegeven dat hacktivisten veelal in fluïde netwerken opereren die vaak open staan voor bijdragen van iedereen. Verder kunnen hackers tijdens een campagne spontaan hun kennis van kwetsbaarheden of eerder gestolen informatie aanbieden.

## Interne actoren

Interne actoren zijn individuen die (tijdelijk) in een organisatie aanwezig zijn of zijn geweest, zoals (ex-)medewerkers, inhuurkrachten en leveranciers. Een interne actor kan de betrouwbaarheid of beveiliging van informatie(systemen) aantasten. De intentie kan wraak zijn, bijvoorbeeld naar aanleiding van ontslag. Ook kan er sprake zijn van financiële of politieke motieven. Interne actoren kunnen op eigen initiatief handelen of door anderen worden benaderd of hiertoe worden aangezet, zoals door staten voor spionagedoeleinden. Daarbij hoeft het niet (altijd) te gaan om geavanceerde technieken. Een ingeplugde USB-stick met malware kan al voldoende zijn.

## Cyberonderzoekers

Cyberonderzoekers willen kwetsbaarheden in ICT-omgevingen vinden om de (te) zwakke beveiliging aan de kaak te stellen. Hun vaardigheden variëren. Zij gebruiken vaak de media om hun bevindingen te publiceren en de bewustwording over de noodzaak van cybersecurity te vergroten. Cyberonderzoekers hebben tijdens (internationale) hackersbijeenkomsten diverse malen gewezen op gevonden kwetsbaarheden. Dit soort publiciteit kan overheidsinstellingen en bedrijven (tijdelijk) extra kwetsbaar maken. Ook omdat kwaadwillenden kunnen profiteren van de onderzoeksbevindingen. In sommige gevallen verdenkt men de cyberonderzoeker zelf van strafbare feiten. Om dit te voorkomen, volgen sinds 2013 diverse publieke en private partijen de leidraad 'responsible disclosure'. Deze partijen ondernemen geen juridische stappen als de onderzoekers zich aan de leidraad houden (zie voor een uitgebreide toelichting bijlage 1).

## Private organisaties

Als private organisaties de vertrouwelijkheid van informatie(systemen) aantasten, doen zij dat meestal om geld te verdienen. Dat kan bijvoorbeeld door digitale diefstal van informatie over concurrenten. Private organisaties kunnen door het aanbieden van producten zoals apps of andere diensten veel gegevens verkrijgen van klanten. Die gegevens kunnen ze vervolgens zelf commercieel gebruiken of doorverkopen aan anderen.[16] De gebruiker heeft daarvoor overigens veelal wel (bewust of onbewust) toestemming gegeven. Toch kunnen gebruikers bij bedrijfsovernames of wijzigingen in gebruikersvoorwaarden voor verrassingen komen te staan. Dit komt doordat de gegevens opeens voor andere doeleinden of door andere partijen kunnen worden gebruikt. Zeker bij cloudtoepassingen is de gebruiker voor het waarborgen van de betrouwbaarheid in hoge mate afhankelijk van de leverancier. Hierdoor is een afhankelijkheid ontstaan van de intenties van deze actoren en tevens een kwetsbaarheid voor de verandering van de intenties.

**Melding aan KPN via responsible disclosure**

Een persoon onder het pseudoniem CrossWire vond in juni 2013 kwetsbaarheden in het KPN-netwerk. Hij kreeg via een nog actieve aansluiting in een leegstaand pand toegang tot een deel van de interne infrastructuur van KPN. Hij meldde dit aan het NCSC, dat het doorgaf aan KPN. Om de kwetsbaarheden te verhelpen, was CrossWire bereid samen te werken met KPN, waarvoor KPN hem dankbaar was.[17]

## Conclusie

Net als in het CSBN-3 luidt het oordeel dat de grootste dreiging voor overheid en bedrijfsleven uitgaat van statelijke actoren (vanwege de digitale spionageaanvallen) en van beroepscriminelen (vanwege de diverse vormen van cybercriminaliteit).

Criminele organisaties professionaliseren verder met de ontwikkeling van een zeer professionele criminele cyberdienstensector. 'Cybercrime-as-a-service' is geen incident meer, maar is onderdeel van de gevestigde structuur. Het aantasten van de betrouwbaarheid en beveiliging van informatie(systemen) komt hiermee binnen het bereik van meer partijen.

15 'How hacktivists have targeted major media outlets', Dark Reading, 21-8-2013, 'Syrian Electronic army no longer just Twi□er feed jackers... and that's bad news', The Register, 1-8-2013, 'Syrian Electronic Army: Hacktivists on the ba□le□eld', The Soufan Group, 19-9-2013..

16 Zie verder katern 'Mondiale Data-exploitatie in context'.

17 'Cyber Security Perspectives 2013', KPN, Politie, NCSC, TNO, 2014, 'Hacker had toegang tot deel KPN-infrastructuur', Security.nl, 18 november 2013 (h□ps://www.security.nl/posting/370041/Hacker+had+toegang+tot+deel+KPN-infrastructuur).

| Actor | Intentie | Vaardigheids-niveau | Doelwit |
|---|---|---|---|
| **Staten** | Voor contraterrorisme of bescherming Nationale Veiligheid<br>Geopolitieke of (interne) machtspositie verbeteren | Hoog | Overheidsinstellingen, defensie-industrie en bedrijven in topsectoren. Organisaties die springplank vormen om anderen te ‘targeten’ |
| **Terroristen** | Maatschappelijke veranderingen bewerkstelligen, bevolking ernstige vrees aanjagen of politieke besluitvor-ming beïnvloeden | Gemiddeld tot laag | Doelwi□en met hoge impact, ideologische symboolfunctie |
| **Beroepscriminelen** | Geldelijk gewin (direct of indirect) | Hoog tot gemiddeld | Producten en –dienstverlening met veel identiteits- of □nanciële gegevens<br>In beginsel iedereen waar op illegale wijze geld aan te verdienen is |
| **Cybervandalen en scriptkiddies** | Baldadigheid, zoeken van uitdaging | Laag | Uiteenlopend |
| **Hacktivisten** | Ideologische doelen dichterbij brengen | Gemiddeld | Nieuwsorganisaties. Gerelateerd aan ideolo-gisch doel dat wordt nagestreefd. Soms ook totaal willekeurig met als enige reden aanwezige kwetsbaarheden |
| **Interne actoren** | Wraak, geldelijk gewin of ideologisch (mogelijk ‘aangestuurd’) | Hoog tot laag | Huidige en/of voormalige werkomgeving |
| **Cyberonderzoekers** | Aantonen zwakheden, eigen pro□lering | Gemiddeld | Uiteenlopend |
| **Private organisaties** | Verkrijging of verkoop waardevolle informatie | Hoog tot laag | Concurrenten, burgers, klanten |

*Tabel 2. Actoren, intenties, vaardigheidsniveau en doelwi en*

“DE OPKOMST VAN CRYPTOWARE IS VERONTRUSTEND”

# HOOFDSTUK 3 » DREIGINGEN: HULPMIDDELEN

**In het vorige hoofdstuk is beschreven welke actoren digitale aanvallen uitvoeren en waarom. Zij maken hierbij gebruik van hulpmiddelen om kwetsbaarheden te misbruiken of te vergroten. Het kan zowel om technische hulpmiddelen als om aanvalsmethoden gaan. De malwaretrends uit 2012 hebben zich voortgezet in 2013. Op veel gebieden werden records gebroken. Ondanks een verdere daling van het aantal gepubliceerde exploits, stijgt de hoeveelheid nieuwe malware nog steeds explosief, ook in het mobiele domein. DDoS-aanvallen leveren steeds hogere bandbreedtes en de markt waarop deze hulpmiddelen worden verhandeld, wordt steeds professioneler.**

## Technische hulpmiddelen

Dalende hoeveelheid exploits, stijgende prijzen Na een duidelijke piek in 2010 is het aantal gepubliceerde exploits[18] de laatste jaren aan het afnemen. De gepubliceerde exploits richten zich nog steeds voornamelijk op Windows-platformen en webapplicaties. Een aanzienlijk deel van de geëxploiteerde kwetsbaarheden is gerelateerd aan Oracle Java en Adobe Reader en Adobe Flash.[19]

Een mogelijke verklaring voor de daling van het aantal exploits is dat het steeds lastiger en kostbaarder wordt om kwetsbaarheden effectief uit te buiten.

De daling in gepubliceerde exploits lijkt te leiden tot stijgende prijzen voor nieuwe zero-day exploits.[20] Dit op basis van het marktmechanisme dat bij een kleiner aanbod de prijzen omhoog gaan. Het kan ook zo zijn dat gestegen prijzen ertoe leiden dat geëxploiteerde kwetsbaarheden niet meer gepubliceerd worden, maar worden verkocht op de zwarte of grijze markt.[21]

De prijsstijging blijkt onder meer uit het prijzengeld van de jaarlijks door HP gehouden Pwn2Own hacking competitie. Daar proberen security-onderzoekers kwetsbaarheden in veelgebruikte software te misbruiken. Het beschikbare prijzengeld[22] is sinds de start in 2007 van 10.000 dollar verveelvoudigd tot meer dan een miljoen dollar.[23]

Het aantal beschikbare exploitkits is ook in de afgelopen periode verder gegroeid. Exploitkits maken gebruik van nog niet gepatchte kwetsbaarheden om malware op een te besmetten systeem te installeren.

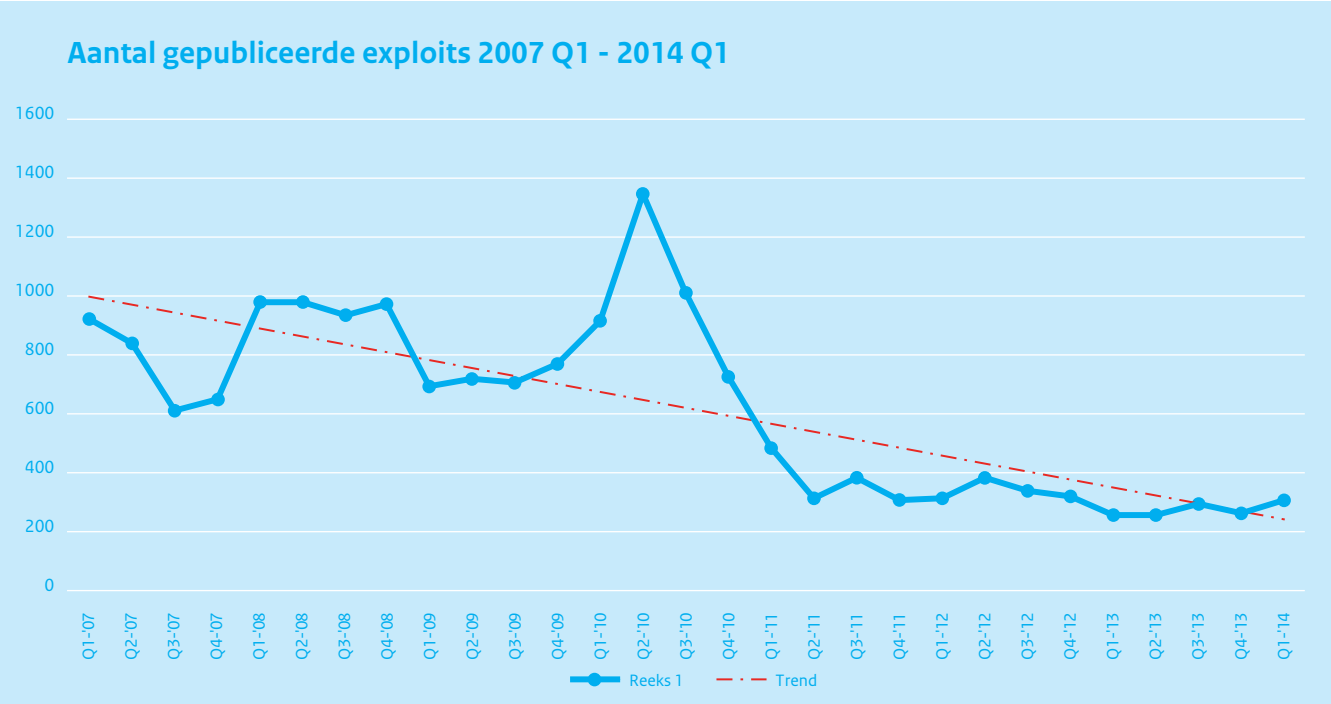
Na de arrestatie van de maker van de veelgebruikte Blackhole exploitkit in oktober 2013 nam het aantal Blackhole-besmettingen in korte tijd snel af, doordat updates (exploits van nieuwe kwetsbaarheden) uitbleven. Andere exploitkits als Angler, Styx en Nuclear wisten het gat in de markt echter snel op te vullen.[24]

Malware groeit en professionaliseert Ondanks een daling van het aantal gepubliceerde exploits, is de hoeveelheid nieuwe malware in 2013 explosief gestegen (zie figuur 5). Het merendeel hiervan is bestaande malware die is aangepast om detectie door antivirus-pakketten te ontlopen. Het merendeel van de malware (meer dan 75 procent) bestaat uit Trojans.[25]

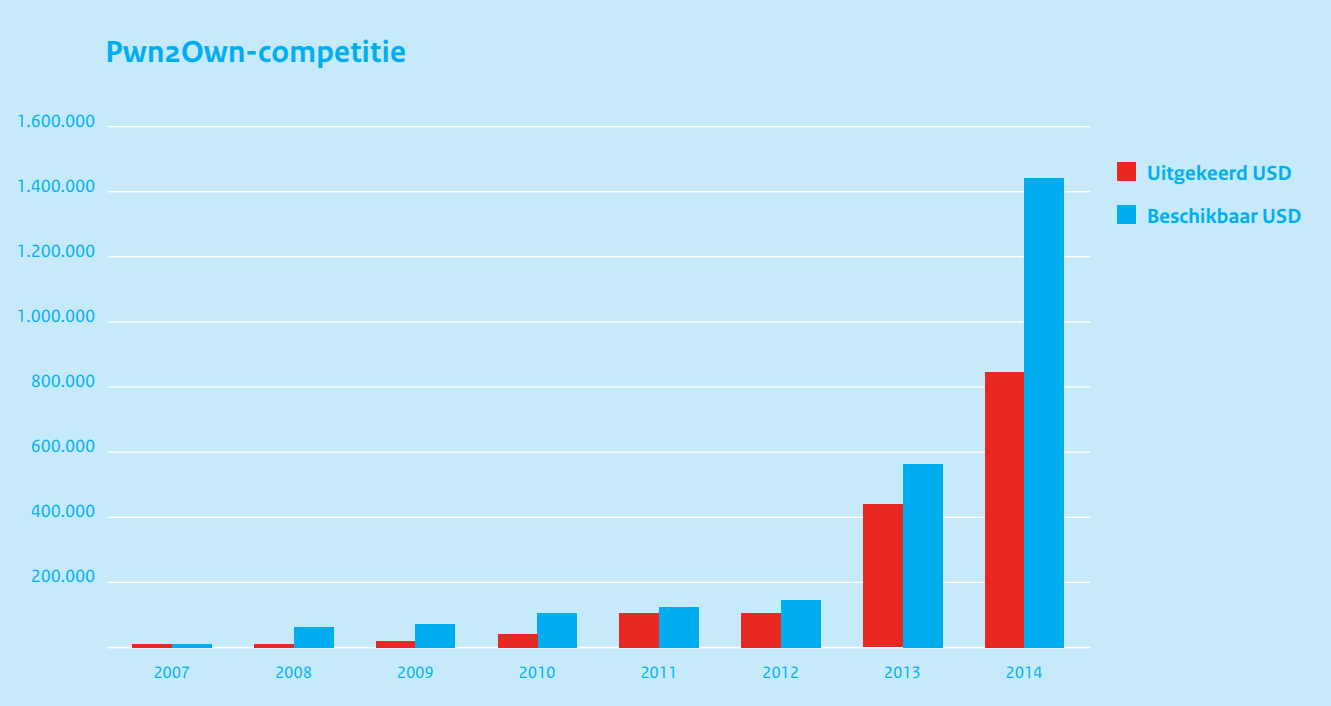
Figuur 6 verduidelijkt de relatie tussen kwetsbaarheden, exploits en malware.

Software kan meerdere kwetsbaarheden bevatten. Een kwetsbaarheid kan ook van toepassing zijn op verschillende softwareproducten. Exploits worden geschreven om één of enkele van deze kwetsbaarheden uit te buiten. Malware wordt op basis van één of meerdere exploits geschreven om het doel van de kwaadwillende gebruiker te bewerkstelligen. Een specifieke exploit kan dus in vele stukken malware terugkomen.

18 So□ware die gebruik maakt van kwetsbaarheid – zie ook voor verdere toelichting op terminologie de Begrippenlijst.
19 h□p://www.av-test.org/en/news/news-single-view/adobe-java-make-windows-insecure/
20 Exploit die misbruik maakt van een kwetsbaarheid waarvoor nog geen patch bestaat.
21 Zie paragraaf Marktwerking.
22 Prijzengeld is het bedrag dat sponsors (ZDI, Google etc.) betalen voor het kopen van de gebruikte zero day exploits.
23 h□p://www.pwn2own.com/2014/03/pwn2own-2014-recap/
24 F-Secure H2 2013 Threat Report
25 Malware die zich installeert op een device en bijvoorbeeld informatie verzamelt of aansluiting op een botnet tot stand brengt.

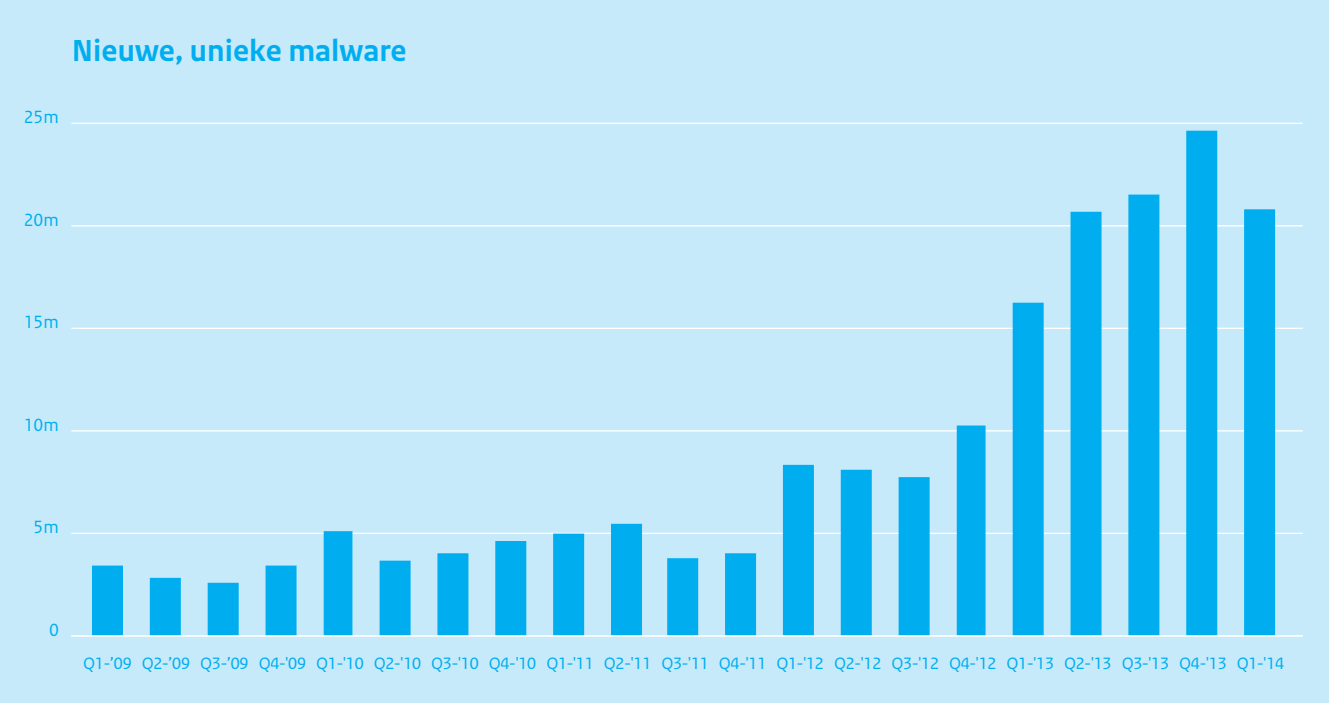



*Figuur 3. Aantal gepubliceerde exploits*[26]

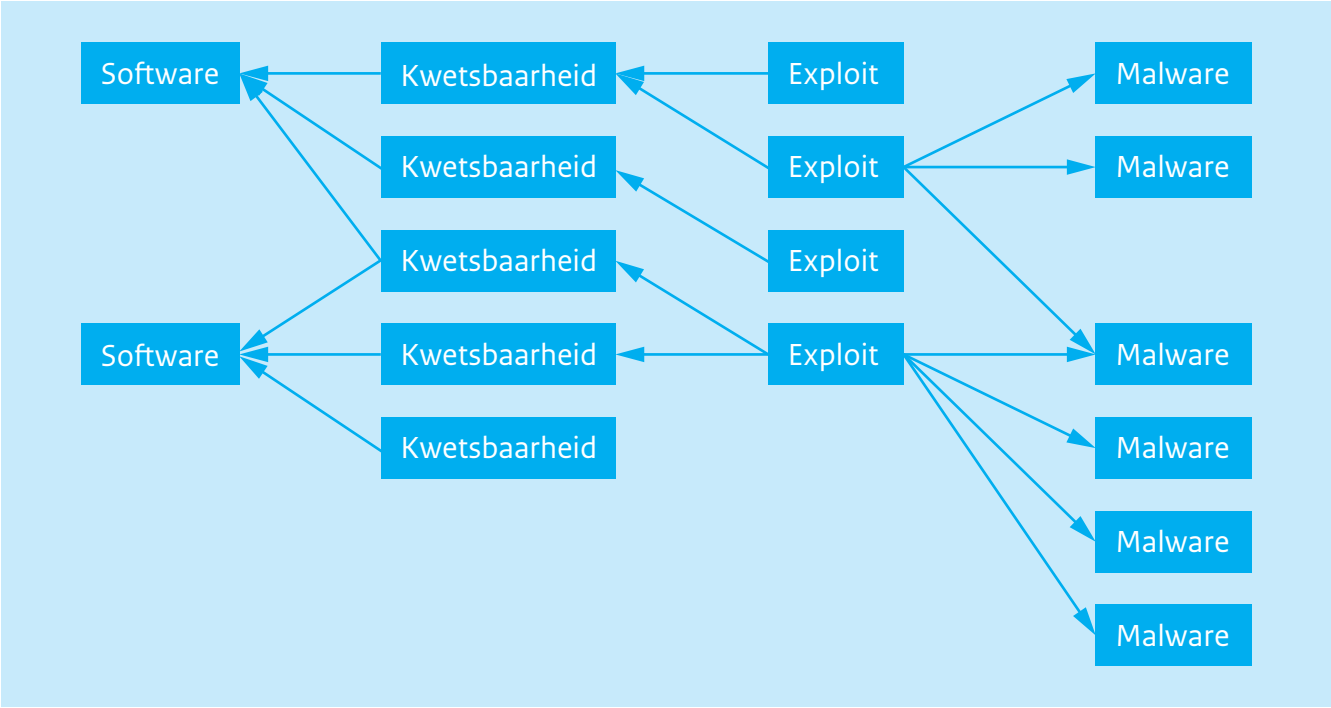



*Figuur 4. Prijzengeld Pwn2Own*[27]

26 Bron: h□p://exploit-db.com
27 Bron: www.cansecwest.com




*Figuur 5. Nieuwe malware*[11]




*Figuur 6. Het gebruik van so warekwetsbaarheden door malware, met behulp van exploits*

28 Bron: AV-test Institute.

Steeds vaker wordt malware opgelopen door slechts het bezoeken van een geïnfecteerde legitieme website. Installatie van de malware vindt voor de bezoeker onzichtbaar plaats, zonder dat deze hiervoor nog actief een download moet accepteren.

Makers van malware proberen hun malware normaliter blijvend op een systeem achter te laten door besmette bestanden weg te schrijven. In 2013 is echter ook vluchtige malware ontdekt,[29] die zich alleen in het werkgeheugen van de computer nestelt. Deze malware verdwijnt bij het herstarten van de computer. Vluchtige malware is hierdoor veel lastiger te ontdekken en te bestrijden dan traditionele malware. Ook maken makers van malware gebruik van zogenaamde online crypter services om malware te laten vercijferen en een nieuwe versie van deze malware te (laten) creëren. Zo zorgen zij ervoor dat deze malware niet door antivirussoftware wordt gedetecteerd.

Verder zijn er in de afgelopen periode geregeld malware-aanvallen geweest die specifiek waren gericht op buitenlandse kassasystemen (point-of- sale- attacks). Voor Nederland is dit vanwege de marktpenetratie van het pinnen minder relevant.

Professionalisering van cybercriminaliteit leidt tot een professionelere ontwikkeling van gebruikte hulpmiddelen. Criminele organisaties zetten professionele ontwikkelteams in om malware te ontwikkelen en aan te passen voor gerichte doelwitten. Ook overheden maken steeds meer gebruik van professioneel en op maat ontwikkelde tools voor cyberspionage[30] of bestrijding van cybercriminaliteit.

Het gebruik van dergelijke middelen is niet voorbehouden aan degenen die de tools ontwikkelen; iedereen kan betrekkelijk eenvoudig geavanceerde malware verkrijgen. Er is niet langer diepgaande kennis van de benodigde techniek nodig om succesvol cyberaanvallen te kunnen uitvoeren. Het aantal potentiële gebruikers dat relatief eenvoudig aanzienlijke schade kan toebrengen, stijgt zo aanzienlijk.

Botnets lastiger te detecteren en te herstellen Botnets worden nog altijd ingezet voor de verspreiding van spam, het uitvoeren van DDoS-aanvallen, klikfraude en keylogging maar tegenwoordig ook voor het verspreiden van ransomware[31] of het minen van cryptocurrencies.[32] In absolute zin lijkt het aantal botnets gedurende de rapportageperiode te zijn gedaald, maar dit zegt weinig over de effectiviteit ervan.[33]

Beheerders van botnets maken steeds meer gebruik van defensieve maatregelen om hun botnet in stand te houden. Criminelen misbruiken bijvoorbeeld het TOR-netwerk om botnets en C&C-servers aan het oog te onttrekken.

Daarnaast wordt er meer intelligentie in de malware gestopt. Hierdoor kunnen geïnfecteerde clients bijvoorbeeld zelf contact zoeken met nieuwe C&C-servers, wanneer het originele C&C-netwerk is ontmanteld.

Meer en zwaardere DDoS-aanvallen Nadat het in 2011 en 2012 relatief rustig was op het gebied van DDoS-aanvallen, keerde de DDoS in 2013 met ongekende hevigheid terug. In april en mei 2013 lagen zowel de grootste Nederlandse banken als de overheid langere tijd onder vuur van deze aanvallen.

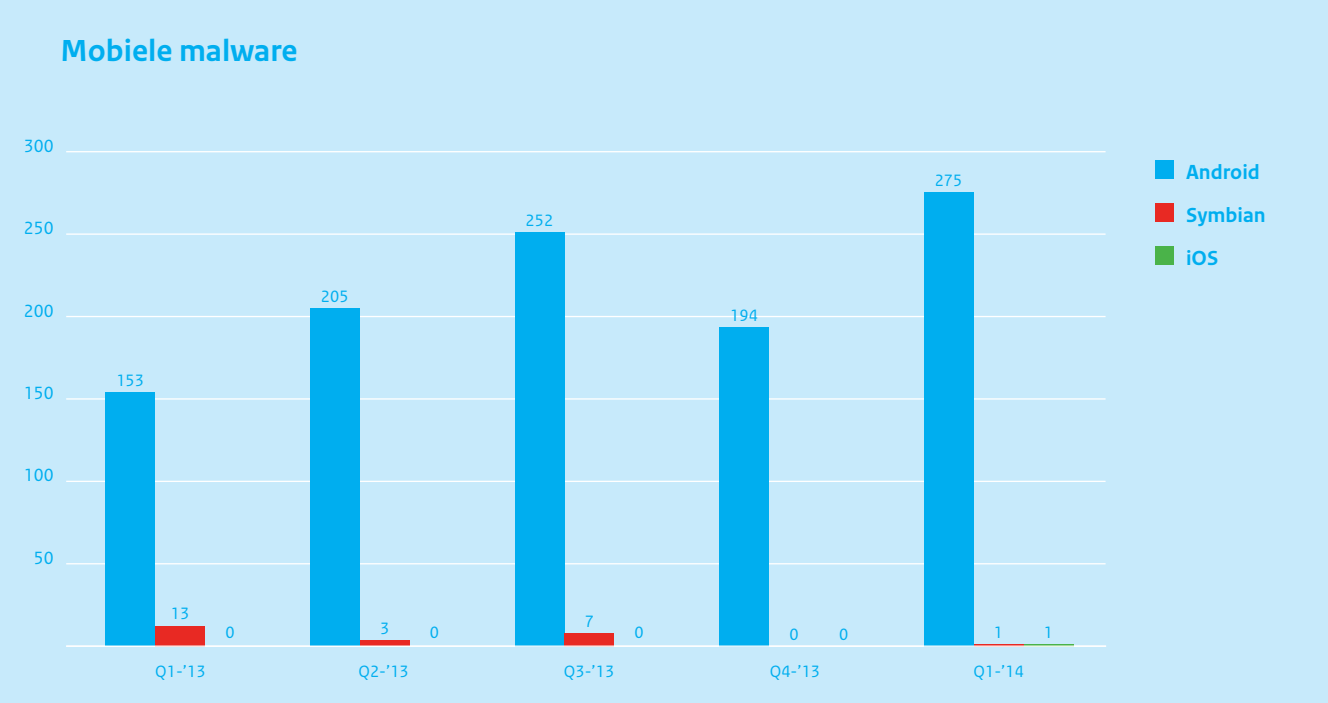
Het is steeds eenvoudiger geworden om een DDoS-aanval uit te voeren, ook voor technisch minder onderlegde cybercriminelen. Eenvoudige hulpmiddelen zijn breed beschikbaar gekomen en botnets kunnen via zwarte markten worden ingehuurd. Hierdoor is het goed mogelijk om al tegen lage kosten een DDoS-aanval te laten uitvoeren,[34] wat zeker bijdraagt aan de vastgestelde stijging van het aantal DDoS-aanvallen. Eenvoudige DDoS-aanvallen kunnen door steeds betere mitigatiemiddelen ook steeds beter worden afgeslagen. Meer geavanceerde, op de applicatielaag gerichte DDoS-aanvallen (layer 7 DDoS) zijn lastiger te herkennen en daardoor lastiger te bestrijden, omdat deze aanvallen het gedrag van legitieme gebruikers nabootsen.

Een nieuwe ontwikkeling in de rapportageperiode is de toename van DDoS-aanvallen die zijn gebaseerd op amplificatie door middel van UDP-protocollen.[35]

**Snake/Uroburos**
Een van de meest geavanceerde stukken malware die de afgelopen jaren is aangetro□en, is de Uroburos rootkit. Er zijn aanwijzingen dat varianten al sinds 2011 in omloop zijn en tot 2014 onopgemerkt zijn gebleven. De complexiteit wordt vergeleken met de beruchte Stuxnet-worm. Uroburos (ook wel Snake genoemd) bevat sporen van Russischtalige ontwikkelaars en vertoont veel overeenkomsten met eerdere inlichtingenoperaties tegen Amerikaanse militaire installaties.[37]

Op deze manier zijn in de rapportageperiode nieuwe records gebroken. In februari 2014 zijn bij een NTP-amplificatieaanval op het Franse webbedrijf Cloudflare bandbreedtes van 400 Gbps gemeten.[38] Voorbeelden van amplificatieaanvallen zijn DNS-amplification en de Chargen aanval. Deze protocollen maken gebruik van UDP. Hierdoor is het niet noodzakelijk om een verbinding tot stand te brengen. Door relatief kleine verzoeken te sturen met een vervalst

29 Zie h□p://www.□reeye.com/blog/technical/2013/11/new-ie-zero-day-found-in-watering-hole-a□ack.html
30 h□p://www.zdnet.be/article/155615/hoe-de-belgische-overheid-werd-gehackt/
31 Zie verdiepingskatern Ransomware en cryptoware.
32 Zie kader cryptocurrencies, pagina 31.
33 Zie voor trendcijfers h□p://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts (geraadpleegd op 13 juni 2014)
34 h□p://krebsonsecurity.com/2014/02/the-new-normal-200-400-gbps-ddos-a□acks/
35 User Datagram Protocol: communicatieprotocol, sneller maar minder betrouwbaar dan TCP.
36 Bron: Verizon 2014 Data Breach Investigation Report
37 h□ps://www.gdata.de/rdk/dl-en-rp-Uroburos
38 h□p://blog.cloud□are.com/technical-details-behind-a-400gbps-ntp-ampli□cation-ddos-a□ack




*Figuur 7. Aantal nieuw ontdekte mobiele malwarefamilies en –varianten* [39]

**Malware in het mobiele domein**
In Nederland worden steeds meer smartphones en tablets gebruikt.[23] Daarmee wordt het interessanter voor kwaadwillenden om malware voor mobiele apparaten te schrijven. Mobiele malware hee nagenoeg hetzelfde doel als 'ouderwetse' pc-malware.

**Er zijn wel enkele opvallende verschillen:**

» Mobiele apparaten verkrijgen hun apps vaak via winkels. Het is dus niet altijd mogelijk applicaties vrij te verspreiden. De makers van het besturingssysteem (zoals Apple, Google en Microso) beheren deze winkels. Zij hebben allemaal beleid voor het actief opsporen en verwijderen van 'rogue apps', malware die is vermomd als bruikbare app. Hierdoor verspreidt mobiele malware zich veel langzamer dan op pc's. De wijze waarop dit beleid wordt gehandhaafd (vooraf goedkeuren versus achteraf doorzoeken) verschilt echter. Dat is mede van invloed op de hoeveelheid aangetroen malware per systeem. Veel mobiele malware wordt verspreid via niet-ociële winkels of webfora. Ook vindt verspreiding plaats via geïnfecteerde, legitieme websites of mobiele botnets. Het 'rooten' of 'jailbreaken' van het mobiele apparaat vergroot het risico aanzienlijk.

» Omdat mobiele telefoons worden gebruikt als tweede kanaal voor authenticatie, zijn er malwarecombinaties die zowel de pc als de smartphone van het slachtoer proberen te besmeen, om zo bijvoorbeeld transacties van internetbankieren te kunnen manipuleren.

» Cybercriminelen kunnen telefoons ook expres laten bellen of sms'en naar dure betaalnummers. Wanneer criminelen een dergelijk nummer zelf beheren, kunnen zij de kosten die de telefoon maakt voor het bellen naar dit nummer zelf innen. De gebruiker krijgt vervolgens de rekening gepresenteerd.

**Een aantal zaken is vergelijkbaar met desktopmalware:**

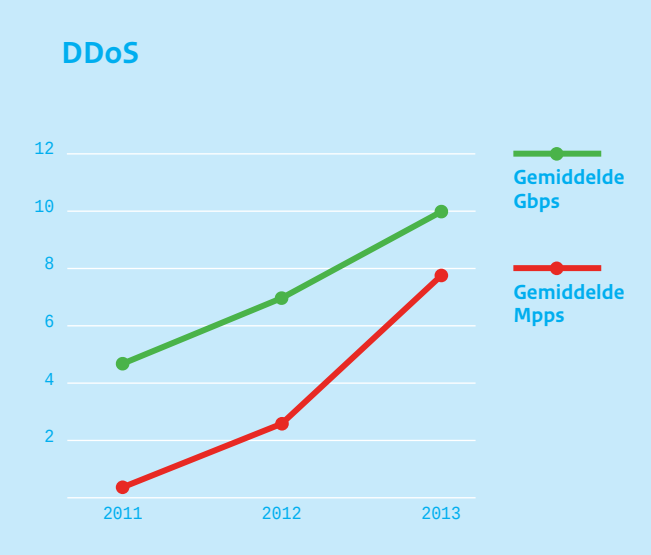
» Malwareschrijvers richten zich op de populairste systemen. Voor pc's is dat overduidelijk Windows is. Mobiele malware richt zich het meest op Android; iOS hee hier minder last van en door het lage gebruik van Windows Phone wordt daar vrijwel nooit malware voor gezien. Hieruit kan overigens niet worden geconcludeerd welke besturingssystemen veiliger of minder veilig zijn. Het zegt enkel iets over de dreiging.

» Antivirusbedrijven leveren speciale antivirusproducten voor smartphones, ongeacht of de fabrikant van de telefoon dit nodig vindt.

Figuur 7 laat zien dat het overgrote deel van de mobiele malware zich op Android richt. De absolute aantallen stellen echter maar weinig voor bij de miljoenen varianten van desktopmalware. Symbian, waarop oude Nokia-toestellen draaien, lijkt nog altijd populairder dan Apple iOS.

39 Bron: hp://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf en hp://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q1_2014.pdf

40 Zie hp://www.marketingfacts.nl/statistieken/channel/mobile_marketing




*Figuur 8. DDoS-bandbreedtes (in gigabit per seconde en megapacket per seconde)* [20]

afzender IP-adres (het doelwit), krijgt dit doelwit de relatief grote antwoorden in UDP formaat te verwerken. Vanuit het perspectief van het slachtoffer lijkt het alsof hij wordt aangevallen door deze legitieme servers. Amplificatieaanvallen worden gebruikt omdat enerzijds het vervalsen van UDP-verkeer zeer eenvoudig is en dit vervalste verkeer niet wordt gefilterd. Bovendien is een groot aantal zogenaamde open services aan het internet gekoppeld (zoals open DNS-resolvers). Figuur 8 geeft de gemiddelde bandbreedte van DDoS aanvallen weer. Over groei door amplificatieaanvallen zijn nog weinig cijfers beschikbaar.

Remote Access Tool (RAT) In 2013 zijn professionele online pokerspelers slachtoffer geworden van besturing op afstand via een zogenaamde RAT-besmetting.[41] Hierbij kijkt iemand mee op het scherm van de geïnfecteerde computer. In dit geval was het doel om zicht te krijgen op de kaarten van de speler en daarmee de tegenstander voordeel te geven in het pokerspel.

**Casus Carberp**

In juni 2013 werd de broncode van het Carberp botnet voor 25.000 dollar op een zwarte markt verkocht, nadat het de afgelopen jaren naar schaling 250 miljoen dollar had opgebracht. Enige maanden eerder waren de uitbaters van het botnet in Rusland en Oekraïne gearresteerd. Het pakket met de broncode besloeg 5 GB en ongeveer 30.000 bestanden. Enkele uren nadat het was verkocht, was het pakket gelekt en daardoor algemeen beschikbaar. Cybercriminelen hebben hierdoor de mogelijkheid Carberp aan te passen en van nieuwe mogelijkheden te voorzien.[42]

Een Rotterdamse hacker die in oktober 2013 werd aangehouden wegens verdenking van inbraak in ongeveer 2.000 computers,[43] zou ook gebruik hebben gemaakt van een RAT.

Ransomware en cryptoware De afgelopen jaren lieten een grote opkomst van ransomware (gijzelingssoftware) zien. Deze ransomware is steeds innovatiever en agressiever. De verschillende verschijningsvormen zijn steeds beter toegesneden op de ontvanger en maken gebruik van innovatieve technologische kapingsmogelijkheden. Ook de ingezette betaalmiddelen zijn steeds slimmer, met gebruikmaking van vouchercodes en cryptocurrencies (zie kader). Eind 2013 kwam een bijzondere vorm van ransomware op: cryptoware.

In Nederland zijn veel ransomware-besmettingen en nog maar weinig cryptoware-besmettingen geconstateerd. In omliggende landen zijn al veel cryptoware-besmettingen gesignaleerd. De opkomst van cryptoware is verontrustend: in een deel van de gevallen lijkt betaling van losgeld te helpen. Dit in tegensteling tot klassieke ransomware.

Ransomware en in het bijzonder cryptoware hanteren een zeer lucratief businessmodel. Dit illustreert verdergaande professionalisering van de cybercrimesector. Opsporingsdiensten hebben het afgelopen jaar veel geïnvesteerd in voorlichting over en bestrijding van ransom- en cryptoware. Zie voor meer informatie het verdiepingskatern Ransomware en cryptoware.

Phishing blijvende ergernis E-mail blijft voor cybercriminelen een belangrijk middel om gegevens van slachtoffers te verkrijgen of om potentiële slachtoffers te verleiden tot het onbedoeld installeren van malware.[44]

De kwaliteit van phishing-e-mails neemt toe; zo bevatten ze minder taalfouten. De opzet is nog vaak hetzelfde: ze vragen de “klant” snel te reageren, onder dreiging van bijvoorbeeld het afsluiten van een bepaalde dienst.

Een veelgebruikte vorm is de combinatie van phishing per e-mail en telefoon. Cybercriminelen nemen telefonisch contact op, laten merken dat ze het nodige weten over de klant en winnen zo zijn/haar vertrouwen. Daarmee verleiden ze de klant om bijvoorbeeld wachtwoorden af te geven. De Waarschuwingsdienst, ECP en de banken informeren klanten constant over dit soort aanvallen en drukken hen op het hart nooit beveiligingscodes af te geven over de telefoon of op niet-standaard websites.

Veel besmettingen met exploit kits of RATs vinden plaats na het klikken op een link in een ontvangen e-mailbericht. Cybercriminelen en statelijke actoren[45] gaan hierbij steeds gerichter te werk door mailberichten interessant te maken voor een specifiek belaagde doelgroep (spearphishing).

41 Bron: F-secure Threat Report H2 2013
42 http://tweakers.net/nieuws/89904/vrees-voor-malwaregolf-laait-op-na-vrijkomen-broncode-carberp-trojan.html
43 Zie kader Persoonlijke afpersing en gerichte datagijzeling relevante nieuwe dreiging, pagina 55.
44 http://ictmagazine.nl/1384/nanciele-phishing-aanvallen-nederland-misbruiken-naam-van-banken/
45 Jaarverslag MIVD 2013.

Nederland host veel mala□de sites Bij vrijwel alle in dit CSBN genoemde dreigingen wordt gebruik gemaakt van hosting. Hostingproviders faciliteren daarmee bewust of minder bewust verschillende vormen van criminaliteit. De meeste hostingproviders hanteren een model van subcontracting, waardoor zij weinig tot geen zicht hebben op de feitelijke gebruikers van hun infrastructuur. Het kan dan ook voorkomen dat een malafide tussenpartij een heel rack doorverhuurt aan cybercriminelen. In diverse rapporten van antivirusbedrijven[46] staat Nederland hoog op de ranglijst van landen waar malafide sites worden gehost. De politie merkt op dat bepaalde Nederlandse hostingproviders vaker als dienstverlener naar voren komen in opsporingsonderzoeken dan anderen.

Digitale certi□caten Een groeiende trend is het signeren van malware met ogenschijnlijk legitieme digitale certificaten. Makers van malware signeren hun product om slachtoffers, maar ook beveiligingssoftware te laten denken dat het om legitieme software gaat. Een deel van de certificaten waarmee cybercriminelen deze malware signeren wordt verkregen door diefstal of aanschaf bij minder betrouwbare certificate authorities. Verder wordt malware verspreid door misbruik van geautomatiseerde content distribution networks (CDNs), die programmatuur inpakken in gesigneerde, legitieme installatiesoftware.[47]

Het groeiende misbruik kan leiden tot minder vertrouwen in digitale certificaten. De effectiviteit van digitale certificaten kan zo op termijn afnemen.

## Werkwijze en organisatie

Marktwerking De daling in het aantal publiek gemaakte exploits per jaar kan mogelijk worden verklaard door de stijgende prijzen die kopers op grijze en zwarte markten betalen voor zero-day exploits. Hierdoor loont het meer om een nieuw ontdekte exploit te verkopen aan de hoogste bieder, dan deze tegen een lagere vergoeding op de witte markt aan de verantwoordelijke leverancier aan te bieden.

Grijze markten beperken zich tot de verkoop van kwetsbaarheden en exploits en zijn op zich niet illegaal. Ook overheden en bedrijven bewegen zich op deze markt. Het verhandelen van kwetsbaarheden en exploits aan partijen anders dan de betreffende leverancier blijft echter omstreden. Het Franse securitybedrijf Vupen[48] levert exploits voor nieuw ontdekte zero day kwetsbaarheden aan overheden van vertrouwde landen.

46 h□p://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012
h□p://www.mcafee.com/tw/resources/reports/rp-quarterly-threat-q2-2012.pdf
47 McAfee Labs Threat s Report, Fourth Quarter 2013.
48 h□p://www.zdnet.com/
nsa-purchased-zero-day-exploits-from-french-security-□rm-vupen-7000020825/

**Toenemend gebruik van Cryptocurrencies**

Afgelopen jaar kocht een Noorse student een appartement met eenvijfde van zijn bitcoins. In 2009 had hij voor 18,50 euro geïnvesteerd in 5000 bitcoins. Eind 2013 waren die meer dan 600.000 euro waard.[49] Cryptocurrencies en vooral de bitcoin hebben de afgelopen jaren een grote bekendheid gekregen. Op het hoogtepunt in 2013 was 1 bitcoin ruim 900 euro waard.[50] De waarde is inmiddels gedaald, maar de populariteit van de bitcoin lijkt niet af te nemen. Steeds meer bedrijven accepteren de bitcoin als betaalmiddel.[51] Naast de bitcoin zijn ruim tweehonderd andere vormen van cryptocurrencies (zoals de litecoin en feathercoin) in gebruik.[52]

De afwezigheid van een centrale bank en het gebruiksgemak van microbetalingen zijn de belangrijkste redenen om gebruik te maken van deze diensten. Het toekomstige gebruik is moeilijk in te scha□en. Door de □uctuerende waarde en de beperkte beschikbaarheid zal het gebruik in absolute zin waarschijnlijk niet sterk toenemen. De mogelijkheden voor het gebruik van cryptocurrencies worden in de dagelijkse praktijk ondertussen wel steeds groter. Op een aantal plaatsen zijn zelfs bitcoinautomaten geplaatst.[53]

De aard en omvang van het gebruik van cryptocurrencies door de Nederlander zijn niet exact bekend. Ongeveer 2 procent van alle bitcoins zou in handen zijn van Nederlandse gebruikers.[54] In het CSBN-3 werd al verwezen naar mogelijkheden voor crimineel gebruik. Dit is inderdaad realiteit geworden.[55] Bitcoins worden in meerdere ransomware-varianten als betaling geëist. Daarnaast is een groeiend aantal afpersingen van bedrijven waargenomen, waarin een dreiging met een DDoS-aanval kon worden afgekocht met bitcoins. Op het TOR-netwerk zijn marktplaatsen te vinden waarop handel in drugs, goederen en diensten plaatsvindt. De betaling wordt grotendeels gedaan in cryptocurrencies. Ook voor het witwassen van crimineel geld wordt gebruik gemaakt van cryptocurrencies. Dit gebeurt niet alleen door het aanscha□en en weer verkopen van (bijvoorbeeld) bitcoins, ook de aankoop van bitcoins is soms onderdeel van de witwasmethode.

Door het toenemende gebruik van cryptocurrencies ontstaat een risico voor de bedrijven die de cryptocurrencymarkt faciliteren. Deze bedrijven kunnen zelf ook slachto□er worden van nieuwe en geavanceerde vormen van criminaliteit, zoals het hacken van exchangebedrijven en digitale portemonnees. Het afgelopen jaar zijn hiervan in Nederland nog relatief weinig signalen aangetro□en. De signalen uit het buitenland wijzen er echter op dat ook deze vorm van criminaliteit een vlucht neemt.

De aanpak van crimineel gebruik van cryptocurrencies is een prioriteit van de Nederlandse overheid.

49 h□p://www.ad.nl/ad/nl/4561/Wetenschap/article/detail/3534376/2013/10/28/Noor-kocht-Bitcoins-voor-18-50-euro-hee□-nu-ruim-6-ton.dhtml
50 h□p://www.bitcoinweb.nl/bitcoinstatistieken/koers-bitcoin-euro/. Dit stuk gaat enkel over de bitcoin, omdat deze cryptocurrency de meeste bekendheid hee□ en het meeste wordt gebruikt.
51 Niet alleen online webshops, maar ook horeca, hotels en drogisterijen accepteren de bitcoin in Nederland (www.bitcoinspot.nl).
52 Bron: h□p://coinmarketcap.com/
53 h□p://www.volkskrant.nl/vk/nl/2680/Economie/article/detail/3619605/2014/03/20/Eerste-Bitcoin-automaat-van-Nederland-geopend-in-Den-Haag.dhtml
54 www.rijksoverheid.nl/...bitcoin/antwoorden-op-vragen-bitcoin.pdf
55 Zie CSBN-3, blz. 30.

Zwarte markten zijn opgezet om cybercrime te faciliteren en zijn ondertussen een wereldwijd verschijnsel geworden. Deze virtuele markten voor exploits, malware en gestolen informatie (zoals creditcard- en accountgegevens) zijn de afgelopen jaren gegroeid en geprofessionaliseerd.

Deze ondergrondse markten zijn voor overheidsinstanties niet of slecht te doorzien. Dat komt door het gebruik van middelen om anoniem toegang te verkrijgen (zoals TOR)[56] en door pseudo-anoniem[57] betalingen te verrichten via cryptocurrencies (zoals de bitcoin). Het hogere segment van de markten is juist exclusief toegankelijk voor een beperkte groep, die grondig is 'gescreend' door de marktbeheerder.

> *"Nederland staat hoog in de ranglijsten van landen waar mala de sites gehost worden."*

Cybercrime-as-a-service Aanbieders bestaan steeds meer uit georganiseerde groepen (cyber)criminelen die hebben ontdekt dat deze markt zeer lucratief is en minder risico's met zich meebrengt dan fysieke criminele activiteiten. Het is een stuk eenvoudiger een wereldwijd distributienetwerk op te zetten voor virtuele handelswaar dan een fysiek distributienetwerk voor bijvoorbeeld verdovende middelen.[58]

Cybercriminelen bieden hun diensten steeds vaker aan aan wie hiervoor wil betalen. Deze diensten worden heel professioneel en compleet geleverd:[59] van technische hulpmiddelen tot infrastructuur en soms zelfs helpdeskfunctionaliteit.

Groot voordeel voor de afnemers is dat zij deze diensten direct kunnen gebruiken, zonder zelf tijd en geld te hoeven investeren in de benodigde kennis en middelen.

## Conclusie

Het jaarlijks aantal publiek gemaakte exploits daalt. Mogelijk wordt het lastiger goede exploits voor kwetsbaarheden te ontwikkelen en is er een verband met de stijgende prijzen voor zero-day exploits. Er is een groeiende (grijze en zwarte) markt voor exploits, waarin ieder jaar meer geld omgaat. Het is onduidelijk of er simpelweg minder exploits zijn of dat het aantrekkelijker is geworden om exploits te commercialiseren.

De hoeveelheid malware blijft ieder jaar hard stijgen. In veel gevallen gaat het om varianten op bestaande malware die slechts een kort bestaan kennen. De vraag is of traditionele antivirusproducten op basis van signature-herkenning nog wel effectief zijn, of dat er daarnaast moet worden ingezet op andere vormen van bescherming tegen malware.

Botnets worden steeds beter verhuld en verdedigd en kunnen dus worden ingezet bij meer en zwaardere DDoS-aanvallen. Mobiele malware neemt wereldwijd aanzienlijk toe, maar tot op heden zijn grootschalige besmettingen in Nederland nog niet vastgesteld. Gerichte spearphishing zorgt voor een toename van deze besmettingen. Ransomware is steeds innovatiever en agressiever. In Nederland zijn veel ransomware-besmettingen en nog maar weinig cryptoware-besmettingen. De opkomst van varianten waar betalen lijkt te helpen is zorgelijk, omdat hierdoor een innovatief en lucratief businessmodel lijkt te ontstaan.

Beschikbare hulpmiddelen om kwetsbaarheden te benutten worden professioneler, uitgebreider en zijn eenvoudiger toe te passen. Door de ontwikkeling van cybercrime-as-a-service neemt de beschikbaarheid van deze hoogwaardige aanvalsmiddelen toe, ook voor technisch minder onderlegde gebruikers. Het wordt zo steeds eenvoudiger om aanzienlijke schade toe te brengen. «

56 TOR staat voor The Onion Router en levert de mogelijkheid om over het internet anoniem te communiceren.
57 Bitcointransacties zijn niet volledig anoniem omdat het bitcoinadres wordt vastgelegd.
58 Markets for Cybercrime Tools and Stolen Data, RAND Corporation.
59 h□p://resources.infosecinstitute.com/cybercrime-as-a-service/

“OOK IN DE TOEKOMST IS FOUTLOZE SOFTWARE ONWAARSCHIJNLIJK”

# HOOFDSTUK 4 » WEERBAARHEID: KWETSBAARHEDEN

**Weerbaarheid gaat over de mate waarin belangen zijn beschermd tegen dreigingen. De mate van weerbaarheid wordt enerzijds bepaald door de aan- of afwezigheid van kwetsbaarheden die de bescherming van onze belangen verminderen en anderzijds door de aan- of afwezigheid van maatregelen die de weerbaarheid vergroten. In dit hoofdstuk wordt ingegaan op de ontwikkelingen op het gebied van kwetsbaarheden. Kwetsbaarheden in so□ware vormen nog steeds de achilleshiel van cybersecurity. Hier was het afgelopen jaar een lichte stijging te zien. Ook de gebruiker blij□ aandacht verdienen als bron van kwetsbaarheid, door trends als BYOD en cloudcomputing.**

Een kwetsbaarheid is een eigenschap van ICT, een organisatie of een gebruiker die actoren kunnen misbruiken om hun doelen te bereiken of die door een natuurlijke of technische gebeurtenis kan leiden tot verstoringen.

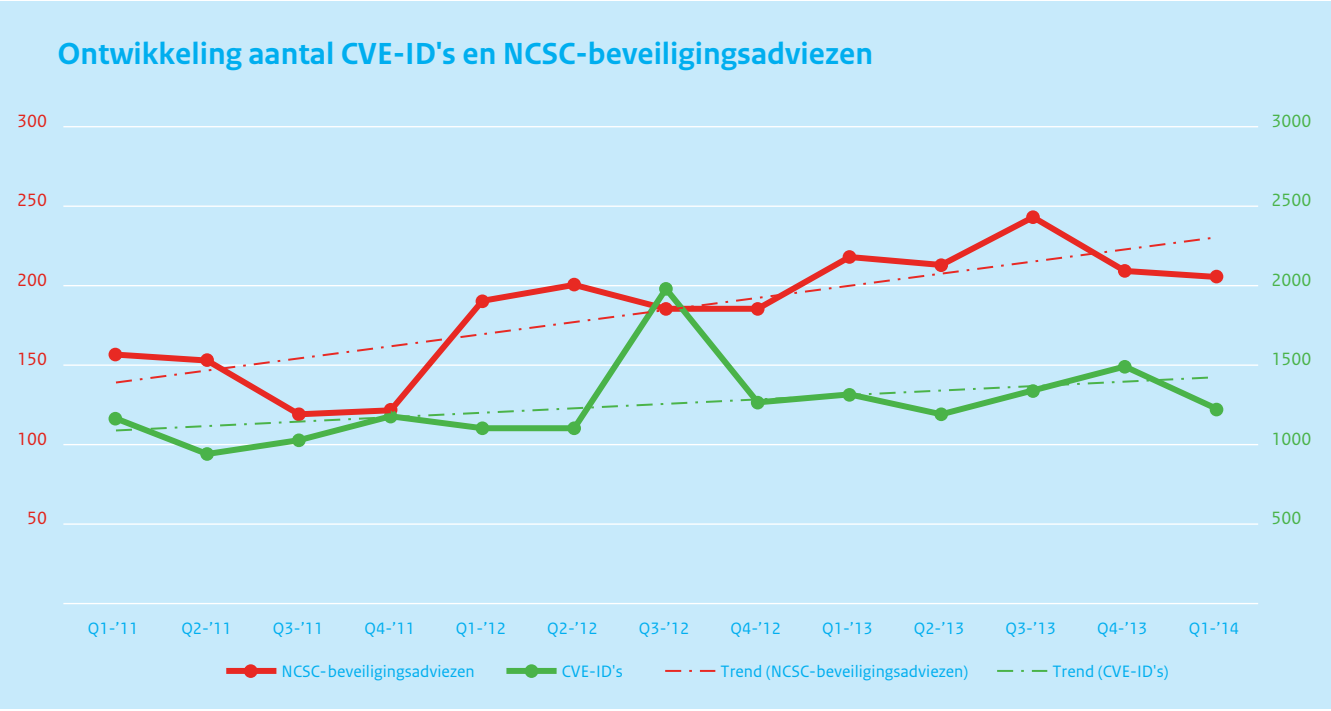
## Technische kwetsbaarheden

Trend kwetsbaarheden in standaardso□ware blij□ licht stijgen De afgelopen rapportageperiode laat een licht stijgende trend zien in het aantal geconstateerde kwetsbaarheden, gebaseerd op CVE-registraties in de National Vulnerability Database.[60] De stijging in het CSBN-3 was sterker door een piek in het derde kwartaal van 2012.

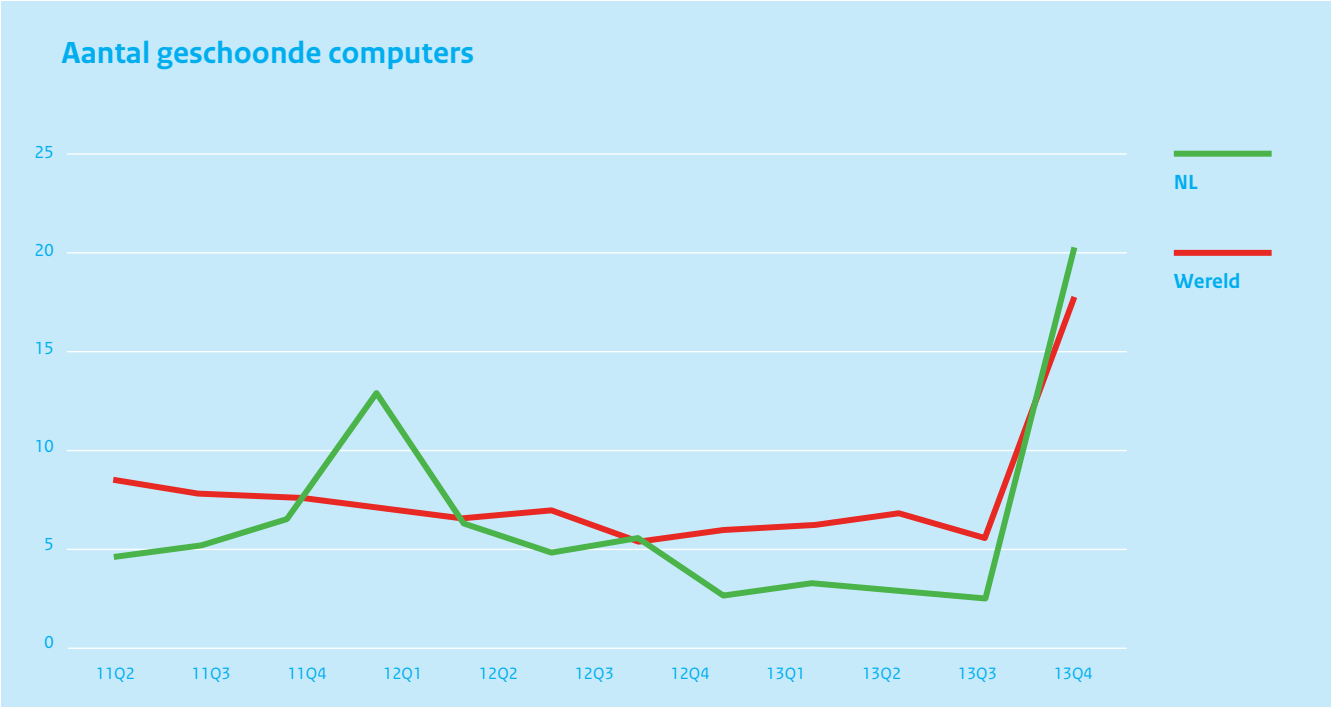
Het aantal NCSC-beveiligingsadviezen bereikte in het derde kwartaal van 2013 een nieuw hoogtepunt. Die stijgende trend houdt verband met de ontwikkeling dat steeds meer partijen zich bij het NCSC aansluiten.[61]

60 De Common Vulnerabilities and Exposures (CVE) is een eenduidige en wereldwijd erkende identi□catie van publiek bekende informatiebeveiligingskwetsbaarheden. Geraadpleegd april 2014: h□p://nvd.nist.gov/

61 Omdat meer partijen zich aansluiten bij het NCSC, wordt over meer so□ware beveiligingsadvies gegeven.




*Figuur 9. Aantal CVE-registraties en NCSC-beveiligingsadviezen per kwartaal*

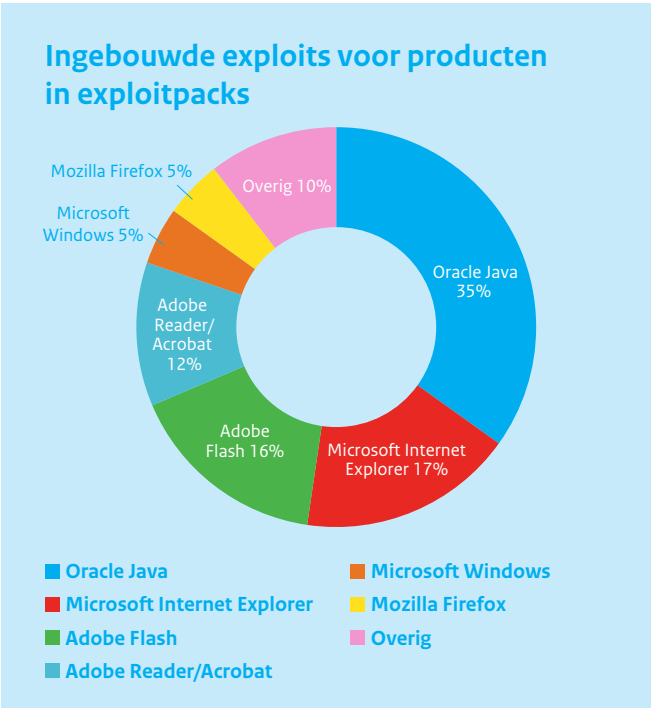



*Figuur 10. Aantal opgeruimde besme ingen per duizend gescande computers in Nederland en de rest van de wereld*[62]

In figuur 9 staan de aantallen CVE-registraties en NCSC-beveiligingsadviezen per kwartaal weergegeven. Beide grafieklijnen hebben een eigen schaal, maar worden gezamenlijk weergegeven om de trend te kunnen vergelijken.

In figuur 10 wordt het aantal opgeruimde besmettingen per duizend gescande computers weergegeven voor Nederland en de wereld. Te zien is dat Nederland meestal iets lager scoort. Dit is een indicatie dat er in Nederland gemiddeld minder malwarebesmettingen plaatsvinden dan elders in de wereld. De plotselinge stijging in beide grafieklijnen in het laatste kwartaal van 2013 is te herleiden op het door Microsoft kwalificeren van Rotbrow en Brantall (al langer bekende software) als malware. Hierdoor ontstaat een (waarschijnlijk) tijdelijke piek in geschoonde systemen.

Kwetsbaarheden in Java meest misbruikt Exploitkits bundelen kant-en-klare exploits voor kwetsbaarheden, waarmee het eenvoudig is om in korte tijd grote hoeveelheden systemen te infecteren. Figuur 11 geeft een inventarisatie weer van Contagiodump[63] van ingebouwde exploits voor producten in 60 exploitkits. De verhoudingen zijn ten opzichte van de rapportageperiode van het CSBN-3 marginaal verschoven. Alleen voor Oracle Java is het aantal exploits relatief sterk gestegen. Ook andere bronnen melden de sterke aanwezigheid van Java in de exploitmarkt.[64] Samen met Java zijn Microsoft Internet Explorer en Adobe Flash en Adobe Reader/Acrobat goed voor 80 procent van de ingebouwde exploits in exploitkits.




*Figuur 11. Misbruikte so ware door exploitkits*

De populariteit van Java onder exploitschrijvers is niet alleen een dreiging voor pc's. Java wordt veel gebruikt als embedded software in bijvoorbeeld auto's, mobiele telefoons (ook niet-smartphones) en televisies. Deze embedded software is veelal lastiger up-to-date te houden dan in standaard pc's, waardoor kwetsbaarheden moeilijker te verhelpen zijn.

Kwetsbaarheden in so□ware blijven de achilleshiel van cybersecurity De kwetsbaarheid van software en systemen blijft onverminderd groot. Hierin lijkt geen verandering te komen. Dit is de technische achilleshiel voor het waarborgen van cybersecurity,

62 Bron: Microso□ Security Intelligence Report volume 16, h□p://www.microso□.com/sir

63 h□p://contagiodump.blogspot.com/ en h□ps://docs.google.com/spreadsheet/ccc?key=0AjvsQV3iSLa1dE9EVGhjeUhvQTNReko3c2xhTmphLUE&usp=drive_web#gid=0 (geraadpleegd april 2014)

64 Cisco: 91 procent van alle web-exploits maakt misbruik van Java (www.cisco.com/assets/global/FR/pdfs/executive_security/sc-01casr2014_cte_lig_fr_35330.pdf). Microso□: ongeveer 72 procent van alle gerichte exploits maakt misbruik van Java (h□p://download.microso□.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microso□_Security_Intelligence_Report_Volume_16_English.pdf

zeker wanneer het veelgebruikte standaardsoftware betreft die in veel systemen wordt toegepast.

Er is nog geen oplossing voor dit probleem Meer aandacht voor concepten als security-by-design[65] en secure software development[66] kan de omvang van het probleem mogelijk inperken, maar ook in de toekomst is foutloze software onwaarschijnlijk.

De populairste aanvalsmethode van cybercriminelen blijft het misbruiken van bekende kwetsbaarheden in veelgebruikte software. Omdat zowel beheerorganisaties als particuliere gebruikers software-updates( waarin bekende kwetsbaarheden zijn opgelost) vaak niet of pas laat uitvoeren, kunnen cybercriminelen wetsbaarheden soms langdurig uitbuiten.

**Casus Heartbleed**

De Heartbleed-kwetsbaarheid[67] hield de gemoederen in april 2014 □ink bezig. Heartbleed liet aanvallers op afstand het interne geheugen lezen van systemen die OpenSSL gebruiken.[68] OpenSSL is een programmeerbibliotheek om beveiligde verbindingen mee op te ze□en: veel verschillende systemen gebruiken het, zoals webservers, VPN-servers of wi□-accesspoints. In de week na publicatie van de kwetsbaarheid gingen organisaties naarstig op zoek naar welke systemen zoal OpenSSL gebruikten en of deze kwetsbaar waren. Het was niet eenvoudig om in te scha□en wat de kans was dat een organisatie getro□en was, of om een aanval achteraf te detecteren. Er was voor deze kwetsbaarheid ook aanzienlijke aandacht in de reguliere (niet-technologische) media.

Heartbleed bestond uit een programmeerfout in OpenSSL, die niet eerder was opgemerkt. De kwetsbaarheid hee□ twee jaar in OpenSSL gezeten. De code van OpenSSL wordt maar beperkt nagekeken, ook al wordt de bibliotheek veel gebruikt. Om dit in de toekomst te voorkomen, hebben grote technologiebedrijven aangekondigd OpenSSL en andere belangrijke opensourceprojecten in de toekomst uitgebreider □nancieel te ondersteunen.[69]

De situatie rondom Heartbleed roept de vraag op of soortgelijke situaties zich ook bij andere essentiële so□warebibliotheken en programma's kunnen voordoen.

65 Zie h□p://cmmiinstitute.com/resource/security-by-design-with-cmmi-for-development-version-1-3/ (geraadpleegd juni 2014)
66 Zie h□p://www.cip-overheid.nl/wp-content/uploads/2014/05/Grip-op-SSD-Het-proces-v1-03.pdf (geraadpleegd juni 2014)
67 Zie h□p://heartbleed.com/ (geraadpleegd: mei 2014)
68 Zie h□ps://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-heartbleed-ernstige-kwetsbaarheid-in-openssl.html (geraadpleegd: mei 2014)
69 Bron: h□p://arstechnica.com/information-technology/2014/04/tech-giants-chastened-by-heartbleed-□nally-agree-to-fund-openssl/

Duurzaamheid van ICT groeiend probleem De trend dat steeds meer apparatuur – waaronder medische apparatuur, voertuigen, televisies en huishoudelijke apparaten – aan het internet verbonden is, zal doorzetten. De software in deze apparatuur zal altijd beveiligingslekken blijven bevatten. Leveranciers en afnemers beschouwen elektronische apparatuur zoals smartphones, nog te vaak als wegwerpproducten, waaraan na de initiële productie en verkoop nauwelijks meer aandacht hoeft te worden besteed.

Bij sommige apparaten is het niet mogelijk software-updates te installeren. Andere apparaten worden door leveranciers voor een beperkte periode voorzien van updates. Ook komt het voor dat er wel updates beschikbaar zijn, maar dat gebruikers hier niet van op de hoogte zijn of niet weten hoe ze deze moeten installeren. Daarnaast weten gebruikers vaak niet welke producten en softwareversies allemaal op hun apparatuur zijn geïnstalleerd.

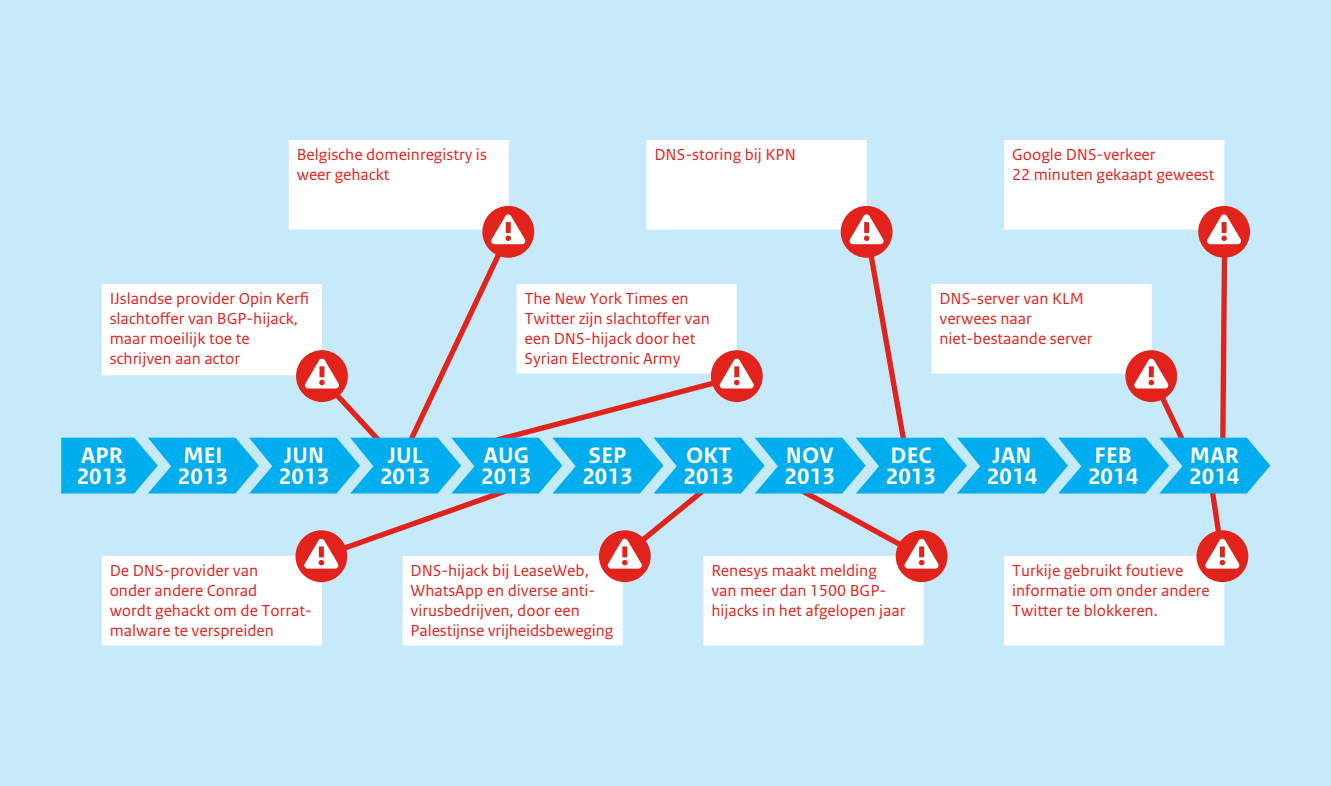
Omdat verouderde software vaak kwetsbaarheden bevat die al langer bekend zijn maar die niet meer worden opgelost, kunnen cybercriminelen deze blijvend misbruiken. Hierdoor ontstaat een groeiend ICT-duurzaamheidsprobleem.[70]

Verschuiving in misbruik van kwetsbaarheden Door de verdere toepassing van organisatorische en technische maatregelen om computers beter te beveiligen en de toenemende marktpenetratie van laptops, tablets en smartphones gaan cybercriminelen zich steeds vaker richten op andere systemen dan de traditionele pc.

Gegevens worden steeds vaker opgeslagen in de cloud. Dit betekent dat de cloud ook voor cybercriminelen interessanter wordt en dat incidenten bij cloudproviders steeds grotere gevolgen voor steeds grotere groepen gebruikers kunnen hebben.

Een andere verschuiving is dat cybercriminelen proberen een zo groot mogelijk bereik voor hun malware te verkrijgen door eerder in het proces te gaan zitten. In plaats van het plaatsen van malware op één enkele website, kan door het besmetten van bijvoorbeeld een provider van online advertenties een grote hoeveelheid sites (en daarmee bezoekers) worden geraakt.

70 Zie ook het verdiepingskatern Duurzaamheid ICT




*Figuur 12. Tijdlijn van DNS- en BGP-incidenten*

**Casus Target point-of-sale-malware**

In januari 2014 werd bekend dat de Amerikaanse winkelketen Target het slachto□er is geworden van een cyberaanval die speci□ek was gericht op hun kassasystemen.[71] De persoonlijke gegevens (waaronder debit- en creditcardnummers) van tientallen miljoenen klanten bleken te zijn gestolen.

In de Verenigde Staten komen aanvallen op winkels omwille van hun opgeslagen creditcardnummers vaker voor. Het incident bij Target valt op door zijn omvang. Niet eerder werd een voorval bekend waarbij zo veel klantgegevens zijn gestolen in een aanval die zich speci□ek rich□e op kassasystemen. De aanvallers zijn waarschijnlijk binnengekomen doordat zij via phishing de inloggegevens van een medewerker van een verwarmingsonderhoudsbedrijf wisten te verkrijgen. Deze medewerker had toegang tot een netwerk van Target dat gekoppeld was aan de kassasystemen.[72]

Door de media-aandacht werd ook in Nederland gekeken naar de kwetsbaarheid van betaalautomaten. Nederland is minder kwetsbaar voor dergelijke aanvallen vanwege het beperkte gebruik van creditcards en de grote voorkeur voor het pinnen. Omdat de EMV-chip die op de pinpas wordt gebruikt cryptogra□sche technieken gebruikt in plaats van een statisch nummer zoals op creditcards, is het onderscheppen van pasgegevens niet voldoende om kopieën te maken en daarmee betalingen te doen. Ook de pincode is een onderdeel van de beveiliging.

### Intrinsieke kwetsbaarheid van "oude" protocollen

De fundamentele bouwstenen van het internet zijn protocollen die ruim 30 jaar geleden zijn ontwikkeld, zonder enige notie van hoe groot internet in de daaropvolgende decennia zou worden. Protocollen als BGP, DNS en SMTP gebruiken nauwelijks enige vorm van verificatie, authenticatie of encryptie en werken op basis van vertrouwen in de integriteit van hun communicatiepartners.

Kwaadwillenden proberen de gebreken in deze protocollen te misbruiken. DNS en BGP, beide noodzakelijk voor het routeren van internetverkeer, zijn een gewild doelwit om internetverkeer naar ongewenste bestemmingen om te leiden en zo slachtoffers bijvoorbeeld massaal met malware te besmetten of vervalste webpagina's te tonen waarmee wachtwoorden kunnen worden gestolen (zie figuur 12).

De incidenten die zich in de rapportageperiode hebben voorgedaan zijn relatief klein. Het is niet denkbeeldig dat zich in het komende jaar grootschaliger incidenten zullen voordoen. Door misbruik van BGP zou op grote schaal internetverkeer kunnen worden afgeluisterd. Overigens kan ook onbewust foutief gebruik van deze kwetsbare protocollen grote gevolgen hebben.[73]

71 h□p://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/ (geraadpleegd: juni 2014)

72 h□p://krebsonsecurity.com/2014/02/email-a□ack-on-vendor-set-up-breach-at-target/ (geraadpleegd: juni 2014)

73 h□p://arstechnica.com/information-technology/2014/03/google-dns-brie□y-hijacked-to-venezuela/ (geraadpleegd: juni 2014)

**Industriële controlesystemen**
Verbetering van de beveiliging van Industriële Controlesystemen (ICS), waaronder SCADA-systemen, blijft aandacht verdienen. Het belang van dergelijke systemen voor de vitale processen in de samenleving staat buiten kijf. De afgelopen periode hebben zich geen grote incidenten voorgedaan. Dit wil echter niet zeggen dat de dreiging is afgenomen.

Het totaal aantal ontdekte kwetsbaarheden in ICS blijft toenemen, net als het aantal security-onderzoekers dat zich op dit specifieke gebied richt. Daarnaast is ook toenemende interesse en onderzoek naar de (on)mogelijkheden van procesmanipulatie via misbruik van kwetsbaarheden in ICS zichtbaar. Gebrek aan security-by-design, zeker bij oude(re) systemen, is hierin een belangrijk probleem.

Een aantal grote leveranciers en belangrijke eindgebruikers van ICS zetten wel stappen om de beveiliging van nieuwe systemen te verbeteren. Maar ook de beveiliging van oude (legacy) systemen moet op orde worden gebracht. Zeker met een toenemende connectiviteit (voor bijvoorbeeld informatie-uitwisseling en bediening) zijn aanvullende maatregelen noodzakelijk.

Grote incidenten met ICS mogen dan wel ontbreken, kleinere incidenten vinden wel degelijk plaats. Uit het jaaroverzicht van ICS-CERT[16] blijkt een toename van het aantal meldingen. Een deel hiervan betrof spearphishing mogelijk met het doel vanuit de kantooromgeving toegang tot ICS te krijgen, maar geen daadwerkelijke manipulatie van ICS.

In Nederland ontving het NCSC geen specifiek op ICS gerichte meldingen. Wel werd een klein aantal aan internet gekoppelde systemen (onder andere gebouwbeheer) onderzocht nadat publiek melding was gemaakt van de openstaande internetkoppeling.

Mogelijk speelt het 'verdienmodel' voor aanvallen op ICS ook een rol bij het beperkte aantal incidenten. Voor cybercriminelen is het aanvallen van ICS maar beperkt interessant: financieel gewin op andere gebieden is eenvoudiger. Er lijkt wel een kleine groep te bestaan die aan op ICS gerichte exploits (en toolkits) geld verdient.

Een aanval op ICS wordt in het kader van "cyberoorlog" als scenario gezien. Met een toenemend aantal staten dat openlijk toegeeft offensieve capaciteiten te ontwikkelen, wordt dit mogelijk een reëler scenario.

Actie blijft nodig en investeren in het versterken van de "digitale dijken" blijft essentieel.

## Kwetsbaarheden veroorzaakt door menselijke en organisatorische factoren

### Gebruikers blijven belangrijke bron van kwetsbaarheid vormen

Gebruikers vormen een belangrijke schakel in de beveiligingsketen. Er is sprake van een toename in het algemene beveiligingsbewustzijn van gebruikers,[75] zowel in de zakelijke als huiselijke context. Desondanks heeft ongeveer 35 procent van de gebruikers geen antivirussoftware geïnstalleerd.[76] Ook phishing-e-mails blijven slachtoffers claimen. Sommige (spear)phishing-e-mails zien er zo legitiem uit, dat het lastig is ze als onveilig te beoordelen. Dit vraagt om meer inzicht van gebruikers dan redelijkerwijs van hen kan worden verwacht.

Voor organisaties geldt dat de medewerkers de beveiligingsketen kunnen maken of breken. Bring your own Device en opslag van gegevens in de cloud stellen deze organisaties voor extra uitdagingen. De mogelijkheden en flexibiliteit voor de gebruiker nemen toe, maar de beheersbaarheid voor de organisatie wordt vaak minder. De kans op 'bedrijfsongelukken' wordt zo groter.

Aanvallers zijn sterk afhankelijk van social engineering om hun aanvallen te laten slagen. Er was in 2013 sprake van meer gerichte aanvallen.[77] Vooral interne actoren met een sleutelpositie binnen een organisatie zijn hiervoor kwetsbaar. Zij kunnen onbewust aan de basis staan van schending van informatie(systemen), bijvoorbeeld door op een phishing e-mail te reageren of een website te bezoeken die met malware is besmet.

Ook worden slachtoffers telefonisch benaderd, waarbij bellers proberen gebruikersnamen en (eenmalige) wachtwoorden te achterhalen om hiermee vervolgens toegang te krijgen tot informatie of systemen.

### Zorgen over big data nemen toe

De waarde van gedragsgegevens voor adverteerders is groot. Het vertrouwen in de zorgvuldige omgang met die gegevens neemt echter af. Het is voor gebruikers in veel gevallen niet duidelijk welke partij welke gegevens heeft vastgelegd en hoe deze vervolgens worden gebruikt of verhandeld. De hoeveelheid beschikbare data en de hoeveelheid mogelijkheden om die data te analyseren maken personen kwetsbaar ten opzichte van grote organisaties, die (onder andere) steeds betere risicoprofielen kunnen maken van hun potentiële klanten.

74 Zie ICS-CERT monitor okt-dec 2013 (www.ics-cert.us-cert.gov)
75 Bron: Special Eurobarometer 404 Cyber security, p. 37-39 http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf
76 Bron: Special Eurobarometer 404 Cyber security, p. 30
77 'Internet Security Threat Report 2014', Symantec, 2014.

**Uitbesteding van systeemkennis** Zowel afnemers als aanbieders van IT-diensten geven in de sectoranalyse onder ISAC's (Bijlage A) aan dat er toenemende aandacht is voor cybersecurity. Hoewel de kosten hiermee afnemen, neemt ook de inhoudelijke kennis over de ingekochte producten en diensten bij afnemers af. Het risico van ingebouwde 'achterdeurtjes' is aanwezig. Men heeft hierdoor geen zicht meer op eventuele cyberrisico's. Een voordeel van uitbesteding is dat dit sneller en eenvoudiger te patchen en te onderhouden is dan maatwerkoplossingen. De keerzijde van de medaille is echter dat brede toepassing van kant-en-klare oplossingen voor een homogener landschap zorgen, waardoor men eerder doelwit is en aanvalsmiddelen kunnen worden hergebruikt.

**Faillissement van wachtwoorden** De kwetsbaarheid van wachtwoordauthenticatie is inmiddels goed bekend. Bij herhaling wordt melding gemaakt van gekraakte websites waarbij wachtwoorden zijn buitgemaakt en gepubliceerd. Deze wachtwoorden zijn dan onveilig opgeslagen of zo zwak gekozen dat ze eenvoudig zijn te kraken. Dit werd onder meer duidelijk bij de diefstal van miljoenen gebruikersgegevens bij Adobe in september 2013.[78] Door de zwakke encryptie van de wachtwoorden, gekoppeld aan de onvercijferd opgeslagen hints die gebruikers hadden ingevoerd om het wachtwoord eenvoudig te kunnen herinneren, was het tamelijk eenvoudig om een deel van de wachtwoorden te reconstrueren. Soms was de hint het wachtwoord zelf.

Gebruikers kiezen hetzelfde wachtwoord of sterk gelijkende wachtwoorden voor meerdere websites,[79] vaak gekoppeld aan hetzelfde e-mailadres. Hierdoor is het kraken van één bron voldoende om toegang te krijgen tot meerdere accounts van dezelfde persoon.

Ondanks de bekende kwetsbaarheden blijft het wachtwoord populair. Hoewel grote cloudproviders steeds vaker overstappen op een vorm van tweefactorauthenticatie, lijkt dit bij kleinere organisaties nog zelden te gebeuren.

## Conclusie

De kwetsbaarheid van software en systemen blijft onverminderd groot. Dit is de technische achilleshiel voor het waarborgen van cybersecurity. Er is nog onvoldoende antwoord op dit probleem. Het aantal fouten (en daarmee het aantal kwetsbaarheden) in software is afhankelijk van de wijze waarop de software tot stand is gekomen. De omvang van het probleem kan worden teruggedrongen, bijvoorbeeld door aandacht te besteden aan concepten als security-by-design.

Cybercriminelen blijven oude en nieuwe kwetsbaarheden in standaardsoftware misbruiken. Basisprotocollen die voor het internet worden gebruikt, zoals BGP, DNS en SMTP, zijn intrinsiek kwetsbaar voor misbruik.

Het aantal aan internet verbonden apparaten, waaronder medische apparatuur, voertuigen, televisies en huishoudelijke apparaten, zal toenemen. De software in deze apparatuur zal beveiligingslekken blijven bevatten. Omdat verouderde software vaak al langer bekende kwetsbaarheden bevat die echter niet meer worden opgelost, kunnen cybercriminelen deze blijvend misbruiken. Hierdoor ontstaat een ICT-duurzaamheidsprobleem.

Toenemende technische kwetsbaarheden, de wijze waarop kwaadwillenden deze benutten en een gebrek aan kennis en hulpmiddelen maken het voor gebruikers steeds lastiger om zich te verweren tegen de dreigingen in een wereld die steeds afhankelijker wordt van ICT. «

78 h□p://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/ (geraadpleegd: juni 2014)

79 Zie h□p://www.csid.com/wp-content/uploads/2012/09/CS_PasswordSurvey_FullReport_FINAL.pdf

“MEDIA BESTEDEN BIJNA DAGELIJKS UITGEBREID AANDACHT AAN CYBERSECURITY”

# HOOFDSTUK 5 » WEERBAARHEID: MAATREGELEN

**Dit hoofdstuk richt zich op het weerbaarheidsaspect maatregelen en schetst de belangrijkste ontwikkelingen op dit gebied van de afgelopen periode. Maatregelen hebben tot doel de digitale weerbaarheid van individuen, organisaties en de samenleving te versterken. De beschrijvingen zijn gebaseerd op open bronnen en informatie die door diverse partijen beschikbaar is gesteld.**

## Bewustwording

Bewustwording van de risico's en het handelingsperspectief is een randvoorwaarde voor cybersecurity. Zonder bewustwording op alle niveaus (van bestuurders tot medewerkers en consumenten) zijn andere maatregelen minder effectief.

Het afgelopen jaar zijn op het gebied van cybersecurity verschillende internationale en nationale campagnes gevoerd. Voorbeelden zijn de Cyber Security Month[80] (oktober 2013, ENISA), Alert Online[81] (28 oktober - 5 november 2013), de Veilig bankieren-campagne[82] (NVB) en Safer Internet Day[83] (februari 2014, DigiBewust).

De Taskforce BID (Bestuur en Informatieveiligheid Dienstverlening) is op 13 februari 2013 voor een periode van twee jaar ingesteld om informatieveiligheid hoog op de agenda te krijgen bij bestuurders en topmanagement van alle overheidslagen. Dit in samenwerking met diverse publiek-private partijen. Ook wordt een Nationaal Commissaris Digitale Overheid ingesteld.

In vergelijking met de rest van Europa blijkt[84] dat Nederlanders relatief veel van internet gebruik maken. Dit gebeurt vaak via smartphones en tablets. Nederlanders hebben veel vertrouwen in het internet om online te bankieren en online aankopen te doen (88 procent in Nederland versus 70 procent in Europa). De awareness is in vergelijking met andere Europese landen hoger. Tegelijkertijd geeft slechts 65 procent (EU 46 procent) van de Nederlanders aan antivirussoftware te hebben geïnstalleerd.

Uit de Veiligheidsmonitor 2013[85] blijkt dat ongeveer 12,6 procent van de Nederlanders in 2013 een of meerdere malen slachtoffer is geweest van cybercrimedelicten (in 2012 12,1 procent). Dit betreft cybercrime in brede zin, dus ook zaken als cyberpesten en fraude bij online aankopen. Tegelijkertijd kent Nederland internationaal gezien een relatief beperkt aantal besmettingen. Dit bevestigt het vertrouwen dat Nederlandse burgers hebben in hun eigen digitale weerbaarheid.[86] De risicoperceptie onder Nederlanders is dan ook beperkt: tweederde van de burgers weet niet spontaan te noemen hoe er via internet misbruik van hun computer kan worden gemaakt. Wel is de behoefte aan informatie over cybersecurity erg groot.[87]

Reguliere media, zoals kranten en actualiteitenrubrieken, besteden bijna dagelijks uitgebreid aandacht cybersecurity. Deze aandacht heeft de potentie om zich te vertalen in verhoogde weerbaarheid.

## Nationale Cyber Security Strategie

Op 28 oktober 2013 is de tweede Nationale Cyber Security Strategie[88] (NCSS-2) gepresenteerd. Deze strategie bouwt voort op de eerste strategie uit 2011. Met de nieuwe strategie wordt ingezet op een veilig digitaal domein waarin kansen van digitalisering worden benut, dreigingen het hoofd worden geboden en fundamentele rechten worden beschermd. Daarbij wordt gezocht naar een wisselwerking tussen veiligheid, vrijheid en maatschappelijke groei en is de ambitie dat Nederland tot de wereldtop behoort op het terrein van cybersecurity. De doelstellingen van de NCSS-2 zijn:

- Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen;
- Nederland pakt cybercrime aan;
- Nederland investeert in veilige privacy bevorderende ICT producten en diensten;
- Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het digitale domein;
- Nederland beschikt over voldoende cybersecuritykennis en - kunde en investeert in ICT-innovatie om onze cybersecurity-doelstellingen te behalen.

80 h□p://cybersecuritymonth.eu/
81 h□ps://www.alertonline.nl/
82 'Hang op, klik weg, bel uw bank!' h□ps://www.veiligbankieren.nl/
83 h□p://www.saferinternetday.nl/
84 European Commission, Special Eurobarometer Cyber Security, 2013.
85 Vergaderjaar 2013-2014, bijlage bij Kamerstuk 28684, nr 400.
86 Microso□ Security Intelligence Report, Volume 15, 2013.
87 NCTV en DPC, « Rapportage Cyber security », november 2013.
88 Vergaderjaar 2013-2014, Kamerstuk 26643, nr 291.

Aan de strategie is tot 2016 een actieprogramma gekoppeld met 37 actiepunten die interdepartementaal en publiek-privaat worden gerealiseerd. Bij de totstandkoming van de strategie zijn ruim honderd publieke en private organisaties betrokken geweest.

Defensie Cyber Strategie De Defensie Cyber Strategie uit 2012 omvat zes speerpunten waarmee Defensie de komende jaren haar doelstellingen in het digitale domein zal verwezenlijken. In het afgelopen jaar is de cybercapaciteit van Defensie verder ontwikkeld. Defensie heeft aangekondigd het Defensie Cyber Commando versneld op te richten.[89] Op het gebied van offensieve cybercapaciteit stelt Defensie dat zij over de kennis en capaciteiten moet beschikken om ter ondersteuning van militaire operaties offensief op te treden in het digitale domein.

## Nationale cybersecuritynetwerken

Aan de hand van de eerste en de tweede cybersecuritystrategie worden in Nederland drie publiek-private samenwerkingsnetwerken ingericht:

- Het Nationaal Detectie Netwerk, gericht op het beter en sneller waarnemen van digitale gevaren en risico's;
- Het Nationaal Respons Netwerk, gericht op het versterken van de weerbaarheid van onze samenleving door gezamenlijke respons op cybersecurity-incidenten;
- Het Nationaal Expertise Netwerk,gericht op het effectiever en efficiënter delen van kennis en expertise op het gebied van cybersecurity.

## Cyberoefeningen

Oefeningen helpen medewerkers en organisaties te leren wat zij moeten en kunnen doen bij (dreigende) incidenten. Net als voorgaande jaren waren er diverse internationale cyberoefeningen, zoals Cyber Storm 4 (maart 2013), Cyber Coalition (november 2013), Oefening NSS (februari 2014) en @tomic 2014 (februari 2014). Ook binnen vitale sectoren vinden veelvuldig oefeningen plaats, zowel voor afzonderlijke als samenwerkende bedrijven. Een voorbeeld is de Cyber Flight oefening (maart 2013).

## Responsible disclosure

Responsible disclosure is het op een verantwoorde wijze verhelpen en openbaar maken van ICT-kwetsbaarheden. Dit gebeurt op basis van een door organisaties hiervoor zelf vastgesteld beleid en in samenspraak met de melder. Deze vorm van samenwerking met de ICT-community heeft vanaf begin 2013 vorm gekregen met de publicatie van de Leidraad Responsible Disclosure van het NCSC. Sinds de invoering hebben in Nederland ongeveer veertig organisaties een responsible-disclosurebeleid ingevoerd, waaronder de belangrijkste partijen in de vitale sectoren telecom en financiën. Het aantal meldingen lag in de rapportageperiode net onder de honderd, met sterke aanwijzingen dat dit komend jaar zal toenemen (zie bijlage 1). In het najaar 2014 zal de eerste voortgangsrapportage naar de Tweede Kamer worden gestuurd.

## Detectie en situational awareness

De aandacht voor cybersecurity verschuift van preventie naar detectie. De praktijk laat zien dat aanvallen niet buiten de deur zijn te houden; om tijdig en adequaat te reageren, zijn het detecteren van aanvallen en incidenten en een goed inzicht in de situatie van groot belang. Concepten als Security Operation Center, Threat Analysis en Situational Awareness winnen aan populariteit, zonder dat hiervan eenduidige definities bestaan of resultaten van zijn gedefinieerd. De verwachting is dat er de komende jaren meer eenduidigheid op het terrein van detectie zal worden bereikt.

**Statistieken Defensie**

Het Defensie Computer Emergency Response Team (DefCERT) waakt over de beveiliging van de netwerken van Defensie. Daartoe monitort en analyseert de eenheid digitale kwetsbaarheden, en adviseert en ondersteunt zij bij cyberincidenten. Een aantal resultaten uit de rapportageperiode:

- DefCERT hee ongeveer 22.000 stuks malware afgevangen op ongeclassi ceerde en Departementaal Vertrouwelijke computersystemen.
- Meer dan 600 hiervan zijn als incident in behandeling genomen. Daaronder bevonden zich meerdere malware-besme ingen waarbij (Defensie- en privé-)computers probeerden deel uit te maken van een botnet.
- DefCERT hee circa 11.500 portscans gedetecteerd die vanaf internet op het internet-koppelvlak met de Defensienetwerken werden uitgevoerd.
- Er zijn meer dan één miljoen binnenkomende, spam-gerelateerde e-mails onderschept (ongeveer 85.000 stuks per maand).
- Ook hee DefCERT per maand ongeveer 1.000 binnenkomende e-mails met een virus onderschept en in quarantaine gezet.

## Technologische maatregelen

Naast organisatorische maatregelen en samenwerking tussen organisaties en op landelijk niveau zijn technologische maatregelen van groot belang voor cybersecurity. De belangrijkste ontwikkelingen op dit gebied zijn hieronder samengevat.

Maatregelen naar aanleiding van DDoS-aanvallen De DDoS-aanvallen in april en mei 2013 hebben geleid tot een toename van DDoS-detecterende en mitigerende maatregelen. De afgelopen periode liet een toename zien van serviceproviders die zich specifiek richten op het opvangen van grootschalige DDoS-aanvallen, om zo hun online diensten ook tijdens en vlak na aanvallen te kunnen blijven verlenen. Steeds meer bedrijven maken gebruik van dergelijke diensten.

89 Vergaderjaar 2013-2014, Kamerstuk 33763, nr 1.

In het kader van de opsporing worden organisaties gestimuleerd aangifte te doen van een DDoS-aanval en ervoor te zorgen dat gegevens over de aanval als bewijsmateriaal worden vastgelegd. In bijlage 1 is meer informatie te vinden over de bij het NCSC gemelde DDoS-aanvallen.

**Statistieken grote multinational**
Enkele statistieken van een grote multinational die zijn infrastructuur 24 /7 monitort en bewaakt:

**Preventief worden per maand:**

» ongeveer 181.000 e-mails geblokkeerd vanwege spam, malware of phishing;
» 98 terabytes van/naar internet verstuurd, waarvan ongeveer 37.000 requests worden geblokkeerd;
» 185.000 virussen verwijderd;
» 60 patches uitgerold.

**In het kader van detectie worden per maand:**

» 500.000 events geregistreerd op de intrusion detection systemen;
» 34 events of interest gedetecteerd;
» 300 botnet besme□ing gedetecteerd.

Iedere maand worden ongeveer 73 security incidenten afgehandeld.

Gebruik IPv6 in Nederland groeit verder Met IPv6 is het eenvoudiger om gegevens tijdens transport te voorzien van beveiliging middels encryptie en authenticatie van data dan met IPv4. Een gebrekkige implementatie van IPv6 kan daarentegen ook tot kwetsbaarheid leiden. Het gebruik van IPv6 is de afgelopen periode, op basis van het IPv6-verkeer op AMS-IX,[90] bijna verdrievoudigd tot meer dan 12 Gbps.

Gebruik cryptogra□sche beveiligingsmaatregelen In het afgelopen jaar hebben grote cloudbedrijven het gebruik van cryptografische beveiligingsmaatregelen verder aangescherpt en versterkt. De Amerikaanse Electronic Frontier Foundation houdt een actueel overzicht van deze maatregelen (waaronder gebruik van HTTPS, StartTLS en versleuteling van verbindingen tussen datacenters) bij.[91]

Inzet tweefactorauthenticatie Steeds meer cloudbedrijven maken het mogelijk voor gebruikers om zich te authenticeren met behulp van tweefactorauthenticatiemiddelen. Banken passen dit principe al veel langer toe.

Bij deze middelen worden additionele verificatiemethodes gebruikt, zoals een sms-bericht. Een gebruiker moet én zijn wachtwoord kennen én in het bezit zijn van een fysiek object (bijvoorbeeld een mobiele telefoon of bankpas) om toegang te krijgen tot persoonlijke informatie. Deze middelen zorgen ervoor dat gebruikers minder kwetsbaar worden voor het uitlekken van wachtwoorden en maken misbruik op afstand minder eenvoudig.

Extra bescherming voor .nl-domeinnamen Naar aanleiding van incidenten met domeinnaamregistraties in de afgelopen periode zijn extra beschermingsmaatregelen mogelijk geworden. Het gaat om het telefonisch controleren van wijzigingen op domeinregistraties bij de eigenaar. De eigenaar van een domeinnaam heeft de keuze om deze maatregelen, tegen betaling, te activeren.[92]

DNSSEC is een andere manier om een domeinnaam te beveiligen. Bezoekers van een website kunnen hiermee verifiëren of ze ook daadwerkelijk bij een website uitkomen en niet worden omgeleid naar een malafide kopie. Sinds 15 mei 2012 is het in Nederland mogelijk domeinnamen te beveiligen met DNSSEC en is het voor iedere registrar mogelijk .nl-domeinnamen met DNSSEC aan te bieden.

ICT-beveiligingsassessments DigiD Op basis van de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van het NCSC heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de DigiD-aansluitnorm vastgesteld. In 2012 zijn de grootverbruikers van DigiD getoetst op basis van deze norm. In de rapportageperiode is in opdracht van de minister van BZK de ICT-beveiliging met betrekking tot de koppeling met DigiD van de overige afnemers getoetst. Externe auditors hebben deze toetsing uitgevoerd. Een deel van de organisaties die DigiD gebruikt, voldeed in 2013 niet aan alle normen. Door het assessmentproces te doorlopen, zijn de betrokken organisaties zich op bestuurlijk niveau bewuster geworden van het belang van informatiebeveiliging. Ook hebben zij verbeteringen doorgevoerd.

Veilig interne□en Mensen zijn met steeds meer en verschillende apparaten verbonden met het internet. Voor een gemiddelde gebruiker wordt het steeds lastiger om op alle apparaten passende maatregelen te nemen. Bewustwording van de risico's is een eerste stap, het aanpassen van gedrag en nemen van benodigde technische maatregelen zou het vervolg hierop moeten zijn. Het NCSC heeft in december 2013 een factsheet uitgebracht met daarin 10 vuistregels voor veilig internetten.[93] De regels zijn onder andere gericht op veilig gebruik van internet, WiFi en wachtwoorden.

90 h□ps://www.ams-ix.net/technical/statistics/s□ow-stats/ipv6-tra□c (7 april 2014).
91 h□ps://www.e□.org/deeplinks/2013/11/encrypt-web-report-whos-doing-what#crypto-chart (7 april 2014).
92 h□ps://www.sidn.nl/over-nl/domeinnaam-beschermen/ (7 april 2014).
93 h□ps://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-10-vuistregels-voor-veilig-interne□en.html

## Onderzoek

Voor een duurzame versterking van de digitale weerbaarheid van Nederland is onderzoek van groot belang, zowel toegepast als fundamenteel. Het kabinet en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) investeren samen in dit onderzoek. Dit op basis de Nationale Cyber Security Research Agenda, die toonaangevende onderzoekers op dit terrein hebben opgesteld. In de NCSRA staat de samenwerking tussen bedrijfsleven en kennisinstellingen centraal. De overheid stelt voor 2014 en 2015 6,4 miljoen euro beschikbaar voor onderzoek. Daarnaast is het afgelopen jaar internationaal intensiever samengewerkt op onderzoeksgebied.

## Onderwijs

Goed onderwijs is belangrijk voor duurzame weerbaarheid. Meerdere hogescholen, universiteiten en bedrijven hebben het afgelopen jaar opleidingen voor cybersecurity opgericht of versterkt. Om de pool van cybersecurity-experts te vergroten en de cybersecurityvaardigheden van gebruikers te versterken, slaan bedrijfsleven en overheid in 2014 de handen ineen in een Taskforce Cybersecurityonderwijs. Deze taskforce adviseert over het cybersecurity-onderwijsaanbod en zet zich in voor een beter aanbod van ICT-onderwijs binnen zowel het lager, hoger als professioneel onderwijs.

Daarnaast werken de Onderwijsinspectie en Surfnet aan het verhogen van de cybersecurity van onderwijsorganisaties zelf.

## Conclusie

Veel weerbaarheidsinitiatieven die in de vorige editie van het CSBN werden genoemd, zijn op dit moment gestart of al in uitvoering. De aandacht voor cybersecurity is in het afgelopen jaar opnieuw toegenomen, vaak door incidenten of nieuw ontdekte, ernstige kwetsbaarheden. Overheid en bedrijfsleven besteden meer aandacht aan maatregelen. Dit gebeurt steeds vaker in gezamenlijkheid. Voor thuisgebruikers blijft het lastig om zich adequaat tegen bestaande en nieuwe dreigingen te beveiligen.

Cybersecurity wordt steeds meer bezien binnen de bredere context van veiligheid, vrijheid en maatschappelijke groei. Met de toename het aantal afhankelijkheden en dreigingen groeit ook de voedingsbodem voor meer beschermingsmaatregelen. Het toegenomen bewustzijn, mede gegroeid door uitgebreide aandacht in de reguliere media, leidde in de afgelopen periode tot nieuwe initiatieven en aanvullende maatregelen op nationaal niveau en bij afzonderlijke organisaties. Voorbeelden zijn samenwerking in nationale netwerken, inrichting van technische maatregelen om DDoS-aanvallen tegen te gaan en gebruik van veiliger standaarden en oplossingen op organisatorisch niveau. Ook is er meer aandacht voor de noodzaak om de eindgebruiker voldoende toe te rusten op verantwoord gebruik van internet en zijn apparatuur. «

**Statistieken Belastingdienst**

De Belastingdienst beschikt over een Security Operations Center (SOC). Het SOC is verantwoordelijk voor het signaleren en opsporen van kwetsbaarheden in de operationele infrastructuur, het duiden van cyberdreigingen en het adviseren van tegenmaatregelen om bestaande risico's op te he□en. Tijdens calamiteiten fungeert het SOC als het Computer Emergency Response Team van de Belastingdienst. Tijdens de rapportageperiode:

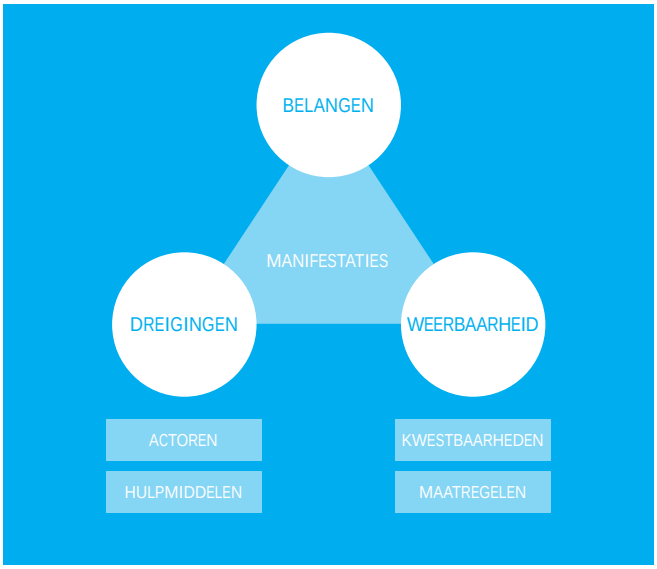
- zijn in de kantooromgeving van de Belastingdienst (ruim 35.000 werkplekken) circa 3.500 meldingen van virussen, 500 meldingen van hack- en cracktools en ruim 19.300 meldingen van het tegenhouden van kwaadaardige so□ware afgegeven;
- hee□ de eerstelijnsbescherming (□rewalls) ruim 297 miljard aanvallen en de tweedelijnsbescherming (Intrusion Detection and Prevention faciliteit) ruim 28.000 aanvallen tegengehouden;
- is er een signi□cante terugloop te zien van de hoeveelheid binnenkomende spam e-mails (van 92,1 procent in de voorgaande periode tot 69 procent in deze rapportageperiode) In de rapportageperiode werden op een totaal van 60 miljoen e-mails 46 miljoen spam-e-mails ontvangen;
- hee□ één DDoS-aanval ertoe geleid dat systemen tijdelijk niet beschikbaar waren. Hierna hee□ nog één DDoS-aanval geleid tot een beperkte beschikbaarheid, alle overige DDoS-aanvallen zijn afgevangen;
- zijn 177 security-incidenten geregistreerd, waarvan 14 'prio-1' incidenten. Al deze security-incidenten zijn door het SOC onderzocht en samen met de betre□ende platformteams opgelost;
- zijn vier responsible-disclosuremeldingen gedaan en opgelost. Geen van deze security-incidenten of kwetsbaarheden hee□ geleid tot een inbreuk op de integriteit en vertrouwelijkheid van de door de Belastingdienst beheerde gegevens.

“NEDERLAND IS EEN AANTREKKELIJK DOELWIT VOOR SPIONAGE”

# HOOFDSTUK 6 » MANIFESTATIES

**Een manifestatie is een daadwerkelijke aantasting van cybersecurity. Belangen worden geschaad omdat een dreiging manifest wordt en de weerbaarheid onvoldoende is. Hierbij kan opzet van een actor in het spel zijn, maar ook fouten van actoren of ongelukken kunnen leiden tot manifestaties. Dit hoofdstuk bevat de belangrijkste manifestaties die zich in deze rapportageperiode in binnen- en buitenland hebben voorgedaan en welke impact dit hee gehad op Nederland.**

Onderstaande tabel geeft een overzicht van de verschillende typen manifestaties met daarbij – indien van toepassing – de belangrijkste actor(en) en beoogde doelen.[94]




*Figuur 13. Samenkomst belangen, dreigingen en weerbaarheid in manifestaties*

| Type manifestatie | Belangrijkste actor(en) en beoogde doelen |
|---|---|
| **Aanval gericht op informatie** | |
| **Digitale spionage** | » Staten: digitale spionage van andere staten en private organisaties<br>» Private organisaties: economische spionage van andere private organisaties |
| **Diefstal/verkrijgen van informatie, eventueel voor publicatie of verkoop** | » Beroepscriminelen: geldelijk gewin<br>» Hacktivisten: maken van een publiek statement of schade toebrengen aan anderen<br>» Cybervandalen: aantonen dat het kan of voor de lol<br>» Cyberonderzoekers: aan de kaak stellen zwakke beveiliging<br>» Private organisaties: geldelijk gewin<br>» Interne actoren: kwetsbaarheden inzichtelijk maken of schade toebrengen aan anderen |
| **Manipulatie van informatie** | » Beroepscriminelen: geldelijk gewin |
| **Aanval gericht op ICT** | |
| **Defacement** | » Hacktivisten: maken van een publiek statement, verspreiden propaganda<br>» Scriptkiddies, cybervandalen: aantonen dat het kan of voor de lol |
| **Verstoring van ICT** | » Staten: inzet van o ensieve cybercapaciteiten in statelijke con icten<br>» Terroristen: als wapen tegen fysieke doelen of als ondersteuning voor terroristische activiteiten<br>» Beroepscriminelen: afpersing en als basis of a eiding voor aanvallen waarbij zij nancieel gewin hebben<br>» Hacktivisten, scriptkiddies en cybervandalen: de verstoring is een doel op zich, omdat het kan of voor de lol<br>» Interne actoren: de verstoring is een doel op zich |
| **Overname van ICT** | » Beroepscriminelen: geldelijk gewin, afpersing, versturen van SPAM en phishing mails<br>» Hacktivisten: hosten van gegevens om propaganda te verspreiden<br>» Scriptkiddies en cybervandalen: aantonen kwetsbaarheden, omdat het kan of voor de lol |
| **Verstoring of uitval van ICT door natuurlijke of technische gebeurtenissen of door menselijk falen** | |

*Tabel 3. Typen manifestaties*

94 Een meer gedetailleerde beschrijving van de actoren, hun motieven en beoogde doelen is te vinden in hoofdstuk 2.

## Aanval gericht op informatie

Dat ICT een cruciale rol in de samenleving speelt, is onder meer terug te zien in de manier waarop informatie wordt geproduceerd, verzameld en gedeeld. Deze informatie is in veel gevallen niet alleen van grote waarde voor de eigenaar, maar ook voor kwaadwillenden. Cyberaanvallen kunnen worden ingezet om toegang te krijgen tot deze informatie. Verkregen informatie kan echter ook weer worden gebruikt om een aanval uitvoeren.

Digitale spionage Uit onderzoek van de AIVD en MIVD blijkt dat buitenlandse overheden op heimelijke wijze proberen gevoelige informatie in Nederland te verzamelen. Naast staten maken ook private organisaties zich schuldig aan digitale spionage, al dan niet door het inhuren van beroepscriminelen. De Hidden Lynx-groep zou volgens Symantec worden ingehuurd voor bedrijfsspionage,[95] het wordt niet waarschijnlijk geacht dat ze de gestolen informatie zelf verwerkt of gebruikt voor direct financieel gewin. De APT-groepering 'Icefog' zou zich volgens Kaspersky vooral richten op kapen van gevoelige documenten, gebruikersnamen en wachtwoorden van met name overheidsinstanties en bedrijven in de militaire en maritieme sector, telecomoperators, industrie en hightech en massamediabedrijven.[96]

> *"Bij het verzenden van phishing-e-mails spelen aanvallers slim in op actuele ontwikkelingen."*

Hoewel manifestaties van dergelijke groeperingen in Nederland nog niet zijn waargenomen, is het voorstelbaar dat deze nog volgen. Nederland is met zijn open samenleving en grote technische en wetenschappelijke kennis en zijn economische positie een aantrekkelijk doelwit voor spionage.[97] Bovendien kan het maanden en soms zelfs jaren duren voordat een Advanced Persistent Threat (APT) wordt ontdekt.

Advanced Persistent Threats Tijdens een APT-aanval kan een aanvaller vertrouwelijke informatie verzamelen of voorbereidingen treffen om de werking van vitale componenten te kunnen verstoren. Weinig APT-aanvallen zijn daadwerkelijk zo geavanceerd, maar slagen juist door een gebrek aan beveiliging en detectiemiddelen bij de doelwitten. Daar komt bij dat in veel aanvallen ogenschijnlijk lukraak exploits worden ingezet in de hoop op een infectie.

Begin 2014 onthulde Kaspersky het bestaan van een APT, genaamd Careto of the Mask, die zich al sinds 2007 zou bezighouden met digitale spionage. De APT zou in al die jaren rond de 380 slachtoffers in 31 landen hebben gemaakt.[98] De gebruikte toolkit was zeer complex, geschikt voor uiteenlopende platformen en maakte gebruik van verregaande technieken om niet opgemerkt te worden. Eenmaal binnen verzamelde Careto allerhande informatie, zoals bestanden, encryptiesleutels, netwerkverkeer en toetsaanslagen. Gezien de code zouden de auteurs van oorsprong Spaanstalig zijn.

APT's blijven een serieuze dreiging. Ontdekking van een aanval leidt mogelijk wel tot het mislukken van die betreffende aanval, maar vooralsnog niet tot het ontmantelen van de verantwoordelijke organisaties. Het bewustzijn over dergelijke aanvallen is de afgelopen periode door een aantal waargenomen incidenten toegenomen.

Diefstal van informatie Diefstal van informatie[99] is het ontvreemden van vertrouwelijke of waardevolle informatie. Zowel actoren van buiten als interne actoren vormen een dreiging.

In de rapportageperiode is een aantal grootschalige datadiefstallen aan het licht gekomen die plaatsvonden vanaf met malware besmette computers die onderdeel waren van een botnet. Zo zijn er meerdere varianten van het Pony-botnet ontdekt waarbij honderdduizenden tot enkele miljoenen gebruikersnamen en wachtwoorden werden buitgemaakt voor websites als Twitter, Facebook, Google en Yahoo.[100] In Duitsland werden de e-mailadressen en wachtwoorden van maar liefst 16 miljoen mensen buitgemaakt door middel van een botnet.[101] Hier zaten ook ongeveer 50.000 Nederlandse e-mailadressen bij.[102]

Bij andere aanvallen werd ingebroken op een website of database. In oktober 2013 werd bekend gemaakt dat een hack bij Adobe ervoor heeft gezorgd dat de gegevens van ten minste 38 miljoen klanten waren gelekt.[103]

In deze rapportageperiode is het opnieuw voorgekomen dat hacktivisten en onderzoekers gegevens ontvreemdden en publiceerden. Bij een aanval op het zakenblad Forbes in februari 2014 werden onder meer de gegevens (naam, e-mailadres, gebruikersnaam, registratiedatum en gehasht wachtwoord) van 1 miljoen lezers, waaronder bijna duizend Nederlanders, buitgemaakt en online gezet. De Syrian Electronic Army (SEA), een groep die het Syrische regime van president Assad steunt, eiste deze aanval op.[104]

95 http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf
96 http://www.securelist.com/en/downloads/vlpdfs/icefog.pdf
97 AIVD, https://www.aivd.nl/onderwerpen/cyberdreiging/cyberaanvallen/cyberspionage/
98 Unveiling Careto The Masked APT, Kaspersky lab.

99 Informatie kan in juridische zin niet worden gestolen, er is sprake van het opheffen van de exclusiviteit van informatie omdat de informatie niet wordt weggenomen.
100 http://www.reuters.com/article/2014/02/24/us-bitcoin-security-idUSBREA1N1JO20140224 en http://threatpost.com/pony-botnet-controller-holds-2-million-stolen-and-weak-credentials/103096 http://news.techworld.com/security/3456099/pony-botnet-plunders-650000-web-logins-in-days-trustwave-reports/
101 http://webwereld.nl/beveiliging/80993-botnet-kaapt-16-miljoen-e-mailadressen-en-wachtwoorden
102 http://www.digibewust.nl/nieuws/botnet-stal-ook-nederlandse-gegevens
103 http://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/ Er wordt ook wel gesproken over 150 miljoen gebruikers, maar dit bericht is nooit bevestigd door Adobe.
104 https://www.security.nl/posting/378473/Website+en+Twitteraccount+Forbes+gekaapt

In augustus 2013 kaartten Australische onderzoekers een aantal lekken in de Snapchat app aan bij het bedrijf dat deze app levert. Volgens de onderzoekers werden hun bevindingen genegeerd, waarop ze in december de details onthulden en een exploit publiceerden waarmee de kwetsbaarheid te misbruiken is. Iemand heeft deze exploit vervolgens gebruikt om de gegevens (een combinatie van gebruikersnaam en telefoonnummer en de regio waar de gebruiker zich bevindt) van 4,6 miljoen Snapchat-gebruikers in een database online te zetten.[105]

**Afpersing door te dreigen met publicatie**
Er wordt ook geprobeerd om geld te verdienen door te dreigen met publicatie van gestolen gegevens. De Rex Mundi groepering hee deze vorm van afpersing meerdere malen ingezet. In juli 2013 versche e deze groep zich toegang tot de klantendatabase (namen, adresgegevens, e-mailadressen, telefoonnummers, gebruikersnamen en wachtwoorden) van Websolutions, een Italiaanse hostingprovider. De aanvallers persten de hostingprovider vervolgens af. Toen het bedrijf niet op hun eisen inging, publiceerden ze de gegevens van meer dan 60.000 klanten.[106] In datzelfde jaar zouden onder andere het Belgische kabeltelevisiebedrijf Numericable, het Canadese uitzendbureau Drake International en de Belgische kredietverstrekker Buy zijn afgeperst door Rex Mundi.[107] Een jaar eerder werd het Nederlandse uitzendbureau Accord al getro en door een hacker met het alias Rex Mundi.[108] Het is niet ondenkbaar dat Nederlandse bedrijven in de toekomst ook slachto er worden van dergelijke vormen van afpersing.

### Manipulatie van informatie

Manipulatie van informatie gaat een stap verder dan het ontvreemden van vertrouwelijke of waardevolle informatie: de informatie waar toegang tot wordt verschaft, wordt gemuteerd of vernietigd.

Manipulatie van informatie manifesteert zich voor een belangrijk deel nog steeds als digitale fraude en dan voornamelijk fraude met internetbankieren. Ondanks dat de Nederlandse Vereniging van Banken en Betaalvereniging Nederland bekend maakten dat de schade door fraude met internetbankieren in 2013 met 72 procent is gedaald ten opzichte van 2012. Dit heeft onder andere te maken met het blokkeren van bankpassen buiten Europa en met de verbeterde detectie van fraude. Toch zien de banken nog steeds een onverminderd hoge dreiging van deze vorm van fraude. Dit heeft te maken met het blijvend grote aantal fraudepogingen.[109]

Een Nederlandse drugsbende kon door manipulatie van informatiesystemen van verladers waarschijnlijk twee jaar lang tot hun aanhouding medio 2013 containers met legitieme lading waarin drugs verstopt zaten, ongemerkt uit de Antwerpse haven smokkelen, voordat de rechtmatige transporteur deze kwam ophalen.[110]

In april 2013 verscheen een rapport van Kaspersky Lab waarin werd geschreven over Winnti, een collectief van Chinese hackers die malware in online games hadden binnengesmokkeld om in-game currencies en mogelijk ook accountinformatie te stelen.[111] In februari 2014 zorgde een cyberaanval voor problemen met bitcoin toen aanvallers probeerden het systeem te manipuleren door valse data over transacties te versturen.[112]

**Fritzbox gebruikers slachto er van telefoniefraude[113]**
In februari 2014 bleken verschillende klanten van XS4ALL de dupe te zijn geworden van telefoniefraude. Bij deze klanten werd zonder dat ze het zelf wisten gebeld naar dure buitenlandse telefoonnummers waarna zij met hoge rekeningen geconfronteerd werden. Dit bleek mogelijk door een kwetsbaarheid die zich bevond in de Fritzbox modems van deze klanten. Ook klanten met Fritzbox modems bij andere providers bleken slachto er te zijn geworden van deze vorm van fraude.

Dit voorbeeld illustreert de kwetsbaarheid van apparaten die verbonden zijn met internet. In dit geval was het mogelijk om de modems te patchen, waarmee de kwetsbaarheid werd verholpen. In het katern Duurzaamheid van ICT wordt nader ingegaan op apparaten die met internet verbonden zijn.

## Aanval gericht op ICT

Naast informatie die staat opgeslagen op ICT-systemen, kunnen ook de systemen zelf doelwit zijn van aanvallers. Door de werking van systemen te verstoren of door de controle hierop over te nemen, kan veel schade worden aangericht.

Defacement Een defacement is een aanval waarmee de inhoud van een bestaande webpagina wordt veranderd, met als primair doel een boodschap te verspreiden via de ICT-infrastructuur van het slachtoffer.

Een aantal defacements werd opgeëist door de hacktivistische groepering Anonymous. Zo zorgden hackers onder de vlag van Anonymous vanuit Indonesië voor defacements van honderden websites van de Australische overheid, naar eigen zeggen in reactie op berichtgeving van spionage door Australië. Ook hackten hackers onder de vlag van Anonymous meer dan 38 websites van de Filipijnse overheid.[114]

105 h ps://www.security.nl/posting/378519/Gegevens+1+miljoen+Forbes-lezers+op+internet+gelekt?channel=rss
106 h ps://www.security.nl/posting/361686/Snapchat+lekt+telefoonnummers+en+namen+gebruikers en
107 h ps://www.security.nl/posting/373975/Gegevens+4,6+miljoen+Snapchat-gebruikers+gelekt
108 h ps://www.security.nl/posting/37053/Gegevens+4_000+Nederlandse+uitzendkrachten+online
109 h p://www.nvb.nl/nieuws/2014/2636/fraude-betalingsverkeer-opnieuw- ink-gedaald.html
110 h p://www.gva.be/regio-antwerpen-stad/drugsma a-neemt-computers-haven-over.aspx
111 h ps://www.securelist.com/en/downloads/vlpdfs/winnti-more-than-just-a-game-130410.pdf
112 h p://www.coindesk.com/massive-concerted-a ack-launched-bitcoin-exchanges/
113 h ps://blog.xs4all.nl/2014/02/06/telefoniemisbruik/
114 h p://thehackernews.com/2013/11/rise-in-website-defacement-a acks-by.html

Hackers uit naam van de Syrian Electronic Army (SEA) zorgden in oktober 2013 voor de defacements van drie Syrische overheids- en honderden commerciële websites.[115] Ook de Microsoft Office-blog werd slachtoffer van een defacement uit naam van de SEA.[116]

Ook dichter bij huis zijn er defacements geweest. Zo werden verschillende Duitse websites gedefaced uit naam van de hackersgroep 'Algeria to the core' en werd in juli 2013 de Belgische domeinregistry DNS.BE slachtoffer.[117] Nederlandse websites lijken in de rapportageperiode bespaard te zijn gebleven van dergelijke aanvallen. In oktober leek de website Leaseweb gedefaced te zijn geweest, maar het bleek dat bezoekers werden omgeleid naar een andere webpagina omdat er een ongeoorloofde aanpassing in DNS-servers had plaatsgevonden.

Verstoring van ICT De verstoring van ICT is erop gericht om de beschikbaarheid van de informatievoorziening, al dan niet langdurig, te schaden. Kwaadwillenden gaan innovatief te werk bij het toepassen van nieuwe technieken op verschillende lagen van netwerken. In Oekraïne zijn gericht stukken ICT-infrastructuur verstoord, waarbij zowel kabels fysiek zijn beschadigd als cyberaanvallen zijn gebruikt.[118]

Na de reeks DDoS-aanvallen op banken in het voorjaar van 2013, zijn verschillende andere organisaties in Nederland ook slachtoffer geworden van deze aanvalsvorm. Onder meer DigiD, gemeentes, politie en onderwijsinstellingen werden doelwit.

Het NCSC registreerde in de afgelopen rapportageperiode aanmerkelijk meer DDoS-aanvallen dan het jaar ervoor (zie bijlage 1), en ook bijna de helft van het aantal beveiligingsadviezen was gericht op kwetsbaarheden in software die misbruikt kunnen worden voor denial-of-service-aanvallen.

Opvallend was een aantal DDoS-aanvallen met een enorme bandbreedte. Zo maakte beveiligingsbedrijf Cloudflare in februari bekend dat het bij een klant een DDoS-aanval had gemitigeerd die pieken kende tot nagenoeg 400 Gbps.[119] Ook Prolexic Technologies en Verizon signaleerden bij DDoS-aanvallen een significante toename in bandbreedte.[120] Lees voor meer informatie over deze nieuwe ontwikkeling in DDoS-aanvallen hoofdstuk 3.

**Afpersing door (te dreigen met) DDoS-aanvallen**
Eerder in dit hoofdstuk werd al gesproken over cyberafpersing, waarbij wordt gedreigd buitgemaakte informatie te publiceren. Een andere vorm van cyberafpersing is het dreigen met het verstoren van ICT (platleggen van complete bedrijfssystemen of websites). Dit heeft in de rapportageperiode ook bij Nederlandse organisaties gespeeld. Van verschillende organisaties werd geld geëist onder dreiging met een DDoS-aanval. In Engeland heeft deze vorm van criminaliteit al geleid tot een veroordeling, in december 2013 werden twee mannen veroordeeld tot 5 jaar gevangenisstraf voor het afpersen van een online casino. Ze dreigden door middel van een DDoS-aanval de website plat te leggen en eisten de helft van de aandelen van het bedrijf.[121]

Ransomware, malware waarmee de computer van een slachtoffer ontoegankelijk wordt gemaakt, blijft slachtoffers maken. Lees voor meer informatie het verdiepingskatern 'Ransomware en cryptoware'.

Overname van ICT Bij overname van ICT verkrijgt een actor de controle over ICT-systemen van een doelwit, met het doel om de resources te misbruiken.

Ook hier viel de Syrian Electronic Army (SEA) deze rapportageperiode op. Ze hebben onder meer blog- en Twitteraccounts van bekende organisaties zoals van de Associated Press, Reuters, Microsoft en The New York Times overgenomen. Ook eisten ze een aanval op waarbij de officiële website, het Twitteraccount en Facebookprofiel van Barack Obama werden overgenomen.

115 http://news.softpedia.com/news/Three-Government-Websites-from-Syria-Hacked-and-Defaced-396126.shtml
116 http://www.tech365.nl/microsoft-office-blog-gehackt-door-syrian-electronic-army/
117 http://blog.trendmicro.com/trendlabs-security-intelligence/certain-german-websites-defaced-on-april-fools-day/ en http://www.ispam.nl/archives/33742/website-dns-be-ook-gehackt
118 Rusland verbiedt kritische websites, NRC Handelsblad 14 maart 2014 en Top Ukrainians Accusing Russia of an Invasion, The New York Times 1 maart 2014 en Ukraine braces for cyber offensive, Jane's International Defense Review, 1 april 2014.
119 http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack en http://krebsonsecurity.com/2014/02/the-new-normal-200-400-gbps-ddos-attacks/
120 http://www.prolexic.com/news-events-pr-threat-advisory-ddos-ntp-amplification.html en http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf
121 http://www.theinquirer.net/inquirer/news/2320104/two-men-jailed-for-cyber-blackmail-threats

**Persoonlijke afpersing en gerichte datagijzeling relevante nieuwe dreiging**

In mei 2014 deed de Nationale Politie simultaan tientallen huiszoekingen bij Nederlandse gebruikers van Blackshades. Met deze criminele malware worden computers op afstand gemanipuleerd. In het najaar werd al een Ro□erdammer opgepakt die met Blackshades webcambeelden had verzameld van meer dan duizend nietsvermoedende slachto□ers. Hij plaatste compromi□erende foto's op een persoonlijke Facebook-account en verwijderde belangrijke bestanden van slachto□ers.[122] Door de gebruiksvriendelijkheid van deze malware is in het geheel geen bijzondere computerkennis vereist bij de dader. De laatste Blackshades-versie maakt het ook eenvoudig om mensen op afstand onder druk te ze□en. Met een druk op de knop worden persoonlijke bestanden versleuteld, waarna een standaard-afpersbericht op het scherm van het slachto□er wordt getoond. Waar ransomware zich richt op brede verspreiding (schot hagel), kan Blackshades gebruikt worden om een speci□eke computer(gebruiker) te benaderen. Dit maakt gerichte datagijzeling tot een relevante dreiging.

In de rapportageperiode zijn er meerdere gevallen geweest waarin internetgebruikers via advertentiesites geïnfecteerd zijn geraakt met malware waarmee toegang tot de besmette systemen kan worden verkregen. Waar gebruikers voorheen nog op een advertentie moesten klikken, is nu het bezoeken van een website met besmette advertentie al voldoende om besmet te raken. Als gebruiker merk je vaak ook niets van de besmetting.[123] In haar jaarrapport 2013 noemt ENISA deze 'drive-by-downloads' de grootste dreiging op internet.[124]

Bij het verzenden van phishing-e-mails spelen aanvallers slim in op actuele ontwikkelingen. Toen bekend werd dat de Rabobank met een opvolger van de Random Reader zou komen, stuurden internetcriminelen valse e-mails over deze Rabo Scanner.[125] De Belastingdienst waarschuwde ook voor een golf aan phishing-e-mails in de periode waarin weer belastingaangifte kon worden gedaan.[126] Verder was er een phishing-e-mail in omloop waarin aandacht werd gevraagd voor het einde van de ondersteuning van Windows XP.[127]

## Natuurlijke of technische gebeurtenissen en menselijk falen

Naast de incidenten die voortkomen uit bewust menselijk handelen, kunnen ook natuurlijke of technische gebeurtenissen en menselijk falen leiden tot verstoringen. In deze paragraaf worden voorbeelden gegeven van dergelijke manifestaties uit de rapportageperiode.

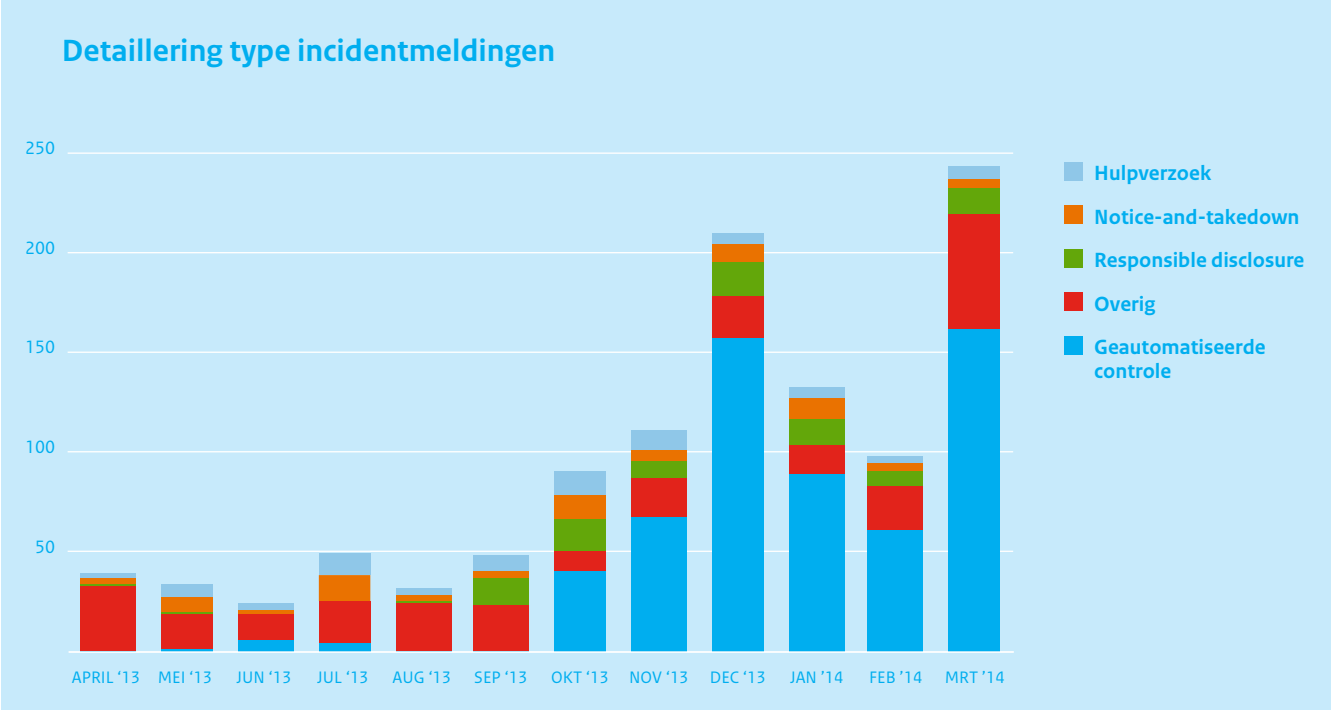
**Verstoring en uitval van ICT door natuurlijke of technische gebeurtenissen** In de rapportageperiode zijn verschillende systemen en datacenters uitgevallen door capaciteitsgebrek, natuurrampen of uitval van de elektriciteitsvoorziening. Het datacenter van Easynet op Schiphol lag in oktober 2013 deels plat door een stroomstoring. Veel bedrijven en websites, waaronder hostingprovider Argeweb, hadden hier last van.[128] Stroomuitval in een datacenter van een van de grootste verwerkers van betalingstransacties zorgde ervoor dat Canadezen hun VISA creditcard urenlang niet konden gebruiken.[129]

Ook deze rapportageperiode werd zichtbaar dat uitval bij een derde partij waarvan een organisatie afhankelijk is, grote gevolgen voor de eigen bedrijfsvoering kan hebben. Een technische storing bij KPN zorgde in oktober 2013 voor problemen bij Dienst Uitvoering Onderwijs (DUO). Diverse systemen van DUO werden door de storing platgelegd waardoor studenten niet konden inloggen op 'Mijn DUO' en medewerkers van de uitvoeringsorganisatie van OC&W niet in staat waren het studiefinancieringssysteem te raadplegen.[130]

**Menselijk falen** Een verstoring of uitval van ICT kan ook plaatsvinden doordat mensen fouten maken. In Nieuw-Zeeland werd hierdoor een netwerkcrash bij een van de ministeries veroorzaakt.[131] De Nasdaq beurs heeft in oktober 2013 enige tijd stilgelegen door een menselijke fout.[132]

Menselijk falen kan ook leiden tot het onbedoeld lekken van gegevens. In Nederland zijn hier meerdere voorbeelden van gezien. De Consumentenbond heeft in maart 2014 bijvoorbeeld een onjuiste e-mailverzending aan 473 consumenten uitgestuurd waardoor de persoonsgegevens (opzeggingsbevestigingen met naam-, adres- en woonplaatsgegevens en eventueel een rekeningnummer met daarbij het geldbedrag dat nog betaald, geïncasseerd of teruggestort moest worden) van 142 ex-leden zijn gelekt.[133] In diezelfde maand werd bekend dat Vodafone via de Telefoongids de telefoonnummers van klanten heeft gelekt die hier niet in wilden worden opgenomen, terwijl klanten die hun nummer wel vermeld wilden hebben niet werden opgenomen. Vodafone wijt dit aan een combinatie van technische en menselijke fouten.[134]

122 h□p://tweakers.net/nieuws/93173/ach□ienjarige-nederlander-ze□e-via-webcam-gestolen-naaktfotos-online.html
123 h□p://www.consuwijzer.nl/nieuws/computervirus-verspreid-grote-en-populaire-nederlandse-websites
124 h□p://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats
125 h□ps://www.rabobank.nl/particulieren/servicemenu/nieuws/rabobank_nieuws/valse_email_rabo_scanner
126 h□p://webwereld.nl/beveiliging/81522-phishingmail-vanaf-noreplybelastingdienst-nl
127 h□ps://www.ncsc.nl/actueel/nieuwsberichten/let-op-windows-xp-phishing-e-mail-in-omloop.html
128 h□p://tweakers.net/nieuws/91624/datacenter-easynet-ligt-deels-plat-door-stroomstoring.html
129 h□p://www.datacenterknowledge.com/archives/2013/01/28/data-center-outage-cited-in-visa-downtime-across-canada/
130 h□p://www.computable.nl/artikel/nieuws/outsourcing/4912359/1276946/mainframestoring-legt-duo-deels-plat.html en h□p://www.computable.nl/artikel/nieuws/overheid/5020424/1277202/duo-claimt-diverse-schades-na-kpnstoring.html
131 h□p://www.nzherald.co.nz/technology/news/article.cfm?c_id=5&objectid=11123875
132 h□p://www.foxbusiness.com/markets/2013/10/29/nasdaq-su□ers-data-service-outage-impacting-indexes-options/
133 h□ps://www.security.nl/posting/380598/Consumentenbond+lekt+persoonsgegevens+ex-leden
134 h□ps://www.security.nl/posting/381613/Vodafone+lekte+telefoonnummers+klanten+via+Telefoongids




*Figuur 14. Typen incidentmeldingen voor periode april 2013 tot en met maart 2014*

Aantallen afgehandelde incidenten Het aantal incidentmeldingen dat het NCSC in de periode van april 2013 tot maart 2014 afhandelde ligt beduidend hoger dan het aantal in de vorige rapportageperiode. Dit is echter voor een groot deel te verklaren door de automatisering van incidentmeldingen die het NCSC uitstuurt (zie figuur 14). Er is echter ook een effect te zien van het gebruik van de Leidraad Responsible Disclosure.

| Categorie | Omschrijving |
|---|---|
| Hulpverzoek | Verzoek van (inter)nationale partijen richting Nederlandse internetserviceproviders om te ondersteunen bij het bestrijden van cyberincidenten die hun oorsprong vinden in Nederland. |
| Notice-and-takedown | Verzoek van een Nederlandse □nanciële instelling bij het bestrijden van phishingaanvallen die zich richten op deze instelling en hun oorsprong (veelal) vinden in het buitenland. |
| Responsible disclosure | Het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie verhelpen en openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid. |
| Overig | Alle incidenten die niet onder één van de andere categorieën kunnen worden geschaard. |
| Geautomatiseerde controle | Geautomatiseerde controles van broninformatie (infecties, mala□de systemen) tegen bij NCSC bekende organisaties op basis van IP-adres, AS-nummer en domeinnaam. |

*Tabel 4. Incidentcategorieën*

Per kwartaal verwerkt het NCSC dus steeds meer incidentmeldingen. Exclusief de geautomatiseerde controles is dit in de rapportageperiode van dit CSBN opgelopen van 89 in het tweede kwartaal van 2013 tot 163 in het eerste kwartaal van 2014. Opvallend daarbij is dat het aandeel incidentenmeldingen uit de private sector langzaam begint toe te nemen. Terwijl in de periode van het CSBN-3 37 procent van alle incidentmeldingen betrekking had op de private sector, is dit in de periode van dit CSBN gegroeid naar 46 procent van alle meldingen. Een oorzaak hiervan kan liggen in de steeds verdergaande samenwerking van het NCSC met en bekendheid bij private partijen en de rol die het NCSC vervult bij het afhandelen van responsible disclosure meldingen. In bijlage 1 wordt dieper ingegaan op deze en andere gegevens over incidenten.

## Conclusie

De impact van cyberaanvallen houdt niet op bij de landsgrenzen. Dit geldt bijvoorbeeld voor de verspreiding van malware zoals ransomware. Van bepaalde manifestaties die hebben plaatsgevonden én uitsluitend impact hebben gehad in het buitenland, is het wel voorstelbaar dat deze ook in Nederland plaats (zullen) vinden. In andere gevallen, zoals bij mobiele malware, lijkt de dreiging wereldwijd juist toe te nemen, terwijl er in Nederland nog weinig wordt opgemerkt. Het gebruik van malware komt overigens bij veel verschillende manifestaties terug en kan dan ook worden ingezet om informatie te achterhalen of om systemen te verstoren.

In de afgelopen rapportageperiode vonden opvallend veel grote datadiefstallen en datalekken plaats. Vaak werden hier botnets voor ingezet, waarbij ook Nederlandse gebruikers slachtoffer werden. Actoren gingen ook gerichter te werk en maakten gebruik van specifieke kwetsbaarheden om zich toegang tot informatie te verschaffen. Misbruik van en door interne medewerkers of ondernemers is een zeer reële dreiging geworden.

Fraude met internetbankieren is in Nederland aanzienlijk gedaald, ondanks het blijvend grote aantal pogingen. Gedurende de rapportageperiode zijn DDoS-aanvallen in aantal en grote toegenomen. Ook Nederlandse instellingen, zoals banken en overheidsorganisaties, waren hiervan slachtoffer.

Zorgwekkend is de ontwikkeling van drive-by-downloads, waarbij alleen het bezoeken van een website met besmette advertenties voldoende is om malware binnen te halen. Ook phishing mails blijven een belangrijke bron voor malwarebesmettingen. Hacktivisten kwamen deze rapportageperiode veelvuldig in het nieuws, voornamelijk met de publicatie van gestolen gegevens en defacements.

Ook technische en natuurlijke gebeurtenissen en menselijke fouten leiden tot manifestaties. Verstoringen en uitval van ICT en het lekken van gegevens zijn helaas niet te voorkomen, ook niet wanneer zorgvuldig en professioneel wordt gehandeld en er aandacht is voor preventieve maatregelen.

Het aantal incidentenmeldingen, zoals hulpverzoeken en notice-and-takedonws, dat het NCSC in de periode van dit CSBN afhandelde ligt beduidend hoger dan het aantal in het vorige CSBN. Per kwartaal verwerkt het NCSC steeds meer incidentmeldingen. Exclusief de geautomatiseerde controles is dit in de rapportageperiode van dit CSBN opgelopen van 89 in het tweede kwartaal van 2013 tot 163 in het eerste kwartaal van 2014. Opvallend daarbij is dat het aandeel incidentenmeldingen uit de private sector langzaam begint toe te nemen. Terwijl in de periode van het CSBN-3 37 procent van alle incidentmeldingen betrekking had op de private sector, is dit in de periode van dit CSBN gegroeid naar 46 procent van alle meldingen.

> *"Opvallend was een aantal DDoS-aanvallen met een enorme bandbreedte."*

Inzicht in dreigingen en actoren De tabel op pagina 61 geeft een overzicht van de relevantie van dreigingen die van de verschillende actoren uitgaan om de doelwitten overheden, private organisaties en burgers aan te vallen.

Ten opzichte van het vorige Cybersecuritybeeld is voor een aantal combinaties het dreigingsniveau gewijzigd. Wanneer het gelijk is gebleven, kunnen de omstandigheden die leiden tot het vaststellen van de relevantie van de dreiging overigens wel gewijzigd zijn. De legenda onderaan de tabel geeft aan wanneer deze relevantie op hoog, midden of laag wordt ingeschat.

Voor overheden zijn in de afgelopen periode digitale spionage door statelijke actoren en verstoring van ICT, met name via DDoS-aanvallen, door beroepscriminelen de meest relevante dreigingen geweest.

Beroepscriminelen lijken zich met hun activiteiten overigens minder op overheden te richten en meer op private organisaties en burgers. Ook de dreiging van cybervandalen en scriptkiddies is de afgelopen periode voor overheden minder relevant geworden. Overname van ICT door hacktivisten is voor overheden relevanter geworden gezien soortgelijke enkele incidenten in het buitenland.

Voor private organisaties is de dreiging door beroepscriminelen relevanter geworden zoals afpersing door (te dreigen met) DDoS-aanvallen of ransomware-varianten. Ook is de dreiging van digitale spionage (met name door statelijke actoren en beroepscriminelen) toegenomen. Gevallen van bedrijfsspionage door private partijen zijn de afgelopen periode in Nederland niet waargenomen, zodat deze dreiging minder relevant is geworden.

Voor burgers ten slotte is met de dreiging vanuit beroepscriminelen het afgelopen jaar relevanter geworden. Door de grote datadiefstallen worden naast private organisaties ook burgers vaak getroffen. Verstoring (cryptoware) en overname (ransomware en botnets) van ICT hebben beide een hoge relevantie. Het commercieel gebruik (en misbruik) van persoonsgegevens door private organisaties is als nieuwe, relevante dreiging aangemerkt. Hoewel in veel gevallen niet illegaal, kunnen de belangen van burgers, die bewust of onbewust toestemming voor gebruik hebben gegeven, toch in het geding komen. Het is vaak niet transparant hoe er door organisaties met persoonlijke gegevens wordt omgesprongen.

| Bron van Dreiging | Doelwi□en: Overheden | Private organisaties | Burgers |
|---|---|---|---|
| **Staten** | Digitale Spionage | Digitale Spionage | Digitale Spionage |
| | O□ensieve cybercapaciteiten | O□ensieve cybercapaciteiten | |
| **Terroristen** | Verstoring/overname ICT | Verstoring/overname ICT | |
| **Beroepscriminelen** | Diefstal en publicatie of verkoop van informatie Q | Diefstal en publicatie of verkoop van informatie | Diefstal en publicatie of verkoop van informatie n |
| | Manipulatie van informatie Q | Manipulatie van informatie Q | Manipulatie van informatie |
| | Verstoring ICT n | Verstoring ICT n | Verstoring ICT 2 |
| | Overname ICT Q | Overname ICT n | Overname ICT |
| **Cybervandalen en scriptkiddies** | Diefstal informatie Q | Diefstal informatie Q | Diefstal informatie |
| | Verstoring ICT Q | Verstoring ICT | |
| **Hacktivisten** | Diefstal en publicatie verkregen informatie | Diefstal en publicatie verkregen informatie | Diefstal en publicatie verkregen informatie |
| | Defacement | Defacement | |
| | Verstoring ICT | Verstoring ICT | |
| | Overname ICT 2 | Overname ICT | |
| **Interne actoren** | Diefstal en publicatie of verkoop verkregen informatie | Diefstal en publicatie of verkoop verkregen informatie | |
| | Verstoring ICT | Verstoring ICT | |
| **Cyberonderzoekers** | Verkrijging en publicatie van informatie | Verkrijging en publicatie van informatie | |
| **Private Organisaties** | | Diefstal informatie (bedrijfsspionage) Q | Commercieel ge-/misbruik of 'doorverkopen' gegevens 2 |
| **Geen actor** | Uitval ICT | Uitval ICT | Uitval ICT |

**Legenda relevantie**

| Laag | Midden | Hoog |
|---|---|---|
| Er worden geen nieuwe trends of fenomenen waargenomen waarvan dreiging uitgaat. OF Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. OF Er hebben zich geen noemenswaardige incidenten voorgedaan in de rapportageperiode | Er worden nieuwe trends en fenomenen waargenomen waarvan dreiging uitgaat. OF Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen. OF Incidenten hebben zich (op enkele kleine na) vooral voorgedaan buiten Nederland. | Er zijn duideljke ontwikkelingen die de dreiging opportuun maken. OF Maatregelen hebben beperkt e□ect, zodat de dreiging aanzienlijk blij□. OF Incidenten hebben zich voorgedaan in Nederland. |

n dreiging is toegenomen Q dreiging is afgenomen 2 dreiging is nieuw

*Tabel 1. Dreigingsmatrix*

# VERDIEPINGSKATERNEN

“DOOR DE DATA-EXPLOSIE ZIJN DIGITALE GEGEVENS NU BESCHIKBAAR IN EEN VORM EN SCHAAL DIE TOT NU TOE NIET BESTOND”

# 1 MONDIALE DATAGROEI IN CONTEXT

**De informatisering van de maatschappij hee□ ingrijpende gevolgen voor de manier waarop mensen hun leven inrichten. Deze trend maakt het leven op vele manieren gemakkelijker, maar brengt ook risico's met zich mee. Dit blijkt uit het gebruik van de groeiende hoeveelheid data door commerciële partijen, criminelen en statelijke actoren. Dit verdiepingskatern gaat in op de verschillende aspecten die deze datagroei met zich meebrengt. Hierbij wordt de structuur uit het kernbeeld gehanteerd, waarbij achtereenvolgens wordt ingegaan op belangen, actoren, hulpmiddelen, kwetsbaarheden en maatregelen.**


**Belangen** Trends van data□catie en dataverzameling ze□en zich voort. Dit leidt enerzijds tot vooruitgang en anderzijds tot risico's voor de belangen van individu en organisatie.

**Dreigingen** Actoren, zowel statelijk als commercieel, beschikken over geavanceerde hulpmiddelen. Er ontstaat een a□ankelijkheid van de intentie van actoren.

**Weerbaarheid** E□ectieve maatregelen om de weerbaarheid te vergroten ontbreken.

## Veranderende belangen

Burgers, bedrijven en overheden creëren, gebruiken en verzamelen meer digitale informatie dan ooit tevoren. Waar in het jaar 2000 nog slechts een kwart van alle informatie digitaal was, liep dat begin 2013 op naar ongeveer 98 procent.[135] Een groot deel van die groei komt niet uit de vervanging van analoge informatie, maar uit nieuwe toepassingen zoals sociale media en cloudcomputing-diensten.

Steeds meer aspecten van ons dagelijks leven worden tegenwoordig direct of indirect vastgelegd: een ontwikkeling die wordt aangeduid als dataficatie.[136] Hierbij valt te denken aan de locatiegegevens die door de smartphone worden geregistreerd, persoonlijke interesses door het klikken op de Like-button van Facebook, muziekvoorkeuren via Spotify en het energieverbruik per apparaat met behulp van slimme energiemeters. Dit alles leidt al jaren tot een exponentiële groei van informatie: een ware data-explosie.[137] Individuele burgers werken hier veelal bewust of onbewust aan mee door hun persoonlijke leven steeds meer te delen met hun sociale netwerk.

Door de data-explosie zijn digitale gegevens nu beschikbaar in een vorm en schaal die tot nu toe niet bestond; opslag van de gegevens kost vrijwel niets meer, en de analysemogelijkheden van grote datasets zijn enorm toegenomen. Hierdoor worden de belangen groter en heeft een eventuele aantasting van de belangen over het algemeen een grotere impact. In de eerste plaats komt dit doordat er simpelweg meer informatie beschikbaar is en verwerkt wordt, maar ook doordat er nieuwe verbanden kunnen worden gelegd die in het verleden onbekend zouden zijn gebleven.

De data-explosie en de daarop gebaseerde diensten hebben een positieve invloed op maatschappelijke groei. Nieuw ontwikkelde toepassingen hebben niet alleen grote economische effecten gehad, maar ook op sociaal-maatschappelijk gebied een vernieuwing teweeggebracht. De nieuwe toepassingen ondersteunen de sociale cohesie en bieden nieuwe mogelijkheden waarmee mensen elkaar weten te vinden, juist doordat ze een deel van hun privacy daarbij inleveren. De toegenomen analysemogelijkheden van de steeds grotere hoeveelheid beschikbare informatie kunnen ten behoeve van het veiligheidsbelang worden ingezet.

Aan de andere kant brengt de dataexplosie ook risico's met zich mee. Door het mondiale transport en de gecentraliseerde verwerking en opslag van enorme hoeveelheden data en gegevens, is de schade en potentiële impact die ontstaat door verstoring, uitval of misbruik van deze informatie veel groter dan voorheen. De belangen van individuen, commerciële organisaties, maar ook van overheden, worden dan geraakt. Bij individuen gaat het hier specifiek over de potentiële schending van het privacybelang, terwijl bij organisaties met name financiële belangen door het verlies

135 h□p://www.foreigna□airs.com/articles/139104/kenneth-neil-cukier-and-viktor-mayer-schoenberger/the-rise-of-big-data

136 Big Data: *A Revolution That Transforms How we Work, Live, and Think*, Mayer-Schönberger en Cukier (2013)

137 'The rise of big data: how it's changing the way we think about the world', Foreign A□airs 92, 3 (may/june 2013), pp. 28-40, h□p://computerworld.nl/big-data/79682-internet-of-things-veroorzaakt-datatsunami

van vertrouwelijkheid in het geding zijn. Ook de maatschappelijke groei kan worden geraakt vanwege de grote afhankelijkheid van de samenleving van cloudgebaseerde diensten en toepassingen.

## Data-exploitatie door verschillende actoren

Dataficatie biedt ongekende mogelijkheden voor innovatief gebruik van de verzamelde gegevens. De voordelen hiervan zijn evident voor gebruikers, maar er kleven ook risico's aan. In de onderstaande paragrafen worden de verschillende actoren toegelicht.

Nederlandse overheid De overheid neemt initiatieven om de rijkdom aan gegevens die zij vanuit haar maatschappelijke rol verzamelt, beter te benutten, zie ook bijvoorbeeld Digitale Overheid 2017. Ook in het kader van het initiatief Open Overheid[138] zijn data, die traditioneel slechts binnen de overheid gebruikt werd, tegenwoordig breder beschikbaar. Private partijen en individuele burgers worden zo in staat gesteld om op basis van deze informatie innovatieve toepassingen te bedenken, die uiteindelijk kunnen leiden tot grotere maatschappelijke en economische groei.

> *"Ook in Nederland bestaat een levendige handel in consumentenpro elen."*

Commerciële partijen Verschillende internationaal toonaangevende bedrijven hebben een bedrijfsmodel dat gebaseerd is op de exploitatie en/of verkoop van grote hoeveelheden gebruikersinformatie. In dergelijke, vooralsnog zeer succesvolle bedrijfsmodellen, worden gratis diensten via het internet aangeboden in ruil voor toestemming voor de exploitatie van persoons- en gebruiksgegevens. De gretige afname van de aangeboden diensten onderstreept dat hiermee tegemoet wordt gekomen aan een grote maatschappelijke behoefte, maar "surveillance is still the business model of the internet", aldus beveiligingsexpert Bruce Schneier.[139] In toenemende mate proberen bedrijven de zelfvergaarde informatie te verrijken met andere informatie uit publieke en private bronnen, waarna het verhandeld kan worden met derde partijen. Ook in Nederland bestaat een levendige handel in consumentenprofielen, met een jaarlijkse omzet van 1,3 miljard euro.[140]

Buitenlandse inlichtingen- en veiligheidsdiensten Ook voor inlichtingen- en veiligheidsdiensten vormt de mondiale datagroei een potentieel rijke informatiebron. Door actief gebruik te maken van de beschikbaarheid van gedetailleerde gegevens zijn de diensten in staat om hun taken te vervullen, wat de veiligheid in de samenleving uiteindelijk ten goede komt. Vanaf juni 2013 verschenen onthullingen over de activiteiten van de Amerikaanse National Security Agency (NSA) in de wereldpers op basis van informatie gelekt door de voormalige werknemer van die dienst Edward Snowden. Kanttekening bij deze nieuwsberichten is dat deze niet uit een diversiteit aan bronnen worden bevestigd. De NSA en haar Britse tegenhanger GCHQ stellen binnen de marges van hun wettelijke ruimte te hebben gehandeld. De aandacht in media werd gericht op vormen van data-exploitatie die normaliter minder in de schijnwerpers staan. In de media wordt de schaal van de activiteiten en de geavanceerde technische capaciteiten benadrukt.

De AIVD en MIVD hebben geen indicaties dat bondgenoten de afgelopen jaren digitale spionageactiviteiten tegen Nederlandse belangen hebben ontplooid.[141] Vanuit niet-bondgenoten achten de Nederlandse inlichtingen- en veiligheidsdiensten, zoals aangegeven in de opeenvolgende jaarverslagen, de dreiging echter aanwezig en toenemend.[142]

In de Nederlandse context acht het kabinet op zichzelf het intercepteren van metadata en het analyseren daarvan in zijn algemeenheid een aanvaardbare methode in het kader van onderzoek naar terroristen, andere gevaren voor de nationale veiligheid of in het kader van militaire operaties.[143]

Cybercriminelen Een laatste categorie actoren met interesse in data-explosie is cybercriminelen. De hoeveelheid en soort gegevens die ten gevolge van de data-explosie centraal wordt opgeslagen vormt een potentieel doelwit voor cybercriminelen. De rijkdom aan gevoelige gegevens biedt een uitstekend startpunt voor criminele activiteiten, zoals (spear)phishing of identiteitsfraude. De nog altijd groeiende omvang van gepubliceerde datadiefstallen is in dit kader onrustbarend.[144]

## Hulpmiddelen

Actoren zetten verschillende hulpmiddelen in om de grote hoeveelheden data te exploiteren.

Commerciële bedrijven verzamelen een grote diversiteit aan gegevens, die worden gegenereerd als onderdeel van het gebruik van hun dienstverlening. Afhankelijk van de specifieke vorm van dienstverlening zijn deze in meerdere of mindere mate gestructureerd, en kunnen bijvoorbeeld de vorm aannemen van e-mails, tweets, clickstreams of demografische classificaties. Vorig jaar is in het CSBN al inzicht gegeven in deze vorm van 'verzamelwoede' van de zijde van het bedrijfsleven.[145]

138 h□ps://data.overheid.nl/openoverheid
139 h□p://www.theatlantic.com/technology/archive/2014/03/don-t-listen-to-google-and-facebook-the-public-private-surveillance-partnership-is-still-going-strong/284612/
140 Michael Persson, "Wie ben ik volgens big data?" (Volkskrant, 12 april 2014)
141 Katern Digitale dreiging door statelijke actoren
142 Katern Digitale dreiging door statelijke actoren
143 Kamerstuk 30977 nr 63
144 h□p://www.spiegel.de/netzwelt/netzpolitik/e-mail-passwoerter-gestohlen-18-millionen-datensaetze-a-962419.html (paragraaf Schwarzmarkt für Zugangsdaten □oriert) h□ps://www.riskbasedsecurity.com/reports/2013-DataBreachQuickView.pdf h□p://blog.trendmicro.nl/security-voorspellingen-2014-maandelijks-grote-datalekken-toename-cybercrime-mobiel-bankieren-en-vergrote-kans-op-identiteitsdiefstal/
145 Zie verdiepingskatern "Grip op informatie", CSBN-3

Programmeermodellen als MapReduce, programmeeromgevingen als Hadoop en de beschikbare verwerkingscapaciteit op steeds krachtiger computersystemen, bieden bedrijven de mogelijkheid om de enorme hoeveelheden data te analyseren. Dit kan uiteindelijk leiden tot nieuwe inzichten die kunnen worden ingezet om commerciële mogelijkheden te creëren.

Buitenlandse inlichtingendiensten beschikken over een verzameling van technisch geavanceerde methoden, technieken en hulpmiddelen, waarmee zij zich structureel en mondiaal toegang tot informatie en ICT-systemen verschaffen.[146] Er zouden activiteiten worden ontplooid die gericht zijn op het verzwakken van (encryptie) tools en technieken die breed ingezet worden om betrouwbare elektronische communicatie mogelijk te maken. Wereldwijd gebruikte standaarden voor de beveiliging van digitale communicatie zouden zijn beïnvloed, maar ook specifieke leveranciers zouden hebben meegewerkt aan het aanpassen van hun beveiligingsproducten, met als doel versleutelde informatie desgewenst toegankelijk te maken voor de inlichtingendiensten. Dit heeft potentieel zorgwekkende implicaties, aangezien het de basis voor het vertrouwen op het gehele internet kan eroderen. Daarnaast kunnen andere partijen hun voordeel doen met mogelijk geïntroduceerde verzwakkingen. Hierbij kan worden gedacht aan cybercriminelen, die dergelijke kwetsbaarheden kunnen benutten voor hun eigen gewin.

## Kwetsbaarheden

De vorm waarin de data-explosie zich momenteel manifesteert, draagt inherente kwetsbaarheden in zich. Zodra meer gegevens worden gegenereerd, kan er meer informatie worden onderschept, gemanipuleerd of verstoord. Als meer informatie van een hoger detailniveau wordt opgeslagen, wordt het ook aantrekkelijker om deze bron van informatie verder te benutten. De kwetsbaarheden die in het gelijknamige hoofdstuk zijn beschreven, zijn in hoge mate ook van specifieke toepassing op de omvangrijke en gedetailleerde dataverzamelingen die tegenwoordig door de beschreven data-explosie beschikbaar zijn.

In aanvulling hierop geldt dat bij commerciële partijen die zich richten op het benutten van grote hoeveelheden aan gebruikers gerelateerde data, het voor de buitenwereld niet altijd transparant is hoe de gegevens worden gebruikt. Dat deze gegevens worden ingezet om gerichte advertenties aan de gebruikers aan te bieden, mag tegenwoordig wel als bekend verondersteld worden. De exacte technieken en besliscriteria achter deze processen zijn echter niet inzichtelijk voor de buitenwereld. Concurrentieoverwegingen en de bescherming van bedrijfsgeheimen spelen hierin een belangrijke rol. Dit heeft echter tot gevolg dat het voor de betroffen partijen wier data in het geding is – of dit nu individuen op een sociaal netwerk zijn, of bedrijven die hun gegevens hebben geoutsourcet naar de cloud – vrijwel onmogelijk is om een zelfstandige rol te spelen in het vaststellen van eventuele kwetsbaarheden.

146 Katern Digitale dreiging door statelijke actoren

Ook in het inlichtingendomein worden de grote datastromen en -verzamelingen met interesse bekeken. Op basis van publicaties van de Nederlandse inlichtingendiensten kan worden geconcludeerd dat buitenlandse statelijke actoren en de buitenlandse inlichtingendiensten inspanningen verrichten om gebruik te maken van de gegevens die in de digitale wereld worden geproduceerd.[147]

## Maatregelen

Om weerbaarheid te vergroten en belangen te beschermen, moeten maatregelen worden genomen. Bescherming tegen de kwetsbaarheden die door de data-explosie worden gegenereerd, is problematisch. Bij commerciële partijen is het moeilijk om als individu of als organisatie maatregelen te nemen, aangezien de leverancier eenzijdig bepaalt welke functionaliteiten en beveiligingsopties worden opgenomen in een dienst. Daarnaast is de leverancier ook in de positie om de voorwaarden gedurende de levensduur van de dienst te veranderen. De gebruiker is dus in sterke mate afhankelijk van de leverancier voor het nemen van maatregelen.

Bij het treffen van dergelijke maatregelen is het echter voorstelbaar dat een aantal buitenlandse inlichtingendiensten over dusdanig geavanceerde technieken beschikt, dat bekende maatregelen niet afdoende zullen zijn om de vertrouwelijkheid van gegevens tegen dergelijke partijen te waarborgen.

De Rijksoverheid heeft er op basis van haar Rijkscloudstrategie voor gekozen om een gesloten Rijkscloud in eigen beheer in te richten als een voorziening die generieke diensten levert binnen de Rijksdienst. Deze voorziening wordt ingericht binnen een eigen beveiligd netwerk en beheerd door een eigen, rijksbrede organisatie. Er is dus gekozen voor een community/private clouddienst in eigen beheer. De overheid zal daarnaast een verkenning uitvoeren naar de haalbaarheid van gescheiden ICT-netwerk voor vitale processen.[148]

In de context van toenemende dreiging en steeds verdergaande technische mogelijkheden speelt het dilemma van het vinden van een goede balans tussen veiligheid en waarborgen ter bescherming van de privacy. Dit dilemma werd bijvoorbeeld door president Obama aan de orde gesteld in zijn speech op 17 januari 2014 waar hij hervormingen van NSA-programma's aankondigde.[149]

147 Katern Digitale dreiging door statelijke actoren
148 Nationale Cyber Security Strategie 2
149 h□p://www.whitehouse.gov/the-press-o□ce/2014/01/17/remarks-president-review-signals-intelligence

**Het recht om vergeten te worden**

Op 13 mei 2014 heeft het Europese hof van Justitie besloten dat exploitanten van (internet) zoekmachines verantwoordelijk zijn voor de verwerking van persoonsgegevens die worden weergegeven op de door derden gepubliceerde webpagina's.[150] Dit naar aanleiding van een zaak aangespannen door een Spaanse burger. Dit is de eerste keer dat een Europees rechtsprekend orgaan het 'recht om vergeten te worden' erkent.[151] Zoekmachines als Google zijn druk bezig om het mogelijk te maken dat gebruikers dit recht ook kunnen uitoefenen.[152]

Het groeiende bewustzijn onder burgers dat hun persoonlijke gegevens waardevol zijn biedt ook commerciële kansen voor partijen die privacy willen beschermen. De bescherming van de privacy van de gebruiker wordt een verkoopargument voor uiteenlopende producten en diensten. Zo kondigde KPN aan dit jaar de Blackphone in het assortiment op te nemen:[153] een telefoon die gebruik maakt van speciale software die de privacybescherming van de klant vooropstelt door onder meer gesprekken te versleutelen en tracking te minimaliseren. Ook privacyvriendelijke sociale netwerken positioneren zich: Diaspora[154] en Vivaldi[155] zijn hierbij bekende namen. Er moet wel worden opgemerkt dat vanwege zogeheten netwerkeffecten het minder aantrekkelijk is om naar een nieuwe communicatiedienst of sociaal medium te verhuizen als de eigen contactpersonen van bestaande diensten gebruik blijven maken.[156]

## Conclusie

Burgers, bedrijven en overheden creëren, gebruiken en verzamelen meer digitale informatie dan ooit tevoren. De trends van datificatie en dataverzameling zullen zich voortzetten. Dit leidt enerzijds tot maatschappelijke vooruitgang en meer mogelijkheden op veiligheidsgebied. Aan de andere kant brengt dit risico's voor het individuele privacybelang en het belang van vertrouwelijkheid van informatie voor private organisaties en overheden met zich mee. Bij toenemende dreiging en steeds verdergaande technische mogelijkheden moet een goede balans worden gevonden tussen veiligheid en waarborgen ter bescherming van de privacy.

Afgelopen jaar hebben mondiale cases laten zien dat deze risico's reëel zijn en dat de belangen geschaad kunnen worden. Het verlies van grip op informatie, een risico dat vorig jaar al in het CSBN is geconstateerd, is een reële dreiging. Daarbij is afgelopen jaar in de media en maatschappelijke discussies grote aandacht geweest voor activiteiten van buitenlandse inlichtingendiensten. De AIVD en MIVD hebben echter geen indicaties dat bondgenoten het afgelopen jaar digitale spionageactiviteiten tegen Nederlandse belangen hebben ontplooid. Vanuit niet-bondgenoten wordt de dreiging echter aanwezig en toenemend geacht.

Commerciële partijen nemen een steeds centralere rol in binnen de informatie-infrastructuur van individuen, bedrijven en overheden. Dit brengt risico´s met zich mee, vanwege de afhankelijkheid van deze bedrijven en de grote hoeveelheid data. Het vergroten van de weerbaarheid blijkt problematisch omdat de aanwezige kwetsbaarheden door de eindgebruiker nauwelijks weg te nemen vallen met gerichte maatregelen.

Op het gebied van dataverzameling en dataexploitatie zijn gebruikers afhankelijk geworden van de intenties van actoren, zowel statelijk als commercieel. Hiermee zijn zij ook kwetsbaar voor een verandering in de intenties van deze actoren. Zodra een statelijke actor of een commerciële partij besluit haar capaciteiten ten nadele van Nederlandse belangen in te zetten, kan deze dreiging manifest worden. Het is voor de betreffende belanghebbenden niet altijd goed zichtbaar wanneer een verschuiving in de intenties zich voordoet.

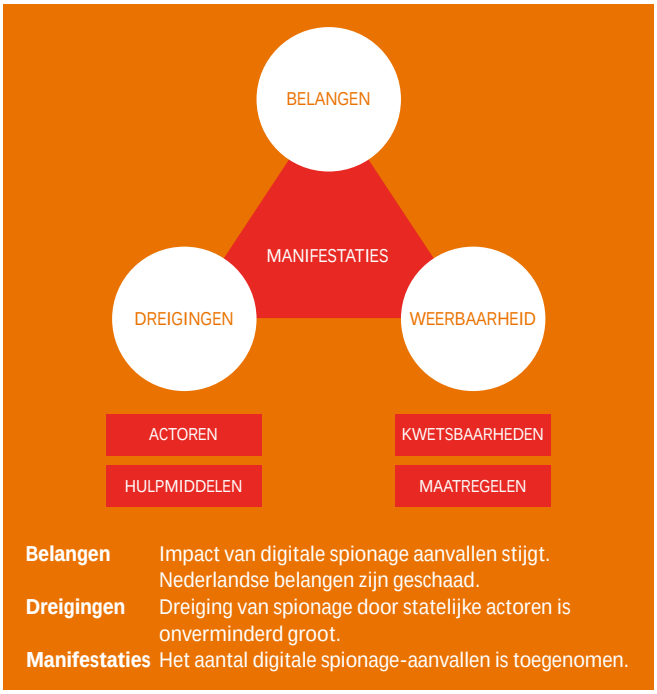
Samenvattend kan worden gesteld dat de belangen groot zijn, de weerbaarheid laag en dat de hulpmiddelen aanwezig zijn om de belangen te bedreigen. Maatregelen om de kwetsbaarheden af te wenden zijn door eindgebruikers slechts moeilijk vorm te geven. Hiermee zijn burgers en bedrijven afhankelijk van de intenties van commerciële en statelijke actoren en kunnen Nederlandse belangen geschaad worden bij veranderende intenties. «

150 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070nl.pdf
151 http://www.elsevier.nl/Tech/nieuws/2014/5/Vanaf-nu-heeft-iedere-EU-burger-het-recht-om-vergeten-te-worden-1521536W/
152 http://www.volkskrant.nl/vk/nl/2694/Tech-Media/article/detail/3663999/2014/05/30/Google-lanceert-recht-om-vergeten-te-worden.dhtml
153 http://forum.kpn.com/t5/Betrouwbaarheid-Veiligheid/Blackphone-is-een-privacy-telefoon/ba-p/199181
154 https://diasporafoundation.org
155 https://vivaldi.net
156 http://www.spiegel.de/netzwelt/web/threema-surespot-textsecure-sichere-whatsapp-alternativen-a-954576.html

“BIJNA ELKE INLICHTINGENDIENST INVESTEERDE DE AFGELOPEN JAREN IN ZIJN DIGITALE CAPACITEITEN”

# 2 DIGITALE DREIGING DOOR STATELIJKE ACTOREN

**De omvang en structurele wijze van digitale aanvallen door statelijke actoren vormen een grote dreiging voor de nationale veiligheid en economie. In de afgelopen rapportageperiode waren diverse publieke en private instellingen in Nederland slachto□er of doelwit van digitale spionageaanvallen door statelijke actoren. Daarnaast is Nederlandse ICT-infrastructuur veelvuldig misbruikt om digitale aanvallen op andere landen uit te voeren. Bijna elke inlichtingendienst investeerde de afgelopen jaren in zijn digitale capaciteiten, waardoor digitale spionage niet alleen is voorbehouden aan grote en geavanceerde inlichtingendiensten. Hoewel er nog weinig precedenten zijn, is de militaire inzet van digitale aanvallen mogelijk een aanzienlijke bedreiging voor nationale en bondgenootschappelijke belangen.**




De trend dat digitale spionage een groeiende dreiging vormt voor overheden en het bedrijfsleven zette het afgelopen jaar door. De inlichtingendiensten AIVD en MIVD hebben vastgesteld dat de dreiging tussen april 2013 en maart 2014 onverminderd groot was. De digitalisering biedt grote mogelijkheden voor spionage, verstoring en sabotage van de economie en het maatschappelijk leven, en een extra mogelijkheid voor de ontplooiing van militaire operaties.

In 2013 zijn Nederlandse belangen geschaad, aangezien overheidsinstellingen, de defensie-industrie en bedrijven binnen topsectoren slachtoffer waren van digitale spionage. De grootste dreiging voor de nationale veiligheid komt van statelijke actoren. De weerstand tegen digitale aanvallen binnen de overheid en het bedrijfsleven bleek niet in alle gevallen toereikend, waardoor de slagingskans van geavanceerde digitale aanvallen door staten ook in de nabije toekomst substantieel is.

Dit verdiepingskatern geeft inzicht in digitale aanvallen door statelijke actoren, en de dreiging die hiervan uitgaat voor Nederland en de inzetbaarheid van de Nederlandse krijgsmacht. De doelwitten van digitale aanvallen, de actoren die hierbij een rol spelen en de impact die dergelijke aanvallen hebben, worden besproken.

## Digitale spionage

De AIVD en MIVD signaleren dat het aantal digitale spionageaanvallen het afgelopen jaar is toegenomen en dat ze bovendien winnen aan complexiteit en impact. De wereldwijde groei van internet, en de afhankelijkheid van internet voor het creëren, verspreiden en opslaan van data, voegen een dimensie toe aan spionage.

Digitale spionage is relatief eenvoudig en goedkoop ten opzichte van traditionele spionage. Het risico van onderkenning is klein en de potentiële opbrengst bijzonder groot. Digitale spionage is daardoor niet langer voorbehouden aan grote, geavanceerde inlichtingendiensten. Bijna elke inlichtingendienst investeerde de afgelopen jaren in zijn digitale capaciteiten. Dat digitale spionage relatief eenvoudig kan worden gerealiseerd, maakt het bovendien een bereikbaar instrument voor statelijke organisaties die vanuit financiële of politiek-ideologische overwegingen inlichtingen willen vergaren over overheden, bedrijven of burgers. Dit leidt tot een grote diversiteit aan spionagedreiging.

Overheid Het afgelopen jaar zijn meerdere digitale spionageaanvallen op Nederlandse overheidsinstellingen onderkend, waarbij het merendeel is gericht tegen de ministeries van Buitenlandse Zaken en Defensie. Bij overheidsinstellingen en in Nederland gevestigde internationale organisaties is veel kennis en inzicht aanwezig waarmee andere landen hun voordeel kunnen doen. Andere

landen trachten via digitale spionage voorkennis te bemachtigen over onder meer politieke besluitvorming, economische plannen en Nederlandse standpunten en onderhandelingsstrategieën op verschillende terreinen. Met deze informatie kan een land proberen om de besluitvorming over bepaalde onderwerpen (heimelijk) te beïnvloeden, zodat een besluit gunstig uitvalt voor dat land.

Defensie De omvang en structurele wijze waarop digitale spionage wordt toegepast, vormt een significante dreiging voor defensiebelangen en de defensie-industrie. De AIVD en MIVD hebben vastgesteld dat de Nederlandse defensie-industrie een gewild doelwit is op het gebied van digitale spionage. Bovendien beschikt de MIVD over aanwijzingen dat de digitale spionagedreiging zich niet alleen rechtstreeks richt op de defensie-industrie, maar ook op partijen met wie de defensie-industrie samenwerkt, zoals financiële instellingen, patentkantoren, advocatenkantoren of consultancyfirma's. Ook in 2013 zijn digitale spionageactiviteiten richting Nederlands defensiepersoneel vastgesteld. Zowel binnen Nederland als in het buitenland zijn e-mailaccounts van Nederlands defensiepersoneel doelwit geweest van (spear) phishing, waarschijnlijk door een statelijke actor.

Defensie is in verschillende regio's in de wereld actief. Zo voert Defensie grote missies uit in Mali en on de wateren rond Somalië, en is Defensie permanent aanwezig in de Caribische delen van het Koninkrijk. De defensienetwerken en -systemen die in deze gebieden worden gebruikt, vormen een doelwit voor potentiële digitale aanvallen en spionage. Binnen multinationale missies hanteert bovendien niet ieder deelnemend land, bewust of onbewust, dezelfde hoge cybersecuritystandaard als de Nederlandse krijgsmacht. In voorkomende gevallen doet de MIVD onderzoek naar incidenten.

Topsectoren Nederland is een aantrekkelijke locatie voor het internationale bedrijfsleven en vormt een speelveld waar de economische concurrentiestrijd zich op afspeelt. De AIVD en MIVD signaleren dat (digitale) spionage door sommige landen wordt ingezet om concurrentievoordeel te verkrijgen. De dreiging van economische spionage ten behoeve van de bevoordeling van de eigen nationale industrie, technisch-wetenschappelijke ontwikkeling en concurrentiepositie op de wereldmarkt, komt van diverse landen.

Het afgelopen jaar is geconstateerd dat steeds meer digitale aanvallen zijn gericht op het bedrijfsleven, waarbij het met name gaat om bedrijven en onderzoeksinstellingen binnen de energie-, biotechnologie-, chemie- en hightech-sector in Nederland en daarbuiten. Deze aanvallen richten zich op het vergaren van vertrouwelijke technisch-wetenschappelijke en financieel-economische informatie om voorkennis te vergaren over naderende transacties, overnames en onderhandelingsposities. De AIVD en MIVD beschikken over aanwijzingen dat het merendeel van de aanvallen afkomstig is van statelijke actoren.

ICT-infrastructuur Nederland heeft een hoogwaardige ICT-infrastructuur. Ons land behoort tot de wereldtop op het gebied van bandbreedte, verbindingssnelheid, internetknooppunten en aantallen datacenters. Hierdoor is Nederland een aantrekkelijke uitvalsbasis en doorvoerhaven voor digitale aanvallen.

Het afgelopen jaar is op grote schaal misbruik gemaakt van de Nederlandse ICT-infrastructuur om (geavanceerde) digitale aanvallen uit te voeren op andere landen. Aanvallers uit meerdere landen infiltreerden via Nederland wereldwijd succesvol honderden computernetwerken met het doel om vertrouwelijke informatie te verzamelen. De digitale aanvallen richtten zich met name tegen gouvernementele organisaties, diplomatieke vertegenwoordigingen, defensie gerelateerde instellingen, internationale organisaties, onderzoeksinstituten en personen. Voor alle onderkende aanvallen geldt dat de omvang, tijdsduur, en doelwitkeuze een door een overheid geïnitieerde of gesponsorde aanval suggereren.

## O□ensieve militaire inzet en digitale sabotage door statelijke actoren

Computer network a□ack Naast de dreiging van (digitale) spionage moet ook rekening worden gehouden met de dreiging die uitgaat van de inzet van offensieve cyberoperaties door statelijke actoren. Internationaal staat dit fenomeen bekend als computer network attack (CNA).[157] Diverse landen ontwikkelen het vermogen om offensieve cyber operaties uit te voeren en nemen militair optreden in het digitale domein op in hun militaire doctrines. Een geavanceerde digitale aanval gericht op het manipuleren, verstoren of vernietigen van overheidsnetwerken, communicatiesystemen, militaire sensoren of wapensystemen kan de effectiviteit van bijvoorbeeld luchtaanvallen of landoptreden vergroten. Daarnaast zouden digitale middelen kunnen worden ingezet om paniek of verwarring te zaaien onder de burgerbevolking, desinformatie te verspreiden of de inzetbaarheid van veiligheids- en hulpdiensten te beperken. Er zijn internationaal nog weinig precedenten van de inzet van dergelijke operaties, maar de mogelijke impact is groot.

Digitale sabotage Al eerder is gebleken dat digitale aanvallen (delen van) vitale sectoren kunnen ontregelen en beschadigen. Vitale sectoren kunnen zelfs met minder geavanceerde aanvallen worden ontregeld. Dit bleek onder meer toen diverse instellingen in het voorjaar van 2013 slachtoffer werden van DDoS-aanvallen. Deze aanvallen leidden weliswaar niet tot maatschappelijke ontwrichting, maar duidelijk is wel dat met een relatief eenvoudig middel als een DDoS-aanval de toegang tot online betalingsdiensten hinderlijk verstoord kan worden, wat tot groot ongemak en onrust kan leiden.

In 2013 kwamen wereldwijd enkele voorbeelden voor van een nieuwe vorm van digitale sabotage, waar mogelijk statelijke actoren bij betrokken waren. Daarbij werden moedwillig grote hoeveelheden data verwijderd of vernietigd op commerciële netwerken in landen die door de aanvallers als politieke opponenten werden beschouwd. Voorbeelden zijn de aanvallen op de overheid van Qatar

157 O□ensieve cybercapaciteiten zijn de digitale middelen die het doel hebben om het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. Deze capaciteiten kunnen in een militaire operatie worden ingezet ter ondersteuning van conventionele militaire capaciteiten. Internationaal staat dit fenomeen bekend als computer network a□ack (CNA).

en een grootschalige aanval op Zuid-Koreaanse commerciële netwerken met verstoringen in de financiële sector tot gevolg. Wanneer statelijke actoren die Nederland niet goed gezind zijn dergelijke aanvallen inzetten tegen Nederland, kunnen de gevolgen voor de inzetbaarheid van de rijksoverheid of het functioneren van publieke instellingen aanzienlijk zijn.

## Actoren van digitale aanvallen

Statelijke actoren Een grote digitale dreiging tegen Nederland gaat momenteel uit van statelijke actoren. Van alle actoren hebben staten de belangen, intentie, middelen en expertise om forse offensieve digitale capaciteiten te ontwikkelen.

In vergelijking met vorig jaar kan worden geconcludeerd dat statelijke actoren geavanceerdere en complexere aanvalstechnieken gebruiken om digitale spionageaanvallen te kunnen uitvoeren. De AIVD en MIVD hebben waargenomen dat de aanvallers in toenemende mate hun doelwit gericht infecteren en proberen data-exfiltratie te laten opgaan in regulier netwerkverkeer. Hierdoor zijn spionageaanvallen moeilijk te onderkennen.

*"Nederland is een aantrekkelijke uitvalsbasis en doorvoerhaven voor digitale aanvallen."*

De dreiging die uitgaat van statelijke actoren is in de voorgaande paragrafen behandeld. De AIVD en MIVD hebben geen indicaties dat bondgenoten het afgelopen jaar digitale spionageactiviteiten ontplooiden tegen Nederlandse belangen.

Niet-statelijke actoren Het afgelopen jaar zette de trend zich voort dat hackerscollectieven zich opwerpen als verdedigers van de belangen van staten. Een voorbeeld hiervan zijn pro-Russische en pro-Oekraïense hackers die tijdens de crisis op de Krim over en weer DDoS-aanvallen en defacements hebben uitgevoerd. De AIVD en MIVD hebben aanwijzingen dat deze hackers gedoogd dan wel gesteund worden door hun nationale overheden. Maar deze relaties zijn schimmig. Tegen Nederland zijn aanvallen van dergelijke hackerscollectieven die belangen van staten behartigen het afgelopen jaar niet waargenomen. Indien Nederlandse belangen niet overeenkomen met belangen van bepaalde staten, is het echter voorstelbaar dat hackerscollectieven ook tegen Nederland worden ingezet.

## Impact van digitale aanvallen

Digitale spionage Digitale spionageaanvallen op overheidsinstellingen hebben gevolgen voor de nationale veiligheid, aangezien de politiek-bestuurlijke en ambtelijke integriteit kan worden aangetast. De internationale onderhandelingspositie van Nederland kan worden ondermijnd doordat standpunten al bekend kunnen zijn bij een andere partij. Daarnaast kan de positie van Nederland als betrouwbare partner worden aangetast en kan ons land als gevolg hiervan imagoschade oplopen.

Bedrijven binnen topsectoren lopen groot risico op schade als gevolg van inbreuken op intellectueel eigendom en door ondermijning van de onderhandelingspositie in aanbestedingstrajecten, contractonderhandelingen, fusies en overnames. Hoewel precieze cijfers ontbreken, is het waarschijnlijk dat de wereldwijde schade honderden miljarden euro's bedraagt als gevolg van inkomstenderving, verlies aan concurrentiepositie en banen, en door kosten voor het nemen van beveiligings- en herstelmaatregelen.

Computer network a□ack en digitale sabotage Met name de combinatie van digitale aanvallen met fysieke militaire middelen vormt potentieel een aanzienlijke dreiging tegen nationale en bondgenootschappelijke belangen. Ook kunnen opponenten in crisisgebieden waar de Nederlandse krijgsmacht wordt ingezet, tegenwoordig in Nederland toeslaan met digitale aanvallen. Met deze backlash-effecten tegen Nederlandse belangen moet in toenemende mate rekening worden gehouden. Bovendien kan Nederland als lidstaat van internationale organisaties als de EU en de NAVO, ook (indirect) slachtoffer worden van aanvallen tegen deze organisaties.

Digitale sabotageaanvallen kunnen de nationale veiligheid schaden, wanneer er sprake is van langdurige en grootschalige uitval van vitale infrastructuren met maatschappelijke en economische ontwrichting tot gevolg. Hierbij kan sprake zijn van interruptie van dienstverlening, financiële schade en zaakschade.

## Conclusie

Digitale spionage vormt net als voorgaande jaren een grote dreiging voor de overheid en topsectoren in Nederland. De aanvallen winnen aan complexiteit, omvang en impact. Bijna elke inlichtingendienst investeerde de afgelopen jaren in zijn digitale capaciteiten, waardoor digitale spionage niet alleen is voorbehouden aan grote en geavanceerde inlichtingendiensten.

Digitale sabotageaanvallen kunnen de nationale veiligheid schaden, indien er sprake is van langdurige en grootschalige uitval van vitale infrastructuren met maatschappelijke en economische ontwrichting tot gevolg.

Hoewel er nog weinig precedenten zijn, is de potentiële impact van de militaire inzet van offensieve cyberoperaties groot. Diverse landen ontwikkelden de afgelopen jaren dergelijke capaciteiten, waaronder landen die Nederland of diens bondgenoten slecht gezind zijn. De ontwrichtende gevolgen van een hoogwaardige digitale aanval tegen nationale of bondgenootschappelijke belangen kunnen groot zijn. «

“DE SOFTWARE-INDUSTRIE IS GEWEND AAN EEN BEPAALDE LEVENSDUUR EN ONDERSTEUNT SOFTWARE DAARNA NIET MEER”

# 3 DUURZAAMHEID ICT

**Apparatuur wordt niet eeuwig ondersteund. Dat is ook niet mogelijk. Apparatuur wordt wel steeds vaker met het internet verbonden. Dit vormt een risico, en kan in de toekomst een groot probleem worden voor het waarborgen van de cybersecurity.**

**Aanvallen via internetverbindingen op systemen met een fysieke werking, zoals auto's of medische apparatuur, kunnen directe gevolgen hebben voor de persoonlijke veiligheid van de gebruikers of de economische continuïteit van organisaties.**

**Een pasklare oplossing is er niet. De traditionele manier van updaten, onderhouden en tijdig vervangen werkt vaak niet voor deze soorten systemen. Daarom moet er nu worden nagedacht over de omgang met de veroudering van apparatuur.**


| | |
|---|---|
| **Belangen** | De toename van automatisering en internetkoppeling van systemen leidt tot een grotere maatschappelijke a□ankelijkheid van goed werkende so□ware. |
| **Dreigingen** | So□ware in apparaten die niet meer wordt onderhouden maar wel aan het internet gekoppeld is, is kwetsbaar voor aanvallen van buitenaf. |
| **Maatregelen** | Oplossingen zijn nog niet geformuleerd. Hiermee ontstaat een risico dat belangen in de toekomst geschaad worden. |

## Duurzaamheid van ICT is een groeiend probleem

De samenleving raakt steeds meer geautomatiseerd: er wordt niet alleen gebruik gemaakt van duidelijke ICT-middelen zoals computers en smartphones, maar ook van minder zichtbare ICT om vele aspecten van het dagelijks leven te besturen.

Voertuigen, medische apparatuur, industriële controlesystemen, televisies en dergelijke worden nu uitgerust met nieuwe techniek en zijn in hoge mate geautomatiseerd (smart). Over enkele jaren zal de software in deze apparaten echter achterhaald zijn, terwijl het gebruik ervan nog doorgaat. De software-industrie is gewend aan een bepaalde levensduur en ondersteunt software daarna niet meer. Als hier dan kwetsbaarheden in ontdekt worden, wordt misbruik op grote schaal mogelijk.

Leveranciers van hardware en consumentenproducten zijn vaak helemaal niet toegerust op ondersteuning en aanpassing van hun producten, nadat deze eenmaal aan de consument zijn geleverd. Hierdoor worden later ontdekte kwetsbaarheden in voorkomende gevallen niet meer verholpen. In de afgelopen periode hebben we voorbeelden van routers gezien,[158] waarbij dit probleem de kop opstak. Fabrikanten staan bovendien onder druk om te innoveren op de ontwikkeling van nieuwe apparaten, niet om oude apparaten toekomstvaster te maken.

Door de steeds verdergaande koppeling met internet kunnen kwetsbaarheden op afstand misbruikt worden, waardoor de werking van producten verstoord kan worden. Dit kan leiden tot ernstige economische problemen en kan mogelijk zelfs gebruikers fysiek in gevaar brengen.

Gebruikers hebben onvoldoende mogelijkheden om software in apparatuur zelf te onderhouden, terwijl leveranciers dit vaak ook achterwege laten of zelfs onmogelijk maken. Deze problematiek kan gezien worden als een gebrek aan duurzaamheid van ICT.

## Oorzaken

Het duurzaamheidsprobleem wordt veroorzaakt door een aantal ontwikkelingen, die deels in dit cybersecuritybeeld en in vorige edities zijn behandeld.

158 h□p://www.rtlnieuws.nl/nieuws/binnenland/spooktelefoontjes-op-rekeningen-xs4all, geraadpleegd op 11 juni 2014

Ten eerste het Internet der Dingen, de ontwikkeling waarbij steeds meer apparaten verbonden zullen zijn met elkaar en met internet. Deze apparaten verzamelen gegevens over hun omgeving en wisselen die gegevens onderling uit. Ten tweede beëindigen softwarefabrikanten de ondersteuning en doorontwikkeling van oude software, terwijl die vaak nog in gebruik blijft. Beveiligingslekken worden dan niet meer opgelost.

## Risico's

De gebruiker is meer en meer onwetend van de potentiële beveiligingsproblemen die 'meesluipen' met de aanschaf van nieuwe apparatuur en het in gebruik blijven houden van oudere apparaten. Het ontbreekt hem veelal aan de benodigde kennis en vaardigheden om hier iets tegen te doen, en de informatie en mogelijkheden die leveranciers bieden, zijn vaak ook onvoldoende. Hierdoor kan de gebruiker of zijn omgeving risico's lopen op zowel digitaal gebied, denk aan gegevensdiefstal, als op fysiek vlak, wanneer er bijvoorbeeld problemen optreden met auto's.

**Windows XP**

Microsoft stopte op 8 april 2014 na ruim twaalf jaar met de ondersteuning van Windows XP. In de praktijk blijken er nog zeer veel XP-gebruikers te zijn, zowel privé als bij bedrijven en overheden.[159] Aangezien er geen nieuwe beveiligingsupdates voor Windows XP meer uitkomen, leidt dit tot een grote hoeveelheid potentieel kwetsbare systemen.[160]

Levensduur van software Computers waarbij gebruikers of beheerders volledige bedieningsmogelijkheden hebben, zijn eenvoudiger te onderhouden. De software-industrie is hierop ingeregeld; programmatuur wordt continu doorontwikkeld en nieuwe versies volgen elkaar in hoog tempo op. Dit leidt ertoe dat gebruikers die blijven vasthouden aan een oudere softwareversie, in mindere mate kunnen rekenen op ondersteuning en beveiligingsupdates. Voor veel bedrijven is de investering daarin onaantrekkelijk. De economische levensduur van software is daarom vaak slechts enkele jaren, beduidend korter dan bijvoorbeeld in de auto-industrie.

In de auto-industrie liggen de verhoudingen dan ook anders dan in de ICT-sector. Nadat de ontwikkeling en productie van een bepaald automodel is voltooid, is de vernieuwingsbehoefte minimaal. Wanneer een nieuwe editie van een model uitkomt, zullen garages echter nog wel in staat zijn om de oudere auto's te onderhouden. Ook bij veiligheidsproblemen, bijvoorbeeld wanneer de remmen als gevolg van een ontwerpfout in bepaalde situaties niet goed werken, kan dit verholpen worden via terugroepacties, ongeacht de leeftijd van de auto. Gebruikers van auto's zijn gewend om te betalen voor het onderhoud van hun voertuig, terwijl dit vooral bij thuisgebruik van ICT veel minder het geval is.

Inmiddels worden auto's voorzien van boordcomputers. Naast zichtbare computers, zoals geïntegreerde navigatiesystemen, zijn auto's ook uitgerust met systemen voor bijvoorbeeld de aansturing van de motor, de remmen, de stuurbekrachtiging enzovoort. Hier sluipt het ICT-duurzaamheidsprobleem de auto-industrie binnen. Meerdere systemen zullen in verbinding staan met de buitenwereld, zoals het binnenkort verplichte eCall-systeem dat bij een aanrijding automatisch de GPS-locatie aan hulpdiensten kan doorgeven,[161] of mogelijk het systeem waarmee de politie op afstand een auto kan uitschakelen.[162]

Koppeling met netwerken brengt een inherent risico op misbruik met zich mee wanneer beveiligingslekken aan het licht komen. Beveiligingsupdates voor software verschijnen echter in een veel hoger tempo dan de auto-industrie gewend is, terwijl auto's veel langer met niet-actuele techniek blijven rijden dan de softwareindustrie gewend is.

## Houdbaarheid en duurzaamheid

Verouderde software in een 'open' omgeving is een toenemend risico. Met de toenemende verwevenheid van software met fysieke voorwerpen wordt duurzaamheid een aandachtspunt, en gebrek daaraan een risico.

Het is belangrijk dat bij de ontwikkeling van producten vooraf wordt nagedacht over de risico's rondom (een gebrek aan) duurzaamheid. Gebeurt dat niet of onzorgvuldig, dan zullen er steeds meer incidenten plaatsvinden die de problematiek onderstrepen, en oplossingen worden steeds lastiger te implementeren.

**Millenniumbug**

Het ICT-duurzaamheidsprobleem is niet nieuw. Aan het eind van de twintigste eeuw ontstond grote onrust over de mogelijke problemen door de datumnotatie (van jaartallen werden alleen de laatste twee cijfers vastgelegd) die in oudere, niet meer onderhouden systemen gebruikt werd. Een groot deel van de automatiseringsindustrie hield zich in die periode bezig met het doorspitten van oude, slecht onderhouden software. Uit angst voor grote problemen werden bijvoorbeeld ten tijde van de jaarwisseling vliegtuigen aan de grond gehouden.[164] Ernstige problemen bleven uiteindelijk achterwege.

159 Volgens Netmarketshare nog zo'n 25 procent, http://marketshare.hitslink.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0, geraadpleegd op 6 juni 2014

160 https://www.ncsc.nl/actueel/nieuwsberichten/stop-met-gebruik-windows-xp.html (geraadpleegd op 10 juni 2014)

161 Zie http://tweakers.net/nieuws/94568/europarlement-stemt-voor-verplichte-invoering-ecall-systeem-in-autos.html, geraadpleegd april 2014.

162 Zie http://tweakers.net/nieuws/94024/eu-overweegt-verplicht-noodstopsysteem-voor-autos.html, geraadpleegd april 2014.

163 http://www.geschiedenis24.nl/andere-tijden/aeveringen/2009-2010/Millenniumbug.html (geraadpleegd op 10 juni 2014)

Op dit moment is er ook nog geen duidelijke oplossingsrichting. Er doemen een aantal vragen op waar nog geen algemene consensus over bestaat:

- Wat mag de redelijke verwachting van de economische levensduur van een geautomatiseerd product zijn?
- Op basis van welke criteria kan gekozen worden om de softwareondersteuning van een product te beëindigen?
- Hoe wenselijk en hoe noodzakelijk is het om internetverbinding voor producten te hebben of te handhaven?
- Hoe kunnen fabrikanten, leveranciers en gebruikers worden aangespoord zich verantwoordelijk te voelen voor het onderhoud van hun producten?
- Is het wenselijk dat gebruikers het onderhoud van hun producten geheel uit handen laten nemen?
- Bij wie ligt aansprakelijkheid voor de risico's rondom niet-verholpen beveiligingslekken?

> *"Verouderde so ware in een 'open' omgeving is een toenemend risico."*

Enkele oplossingen lijken voor de hand te liggen, maar daar zijn kanttekeningen bij te maken:

- Onderhoudsverplichting: het verplichten van leveranciers tot het blijven ondersteunen van software leidt ertoe dat de kosten doorberekend worden aan consumenten. Gezien de snelheid van veranderingen in de ICT zou dit kunnen leiden tot kosten die niet in verhouding staan tot de baten, en een afname van het innovatieve karakter van de industrie.
- Houdbaarheidsdatum: bij het toevoegen van een houdbaarheidsdatum op producten stijgt het bewustzijn van consumenten, maar er is niet noodzakelijkerwijs een verband tussen bewustwording en het ernaar handelen. Er bestaan bovendien grote verschillen in de periode waarin consumenten gebruik blijven maken van apparatuur, waardoor het een optie zou kunnen zijn om een 'self-destruct' in apparaten te bouwen.
- Onzichtbare automatische updates: wanneer producten op afstand van updates worden voorzien, raken gebruikers het beheer over hun eigen product kwijt. Dit leidt tot een aansprakelijkheidsvraagstuk, zeker als de update een keer fout gaat: zijn de gebruikers van het product nog wel verantwoordelijk voor de werking en veiligheid ervan, of heeft de fabrikant dat overgenomen?

Ook het risico op misbruik neemt toe als apparatuur op afstand beheerd wordt. Wanneer het updatemechanisme zelf beveiligingslekken bevat of certificaten van de leverancier worden ontvreemd, kunnen kwaadwillenden mogelijk vervalste updates aanbieden en daarmee de controle krijgen over het systeem.

## Conclusie

De toename van aan internet verbonden apparatuur (inclusief medische apparatuur, maar ook voertuigen, televisies en huishoudelijke apparaten) zal doorzetten. De software in deze apparatuur zal altijd beveiligingslekken bevatten. Veel apparatuur kan niet eenvoudig geüpdatet worden en ook zal niet alle software voor langere tijd door de leverancier onderhouden (kunnen) worden. De apparatuur zal kwetsbaar worden, en gezien de grote afhankelijkheid ontstaat een (potentieel) probleem met het waarborgen van de maatschappelijke veiligheid. «

“HET IS DUIDELIJK DAT HET INTERNET DER DINGEN EEN STEEDS PROMINENTERE PLAATS IN ONZE MAATSCHAPPIJ ZAL INNEMEN”

# 4 INTERNET DER DINGEN

**Steeds meer apparaten verzamelen gegevens over hun omgeving, en wisselen deze gegevens onderling of via het internet uit. Gartner schat dat er in 2020 ruim 25 miljard apparaten verbonden zullen zijn met het internet. Dit concept, dat bekendstaat als het Internet der Dingen, biedt veel toepassingen om ons leven gemakkelijker, veiliger en/of vrijer te maken. In de komende jaren zullen steeds meer apparaten allerlei sensoren bevatten. Met een internetverbinding wisselen ze deze gegevens voortdurend uit. De ontwikkeling staat nu echter nog in de kinderschoenen. Wat gaat er gebeuren als deze toepassingen een grotere vlucht gaan nemen? Worden we dan vierentwintig uur per dag geobserveerd door onze koelkast, kleding en camera's? Hoe gaan we om met beveiliging van gegevens en privacy op deze apparaten, die nauwelijks van beveiliging voorzien zijn?**


| | |
|---|---|
| **Belangen** | Het Internet der Dingen kan het leven gemakkelijker, veiliger en/of vrijer maken, maar kan deze belangen tegelijkertijd ook schaden. |
| **Dreigingen** | Het ontwikkelen van het Internet der Dingen zou kunnen leiden tot onveilige situaties of schendingen van grondrechten. |
| **Weerbaarheid** | Aandacht voor de weerbaarheid en de eventuele grenzen en gevolgen van Internet der Dingen is een belangrijk instrument om de belangen te borgen. |

## De toekomstvisie 'Internet der Dingen'

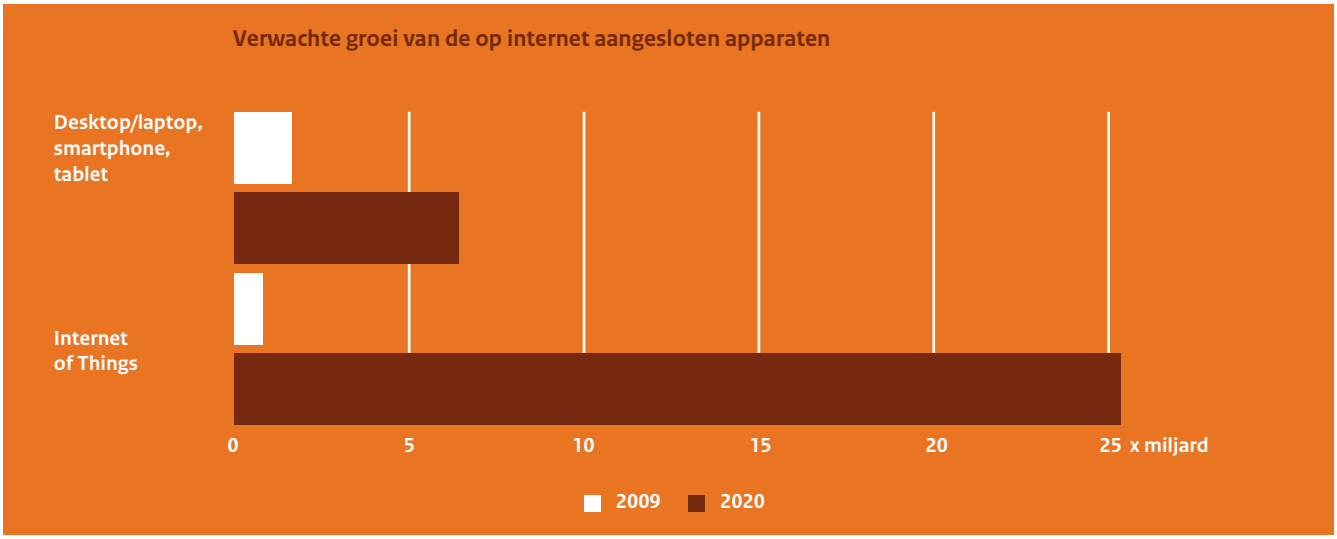
De term 'Internet der Dingen' ('Internet of Things') beschrijft een ontwikkeling waarbij steeds meer apparaten verbonden zijn met elkaar en met internet. Deze apparaten verzamelen gegevens over hun omgeving en wisselen die gegevens onderling uit. Smartphones zijn een populair voorbeeld: in 2013 zijn er meer dan een miljard van verkocht.[164] Ook andere apparaten worden meer en meer verbonden en wisselen gegevens uit. De gegevensverzameling gebeurt met sensoren: die meten zaken als luchtdruk, temperatuur of geluidsniveau. Verschillende apparaten beschikken over verschillende gegevens, die ze uitwisselen via een internetverbinding. Op basis van deze gegevens kunnen de apparaten zelfstandig handelen. Deze manier van werken geeft aanleiding tot uiteenlopende toepassingen. Sommige toepassingen bestaan al, andere kunnen nog ontstaan. Hieronder staan enkele toepassingen geschetst. Het is nu nog niet te zeggen welke toepassingen een vlucht zullen nemen; dit overzicht is mede daarom verre van volledig.

Toepassing: Huizen reageren op bewoners De apparaten die mensen in huis hebben, bieden goede mogelijkheden voor het uitwisselen van gegevens. Daardoor kunnen bewoners hun leven gemakkelijker, veiliger en milieuvriendelijker maken. Op beurzen is deze technologie al in actie te zien,[165] en meerdere energieleveranciers bieden al slimme thermostaten aan.[166] Een koelkast kan zelf detecteren welke producten hij bevat. Is er een product op of over datum? Dan informeert de koelkast de bewoner, en bestelt hij zelf direct nieuwe producten. Apparaten die onderhoud vergen of waarbij een defect dreigt, kunnen de eigenaar informeren en zelfstandig een afspraak met een onderhoudsmonteur plannen. Een thuisthermostaat detecteert wanneer bewoners aanwezig zijn, geeft hen inzicht in hun energieverbruik en laat hen het energieverbruik centraal beheren. De thermostaat besluit zelf wanneer bepaalde energie-intensieve activiteiten zoals het drogen van een was of het draaien van de afwasmachine het beste kunnen plaatsvinden, zowel voor het milieu als voor de portemonnee van de bewoner.

164 Bron: http://webwereld.nl/markrends/81100-in-1-jaar-1-miljard-smartphones-verscheept (geraadpleegd op 22 mei 2014)

165 Zie bijvoorbeeld: http://www.nu.nl/gadgetbeurs-ces/3000476/huis-van-toekomst-jaar-nederland.html (geraadpleegd op 22 mei 2014).

166 Zie bijvoorbeeld http://www.consumentenbond.nl/energie/extra/energiemeter/ (geraadpleegd op 22 mei 2014).




*Figuur 16. Verwachte groei van de op internet aangesloten apparaten[167] (x miljard)*

Toepassing: De openbare ruimte is veiliger Door het combineren van gegevens die verschillende apparaten verzamelen, kan zowel de algemene als de persoonlijke veiligheid in de openbare ruimte worden vergroot. Al in 2005 detecteerde de gemeente Groningen met behulp van microfoons signalen van agressie of angst in het uitgaanscentrum.[168] Deze gegevens werden toen alleen gedeeld met de politiemeldkamer. In de toekomst zouden deze bijvoorbeeld ook via een app bij bezoekers van het centrum terecht kunnen komen, waardoor zij geïnformeerd kunnen besluiten bepaalde gebieden te mijden. In tweede instantie kan deze app ook zelf gegevens verzamelen via de geluids- en locatiesensoren van de smartphone. De politie en andere bezoekers kunnen zo ook agressie en angst waarnemen op plaatsen die niet met de door de politie geïnstalleerde microfoons te bereiken zijn.

Toepassing: Medische ingrepen zijn minder ingrijpend Met behulp van sensoren die gegevens uitwisselen, kunnen patiënten na een operatie eerder naar huis. Ze slikken een elektronische 'pil' die hun fysieke toestand voortdurend monitort en de resultaten deelt met de betrokken arts. Zulke elektronische pillen worden al geleverd en beperkt gebruikt.[169] Als een patiënt afhankelijk is van anderen, zoals kinderen, gehandicapten of ouderen, kunnen de gegevens ook gedeeld worden met hun betrokken familieleden of andere mantelzorgers. Voor chronische patiënten kan een dergelijke pil ook gebruikt worden voor het langdurig bijhouden van hun fysieke gesteldheid.

Toepassing: Verkeer stroomt beter door Het combineren van locatiegegevens van auto's, mobiele telefoons en autonavigatiesystemen maakt het mogelijk om sneller en effectiever te reageren op auto-ongelukken, dreigende verstoppingen en files. In de afgelopen periode zijn meerdere van dit soort dynamische systemen op de markt gekomen.[170] Navigatiesystemen kunnen bestuurders adviseren een andere route te nemen als ze afrijden op een plaats waar veel bestuurders stilstaan. Zo wordt voorkomen dat files ontstaan of uitbreiden. Automobilisten komen hierdoor eerder op hun bestemming. Doordat ze korter stilstaan, stoten hun auto's ook minder uitlaatgassen uit.

## Hoe werkt het Internet der Dingen op hoofdlijnen?

In het Internet der Dingen worden apparaten voorzien van steeds meer sensoren die hun omgeving waarnemen. De apparaten met deze sensoren zitten op steeds meer plaatsen en kunnen op al die plaatsen gegevens vergaren. De apparaten zijn verbonden met het internet of elkaar en wisselen zo verzamelde data uit. Sommige van deze apparaten nemen ook autonoom beslissingen op basis van verzamelde en ontvangen gegevens.

Sensoren nemen de omgeving waar Apparaten gebruiken sensoren om gegevens over de omgeving te verzamelen. Een sensor is een elektronisch 'zintuig', waarmee het waarnemen van een bepaald aspect van de omgeving mogelijk wordt gemaakt. Aspecten die sensoren waar kunnen nemen, zijn bijvoorbeeld locatie (met een GPS-sensor), temperatuur, geluidsniveau, bloeddruk of samenstelling van de lucht. Sommige sensoren kunnen zeer gedetailleerde informatie waarnemen, zoals microfoons of camera's.

Steeds meer apparaten beva□en sensoren Omdat steeds meer apparaten sensoren bevatten, kunnen sensoren op steeds meer plaatsen gegevens verzamelen. Smartphones bevatten veel verschillende sensoren, zoals een microfoon, camera, GPS-sensor, druksensor, versnellingsmeter, kompas en lichtsensor. De verwachting is

167 Bron: Gartner (november 2013).

168 Bron: 'Luisterende' camera succesvol h□p://www.volkskrant.nl/vk/nl/2686/Binnenland/article/detail/667972/2005/06/03/Luisterende-rsquo-camera-succesvol.dhtml (geraadpleegd op 22 mei 2014).

169 Zie bijvoorbeeld: Hi-Tech Health Monitor Works When You Swallow It, h□p://sanfrancisco.cbslocal.com/2014/02/23/new-digital-health-monitor-actually-works-from-inside-the-body-you-swallow-it/ (geraadpleegd op 22 mei 2014).

170 Zie bijvoorbeeld: h□p://www.tomtom.com/en_us/services/live/hd-tra□c/ (geraadpleegd op 22 mei 2014).

dat steeds meer apparaten om ons heen ook sensoren zullen gaan bevatten, zoals huisapparatuur en auto's. Twee categorieën hebben een aparte naam gekregen: wearables en swallowables. Wearables zijn kledingstukken die sensoren bevatten en gegevens uitwisselen, zoals een t-shirt dat de lichaamstemperatuur meet. Een ander populair voorbeeld is Google Glass. Swallowables zijn apparaten die via de mond worden ingenomen en gegevens uitwisselen. Deze apparaten nemen de fysieke gesteldheid van de inslikker waar: een voorbeeld is de elektronische pil uit de vorige sectie.

### Deze apparaten wisselen gegevens uit met elkaar en het internet

Apparaten worden steeds vaker van een internetverbinding voorzien, of worden contactloos uitgelezen via near-field communication (NFC). Zo wisselen apparaten verzamelde gegevens uit, of verzenden ze deze naar een centrale server. De onderlinge uitwisseling van gegevens valt in een van drie categorieën:

- Dezelfde apparaten in bezit van verschillende personen wisselen onderling gegevens uit. Een voorbeeld is de uitwisseling van locatiegegevens tussen autonavigatiesystemen, zoals beschreven in de vorige sectie.
- Verschillende apparaten in bezit van dezelfde persoon wisselen onderling gegevens uit. Een voorbeeld is een auto die alleen van het slot gaat als de smartphone van de eigenaar in de buurt is.
- Verschillende apparaten in bezit van verschillende personen wisselen onderling gegevens uit. Een voorbeeld is het met verschillende apparaten verzamelen van informatie over het geluidsniveau in een uitgaansgebied, zoals beschreven in de vorige sectie.

Deze categorieën kennen elk hun eigen vraagstukken met betrekking tot interoperabiliteit, privacy en beveiliging. Zo is het eenvoudiger om gegevens uit te wisselen tussen dezelfde apparaten, omdat daarvoor geen aparte standaard voor gegevensuitwisseling hoeft te worden gebruikt. Ook vormt het uitwisselen van gegevens tussen apparaten van verschillende eigenaren over het algemeen een groter privacyrisico dan tussen apparaten van dezelfde eigenaar.

### Deze apparaten bieden inzicht en handelen soms autonoom

Naast het bieden van inzicht in de omgeving of het eigen gedrag, handelen sommige apparaten ook zelfstandig. Op basis van verzamelde en uitgewisselde informatie voert het apparaat acties uit om een proces in gang te zetten of juist in te grijpen in een bestaand proces. Voorbeelden bestaan in allerlei domeinen. Een auto die detecteert dat hij te dicht op zijn voorganger rijdt, zal niet alleen een piepsignaal geven, maar ook automatisch afremmen. Een koelkast die vaststelt dat de melk over de houdbaarheidsdatum is, stuurt niet alleen een bericht aan de bewoner maar bestelt ook nieuwe melk. Een elektronische pil die het herstel van een patiënt na een operatie monitort, alarmeert bij complicaties direct de verantwoordelijke arts.

> *"Thermostaten besluiten zelf wanneer bepaalde energie-intensieve activiteiten het beste kunnen plaatsvinden."*

## Welke risico's met betrekking tot het Internet der Dingen worden nog onvoldoende onderkend?

De hiervoor geschetste scenario's bieden een positief beeld op de toekomst van het Internet der Dingen, waarbij echter wel kanttekeningen te plaatsen zijn. De ontwikkelingen zullen leiden tot maatschappelijke discussie. Door het tijdig voeren van deze discussie, kunnen we de uitkomsten meewegen in de verdere ontwikkeling van het Internet der Dingen.

### Koppelen en gegevensuitwisseling kennen beveiligings- en privacyrisico's

De meeste verzamelde gegevens in het Internet der Dingen kennen op het oog een beperkt privacyrisico. Echter, in samenhang met andere gegevens kan het resulterende risico vele malen groter zijn. Door het uitwisselen en combineren van gegevens kunnen deze bijvoorbeeld opeens wel tot een persoon te herleiden zijn. Ook kunnen gegevens gecombineerd een verhaal vertellen over de persoon dat uit de afzonderlijke gegevens niet af te leiden is. In het Internet der Dingen zijn de verzamelde gegevens omvangrijker, intiemer en breder verspreid dan eerder.

Ieder apparaat dat software bevat en aan het internet gekoppeld is, is kwetsbaar. Veel van de apparaten uit het Internet der Dingen zijn ook nog eens geen volwaardige computer. Van een apparaat dat beperkte opslag- en rekencapaciteit heeft, valt niet te verwachten dat het om kan gaan met complexe cryptografische protocollen. Dat betekent dus dat het manipuleren of onderscheppen van uitgewisselde gegevens een nog groter risico vormt dan voor klassieke apparaten als desktops of tablets.

Daarnaast is bij veel van de nieuw verbonden apparaten niet duidelijk hoe ze worden voorzien van beveiligingsupdates. Wordt er een lek gevonden in de besturingssoftware, dan zal dat niet zonder meer te repareren zijn. Bij het ontwerp van zulke apparaten dienen conservatieve beveiligingskeuzes gemaakt te worden, bijvoorbeeld met betrekking tot gekozen sleutellengtes. Dat staat echter op gespannen voet met de bovengenoemde beperkte rekencapaciteit. Meer informatie hierover is te vinden in het verdiepingskatern Duurzaamheid ICT.

Het is moeilijk voor mensen om controle te houden over de grote en veelzijdige verwerking van gegevens in het Internet der Dingen. Een gebruiker zal ten minste controle willen houden over welke gegevens er verzameld worden en met wie die worden uitgewisseld. Veel van de genoemde apparaten bieden standaard geen mogelijkheid voor beheer van de verzamelde gegevens.

**De alomtegenwoordigheid van sensoren die data verzamelen kan een gevoel van constante en onzichtbare surveillance geven** Met het Internet der Dingen worden aspecten van het leven waargenomen die tot voor kort onttrokken werden aan voortdurende observatie: het gedrag, de fysieke gesteldheid en de thuisomgeving zijn drie voorbeelden. Het is lang niet altijd duidelijk wie er uiteindelijk allemaal kan beschikken over de verzamelde gegevens: worden gegevens verkocht aan marketeers, of zijn ze in te zien door de overheid? Iemand weet vaak niet wanneer en door wie hij gadegeslagen wordt. Dit kan een gevoel oproepen van constante en onzichtbare surveillance.

Personen die zich geobserveerd voelen, gaan sociaal wenselijker gedrag vertonen.[171] Aan de ene kant is dit positief, omdat op die manier bijvoorbeeld onwenselijk gedrag voorkomen kan worden. Aan de andere kant wordt de ruimte om een onbespied leven te leiden zo wel verregaand beknot.

**Voor tegenstanders zal het steeds moeilijker worden zich te onttrekken aan de opkomst van het Internet der Dingen** Het Internet der Dingen zal een steeds prominentere plaats innemen in ons leven: persoonlijk, sociaal en professioneel. Het is denkbaar dat sommigen, gelet op de al geschetste bezwaren, liever niet deelnemen aan deze ontwikkeling. Dit zal niet eenvoudig zijn: zelfs als ze geen apparaten bezitten die deel vormen van het Internet der Dingen, dan nog zullen ze voortdurend waargenomen worden door de apparaten van anderen in hun omgeving.[172]

In het geval van competitieve momenten zoals examens speelt deze vraag ook. Nu is het nog mogelijk om apparaten niet te gebruiken en in te leveren. Echter, het is denkbaar dat zulke apparaten ooit niet te verwijderen zullen zijn, zoals implantaten, of dat deze zo alomtegenwoordig zijn dat afgeven niet nodig wordt geacht. Hoe gaan we dan om met de achterstand die deelnemers oplopen door zulke apparaten niet te willen of kunnen gebruiken?

## Waar staan we momenteel in de ontwikkeling van een Internet der Dingen?

**Er zijn al veel apparaten met sensoren verbonden met het internet** Er bestaan momenteel al veel apparaten die beschikken over een internetverbinding en een of meer sensoren. Steeds meer mensen beschikken over een smartphone, en zoals eerder gezegd zitten deze apparaten vol sensoren. Moderne auto's beschikken ook over zowel een internetverbinding als een uitgebreid scala aan sensoren. Ook thuisthermostaten worden steeds vaker in een met internet verbonden uitvoering geleverd. Voorbeelden hiervan zijn Nederlandse energieleveranciers die slimme thermostaten aanbieden[173] en de producten van het Amerikaanse bedrijf Nest, dat is overgenomen door Google.[174]

**Deze apparaten wisselen nog maar beperkt gegevens uit** Hoewel steeds meer apparaten verbonden zijn met het internet en elkaar, wisselen ze onderling nog maar beperkt gegevens uit. Daardoor treden de geschetste risico's nog maar beperkt op. De nu al bestaande uitwisselingen bestaan meestal uit apparaten of applicaties van dezelfde leverancier. Een voorbeeld is een elektronische pil die uit te lezen is met een app die de maker van de pil ook levert. Volwassen standaarden voor dergelijke gegevensuitwisseling tussen apparaten ontbreken. Daardoor is het uitwisselen tussen producten van verschillende leveranciers nog maar beperkt mogelijk.

## Conclusie

De ontwikkeling naar een Internet der Dingen bevindt zich nog in een pril stadium. Het feit dat we weten dat steeds meer apparaten met sensoren onderling of via internet gegevens uit zullen wisselen, betekent nog niet dat we weten op welke manieren en onder welke voorwaarden dit zal gebeuren. Het is nu nog niet te zeggen welke toepassingen een vlucht zullen nemen. Wel is duidelijk dat het Internet der Dingen een steeds prominentere plaats in onze maatschappij zal innemen.

Voor de apparatuur in het Internet der Dingen is het in voorgaande katern geschetste ICT-duurzaamheidsprobleem zeer relevant. Immers de apparatuur is gekoppeld en de software in de apparatuur zal beveiligingslekken bevatten. In potentie kunnen belangen geschaad gaan worden.

Het is ontegenzeggelijk dat de voordelen van het Internet der Dingen groot kunnen zijn, zowel voor de individuele consument, die meer grip op zijn energieconsumptie krijgt of meer gebruikersgemak, als voor de maatschappij, waar problemen eerder opgespoord of makkelijker opgelost kunnen worden. Om verantwoordelijk om te gaan met deze ontwikkeling, is aandacht nodig voor de beveiligings- en privacyaspecten. Het moet duidelijker worden wat de spelregels zijn waaronder het Internet der Dingen gaat functioneren, en of het veilig en verplicht is. «

171 Aan het einde van de 18e eeuw formuleerde Jeremy Bentham deze gedachte al in zijn geschrift 'Panopticon'. Hij stelt hierin een gevangenis voor waarin elke gevangene constant gadegeslagen kan worden. Zie verder: http://cartome.org/panopticon2.htm (geraadpleegd op 22 mei 2014)

172 Deze kwestie speelt ook rond Google Glass. Google heeft daarom etiquetteregels opgesteld voor het gebruik van de bril: https://sites.google.com/site/glasscomms/glass-explorers (geraadpleegd op 22 mei 2014).

173 Bron: http://www.consumentenbond.nl/energie/extra/energiemeter/ (geraadpleegd op 22 mei 2014).

174 Bron: https://investor.google.com/releases/2014/0113.html (geraadpleegd op 22 mei 2014).

“HET GEBRUIK VAN ANONIMISERINGS-TECHNIEKEN MAAKT HET MOEILIJK OM DE VERSPREIDERS VAN RANSOMWARE TE ACHTERHALEN”

# 5 RANSOMWARE EN CRYPTOWARE

**Ransomware is steeds innovatiever en agressiever, en ook de gebruikte betaalmiddelen zijn steeds geavanceerder. In de afgelopen jaren is ransomware sterk in opkomst, en vanaf eind 2013 in een bijzondere vorm: cryptoware. In Nederland zijn veel ransomware-besme□ingen en nog maar weinig cryptoware-besme□ingen geconstateerd, maar in omliggende landen komen veel cryptoware-besmettingen voor. De opkomst van cryptoware is verontrustend, aangezien betaling van het losgeld in een beperkt deel van de gevallen lijkt te helpen. Dit in tegensteling tot klassieke ransomware.**

**Ransomware en in het bijzonder cryptoware hanteren een zeer lucratief businessmodel, dat een inkijk gee□ in de verdergaande professionalisering van de cybercrime-sector. Actieve preventie en een brede maatschappelijke aanpak zijn noodzakelijk, temeer nu het gijzelen van data steeds eenvoudiger wordt.**


**Belangen** Ransomware wordt op steeds meer platforms toegepast. Cryptoware maakt zijn opmars in het buitenland en bedreigt ook Nederland.

**Dreigingen** Ransomware is een hardnekkige vorm van cybercrime. Ransomware en in het bijzonder cryptoware hanteren een lucratief businessmodel.

**Weerbaarheid** Klassieke ransomware is relatief makkelijk te verwijderen. Het tre□en van correctieve maatregelen voor cryptoware is vrijwel onmogelijk. Ransomware en cryptoware zijn een prioriteit onder opsporingsdiensten.

## Wat is ransomware?

Ransomware, 'gijzelingssoftware', is een hardnekkige vorm van malware, die toegang tot de computer blokkeert. Het slachtoffer is niet meer in staat om gebruik te maken van het systeem: er is alleen maar een dreigende boodschap te zien. Hierin wordt het slachtoffer aangezet om een betaling te doen. Vaak doen de digitale afpersers zich voor als de politie, maar ook de namen van andere autoriteiten, zoals in Nederland het Koninklijk Huis of Buma/Stemra, worden misbruikt.

Ransomware is geen specifiek Nederlands fenomeen; de verspreiding ervan gebeurt wereldwijd. Eenmaal geïnstalleerd op een computer bepaalt de ransomware met behulp van plaatsbepalingstabellen in welk land 'zijn' geïnfecteerde systeem zich bevindt. Daarmee kan een boodschap worden vertoond die aansluit bij het betreffende land. Als de locatie niet bepaald kan worden, wordt volstaan met een scherm dat afkomstig lijkt van Europol of Interpol.

Sinds 2012 komt ransomware in Nederland zo vaak voor dat de Nationale Politie er in internationaal verband een grootschalig onderzoek naar is begonnen.[175] Voor slachtoffers geldt het devies: betalen is zinloos, verwijderen kan immers eenvoudig met een gratis antivirustool. Ook bieden leveranciers diverse oplossingen voor ransomware. Voor cryptoware ligt dit lastiger.

175 Zie h□p://www.politie.nl/onderwerpen/ransomware.html

**Hoe gaan ransomware-criminelen te werk?**
De modus operandi van ransomware is een combinatie van techniek en social engineering.

De technische component bestaat vooral uit het continu (door) ontwikkelen van de programmatuur zelf, het gebruik van zogenoemde exploitkits en het gecoördineerd verzamelen van verkregen betaalcodes.[2] De computer van een slachtoffer raakt doorgaans besmet doordat hij een webpagina bezoekt en ongewild wordt doorgeleid naar een pagina waarop een exploitkit de kwetsbaarheden van zijn computer verkent, die vervolgens worden uitgebuit om de ransomware te plaatsen.

De social engineering bestaat uit het onder druk zetten van potentiële slachtoffers. Hiertoe moet de boodschap overtuigend overkomen. Dit betekent dat kennis van de taal en de lokale autoriteiten noodzakelijk is. In sommige varianten wordt verwezen naar (zogenaamd) door het slachtoffer bezochte websites, waarbij vooral pornosites worden weergegeven. Schuld- en schaamtegevoel zijn de belangrijkste emoties waarop ransomware-criminelen inspelen.

Overigens worden bij cryptoware dergelijke valse redenen zelden waargenomen. Hier verschijnt een melding namens de criminelen, nadat eerst ongemerkt de belangrijkste bestanden zijn versleuteld. Vervolgens wordt druk toegepast, bijvoorbeeld door een klok te tonen die afteelt: indien het slachtoffer voor de deadline niet betaalt, zou het onmogelijk worden de bestanden te ontsleutelen.

## Trends & ontwikkelingen

Hoe ransomware vernieuwend blijft Een vorm van cybercrime die grotendeels leunt op oplichting is niet gebaat bij teveel bekendheid bij potentiële slachtoffers. Daders moeten daarom blijven innoveren. In de periode van april 2013 tot maart 2014 is een aantal innovaties op het gebied van ransomware waargenomen. Sommige vormen schakelen de webcam van het slachtoffer in, zodat er beelden van de persoon in kwestie worden opgenomen en deze zichzelf op het scherm ziet. Met audiobestanden kan een slachtoffer nu in zijn eigen taal vermanend worden toegesproken. En werden slachtoffers in het verleden vaak beschuldigd van het kijken naar kinderporno, sinds 2013 tonen sommige varianten van ransomware zelf kinderporno op het scherm van het slachtoffer.

Ook in de wijze waarop het losgeld moet worden betaald is meer variatie gekomen. Van betaling per sms werd in 2011 overgestapt op betaling met vouchercodes. Inmiddels eisen sommige vormen van ransomware betaling middels bitcoins. De bijbehorende anonimisering maakt het lastiger de daders te achterhalen. Betaling in bitcoins vraagt echter wel meer technische vaardigheden van het slachtoffer dan betalen met vouchercodes. Dit kan er toe leiden dat slachtoffers minder snel (kunnen) betalen.

Een derde ontwikkeling is de opkomst van ransomware op smartphones. Mobiele ransomware werd eind 2013 op Android-toestellen aangetroffen.

Opkomst cryptoware De nieuwste en meest opvallende ontwikkeling in ransomware is de opkomst van cryptoware. Medio vorig jaar werd de eerste variant gesignaleerd in Amerika, genaamd CryptoLocker.[177] Eind 2013 werd cryptoware voor het eerst in Nederland waargenomen. CryptoLocker wordt met name in de VS en andere Engelstalige landen verspreid[178] en lijkt sterk gericht op bedrijven. Later werden ook steeds meer particulieren slachtoffer.

Cryptoware vergrendelt niet de computer zelf, maar versleutelt bestanden van de gebruiker. Niet alleen bestanden op de harde schijf van de computer, maar ook op de virtual (cloud) disk, externe harde schijven, usb-sticks en bedrijfsnetwerken kunnen door een besmetting worden versleuteld – inclusief 'warm' aangesloten backupschijven. Het bereik van de versleuteling hangt af van de privileges van de getroffen gebruiker binnen het betreffende netwerk.

Het grote verschil met de eerder besproken vormen van ransomware is dat verwijderen van de malware niet helpt: de bestanden zijn en blijven versleuteld. Hiervoor wordt gebruik gemaakt van diverse krachtige encryptie-algoritmen. Voor ontsleuteling is een unieke decodeersleutel nodig, die voor het slachtoffer slechts enkele dagen te koop is. In het geval van CryptoLocker vervijfvoudigt de vraagprijs na 72 uur. Betaling leidt niet zonder meer tot het vrijgeven van de bestanden. Verwijdering van de malware (door antivirussoftware) bemoeilijkt het terugkrijgen van de files. De daders achter Cryptolocker hebben zelfs een 'helpdesk' opgezet waar slachtoffers hun privésleutel kunnen kopen.

Net als bij ransomware is de hoogte van het losgeld relatief laag, bedragen van honderden euro's zijn gebruikelijk. De meeste slachtoffers zijn financieel in staat om de betaling te voldoen, zolang ze de deadline niet overschrijden. Dit geldt zeker voor bedrijven en overheden, waarbij de kleinere partijen een groter risico op infectie lopen doordat hun bescherming tegen malware in veel gevallen lager is. Aangezien de bestanden op geen enkele andere wijze teruggekregen kunnen worden, moet het slachtoffer zijn verlies nemen of het losgeld betalen. Hierdoor lijkt het businessmodel achter cryptoware nog winstgevender dan dat van eerdere ransomware. Opsporingsinstanties verwachten dan ook een toename van deze vorm van cybercrime in de nabije toekomst.

176 Zie http://www.politie.nl/onderwerpen/ransomware.html

177 Zie http://nakedsecurity.sophos.com/2013/10/18/CryptoLocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/
178 http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

| Casus | Duur campagne/ onderzoek (dagen) | Aantal besme□e computers | Aantal betalingen | Geëist losgeldbedrag[179] | Omzet tijdens periode[180] (ordegroo□e) |
|---|---|---|---|---|---|
| **Symantec: Reveton** | 18 | 500.000 | ± 15.000 | € 73 - € 146 | € 1.500.000 |
| **Symantec: RansomLock** | 41 | 68.000 | 1.972 | € 146 | € 300.000 |
| **Kafeine: Reveton** | 2 | 25.120 | 825 | € 87 | € 70.000 |
| **Dell/Spagnuolo: CryptoLocker[181]** | 100 | 200.000 - 250.000 | 771 | € 68 - € 1.167 (trend: € 219) | € 277.000 - € 715.000 |

*Tabel 6. Vergelijking van ransomwarecampagnes in termen van omvang en gescha e omzet.*

## Omvang en schade

Diverse onderzoeken door de antivirus-industrie en de politie laten zien dat zeker drie procent van de ransomware-slachtoffers (klassieke verschijningsvorm) het losgeld betaalt.[182] Hoeveel slachtoffers Nederland kent, is onbekend, omdat lang niet elk slachtoffer aangifte doet. De betalingsbereidheid in Nederland was in het verleden, in vergelijking met de ons omringende landen, opvallend hoog. Sinds een grote bewustwordingscampagne in het kader van Alert Online lijkt deze te zijn afgenomen.

De Nederlandse politie nam in 2012 gedurende een maand 270 aangiften op van besmettingen met ransomware die het toenmalige KLPD-logo vertoonde. Van de aangevers zei meer dan 18 procent het losgeld te hebben betaald.[183] Bij de Duitse politie waren op een zeker moment in 2013 70.000 besmettingen bekend, waarbij 2.400 mensen (3,4 procent) het losgeld betaalden.

> *"Het gebruik van anonimiseringstechnieken maakt het moeilijk om de verspreiders van de ransomware te achterhalen."*

Ook de antivirusindustrie heeft cijfers over de opbrengst van ransomware. Zo stelt Symantec in een rapport uit 2012 dat een minder bekende ransomware-variant (RansomLock) in ruim een maand 68.000 computers besmette. Een wereldwijd 500.000 computers in achttien dagen tijd. Een bijzonder inzicht geeft onderzoeker 'Kafeine' via Krebsonsecurity.[184] In 2012 is andere criminele organisatie infecteerde, gebruikmakend van de bekendere ransomware variant Reveton, onderzoek gedaan aan de infrastructuur van een Reveton-variant, die actief was in elf landen. De opbrengst per land werd inzichtelijk gemaakt. In de twee onderzochte dagen werd per dag ruim 35.000 euro succesvol afgeperst, waarvan 5.000 euro in Nederland. De betalingsbereidheid van Nederlanders, rond de 4,5 procent was opvallend hoog te noemen.

Over de omvang van cryptoware-besmettingen is minder bekend. Wel is er een inzicht gevende casestudy, waarbij in het laatste kwartaal van 2013 tussen de 300.000 en 700.000 euro werd buitgemaakt.[185] Onderzoekers schatten (op basis van zogenoemde sinkhole-data) dat in de eerste honderd dagen dat CryptoLocker werd verspreid, wereldwijd 200.000 tot 250.000 computers werden geïnfecteerd. Onderzoeker Michele Spagnuolo meldde dat de losgeldeis die werd waargenomen stabiliseerde op 300 dollar: iets meer dan het losgeld bij 'klassieke' ransomware dus. Het is nog niet mogelijk uitspraken te doen over de winstgevendheid van CryptoLocker ten opzichte van 'klassieke' ransomware.

179 Omgerekend van dollar naar euro met wisselkoers $1 - €0,73.
180 Gezien de hoeveelheid onzekere factoren is hier een afgerond 'best estimate' weergegeven.
181 In dit onderzoek is alléén gekeken naar de losgeldbetalingen via bitcoin. CryptoLocker biedt echter ook alternatieve betaalwijzen. Hierdoor is de gemaakte omzet met zekerheid (veel) groter.
182 Symantec, 2012, Ransomware: A Growing Menace h□p://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf
183 Dit speci□eke hoge percentage houdt mogelijk mede verband met de motivering om aangi□e te doen.
184 h□p://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation/
185 Dell SecureWorks berekende deze marges aan de hand van de dagkoers van de bitcoin over die periode; een variatie tussen de 310 en 799 dollar per bitcoin (2013).

Over de omvang van cryptowarebesmettingen in Nederland is nog weinig bekend. Bij de politie zijn enkele tientallen aangiftes binnengekomen, met name van kleinere organisaties. Enkele slachtoffers betaalden losgeld, maar de meesten hebben alleen al hun software opnieuw laten installeren.

**Criminelen achter ransomware**

Het aantal groepen dat betrokken is bij de verspreiding van ransomware is onbekend. Schattingen worden gemaakt door de ransomware te analyseren en op te delen in families aan de hand van de karakteristieken, maar dit is geen waterdicht systeem. In eerste instantie ging het waarschijnlijk om enkele criminele groepen, maar nadat de broncode van Reveton op de markt kwam, nam het aantal groepen snel toe. Europol[186] zag begin 2013 twee of drie groepen die actief waren in de verspreiding van ransomware, aan het eind van dat jaar leken er tien groepen actief te zijn. Een ransomwarebende heeft veel verschillende specialisten nodig, zoals exploitkit-operators, trackers en botmasters. Voor het aanpassen van de malware aan verschillende landen zijn vertalers en webdesigners nodig. Om herkenning door antivirus-programmatuur te voorkomen, moet de malware steeds opnieuw worden aangepast door 'packers', ook wel 'malware-obfuscators' genoemd. Voor het witwassen van het buitgemaakte geld worden vaak professionele witwasorganisaties ingehuurd. De online-processen worden mogelijk gemaakt door onbewuste facilitators, maar ook door bewust criminele dienstverleners (zie hoofdstuk 2: Actoren). Te denken valt aan advertentiebureaus, webhosters, (bulletproof) hostingproviders, forumhosters en domainregistrars.

## (On)mogelijkheden in de aanpak

Vanwege het innovatieve karakter, de grootschalige toepassing en de groeiende maatschappelijke schade zien opsporingsdiensten in Nederland en omringende landen de aanpak van ransomware en cryptoware als een van hun belangrijkste prioriteiten. Hierbij lopen zij tegen een aantal obstakels aan. Het gebruik van anonimiseringstechnieken (in praktijk: proxies en VPN's) maakt het moeilijk om de verspreiders van de ransomware te achterhalen; voor elke proxy die in een ander land staat moet uiteindelijk een nieuw rechtshulpverzoek worden gedaan. Anonimisering van de betalingswijze, zoals door het gebruik van vouchercodes en cryptocurrencies, maakt het lastig het geldspoor te volgen. Ook het feit dat wetgeving verschilt van land tot land, vertraagt onderzoeken naar ransomware aanzienlijk.

Nederlandse instanties werken bij de bestrijding van ransomware samen met internationale partners zoals Europol. In het binnenland wordt energie gestoken in de samenwerking tussen politieeenheden. De bestrijding van ransomware vraagt echter om een bredere aanpak dan alleen strafrechtelijk onderzoek. Er is intensieve samenwerking nodig met partijen die elk hun eigen interventies uitvoeren, waarbij het vergroten van de weerbaarheid de meeste winst op zal leveren.

In 2013 is een grote landelijke awarenesscampagne tegen ransomware gevoerd samen met voucherverkooppunten.[187] Kopers van betaalcodes werden erop geattendeerd dat betaling niet leidt tot vrijgave van het systeem en dat de computer beter op een andere wijze van het virus geschoond kan worden. Ook het televisieprogramma Opsporing Verzocht besteedde aandacht aan de opkomst van ransomware. Sinds de opkomst van cryptoware is de boodschap vooral gericht op het belang van het maken van externe reservekopieën.

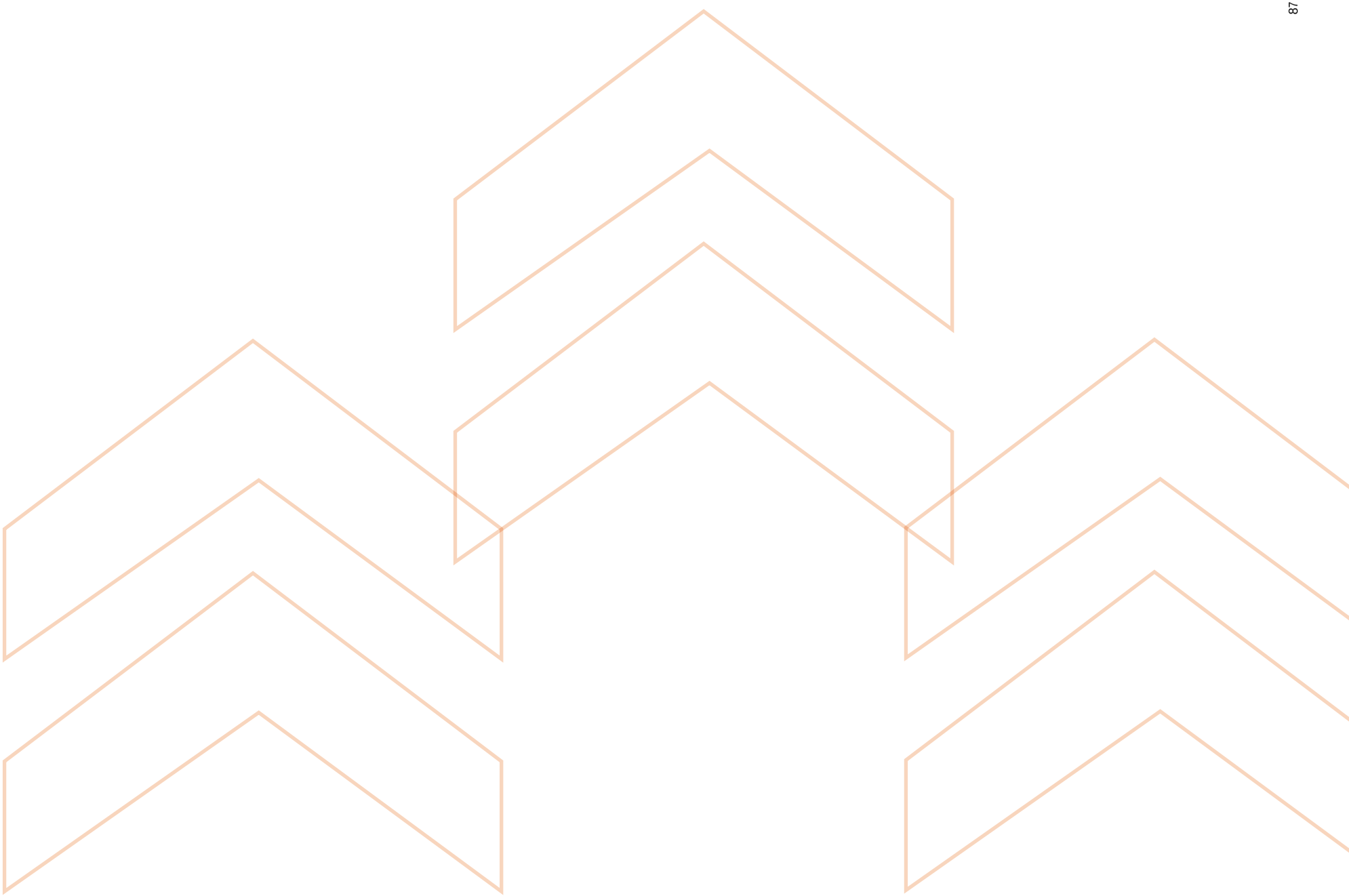
## Conclusie

Ransomware is een hardnekkige vorm van cybercrime, die door constante innovatie voorlopig niet weg te denken is uit de wereld van cybersecurity. Ransomware en in het bijzonder cryptoware hanteren een zeer lucratief businessmodel, hetgeen een inkijk geeft in de verdergaande professionalisering van de cybercrime-sector.

Het gijzelen van systemen en data wordt steeds eenvoudiger. Opsporing van daders helpt, maar blijkt niet voldoende om slachtofferschap te voorkomen. Samenwerking tussen publieke en private partijen en een integrale aanpak zijn mogelijke maatregelen om de weerbaarheid te vergroten. «

186 https://www.europol.europa.eu/sites/default/files/publications/policeransomware-threatassessment.pdf

187 http://www.politie.nl/binaries/content/assets/politie/documenten-algemeen/onderwerpteksten/politievirus-factsheet-winkeliers.pdf



# BIJLAGE 1 » NCSC-STATISTIEKEN

**Deze bijlage biedt een overzicht van de door het NCSC afgehandelde responsible disclosures, beveiligingsadviezen en incidenten. Hierover worden statistieken berekend en deze worden vergeleken met eerdere rapportageperiodes om trends en overige ontwikkelingen te identi□ceren.**

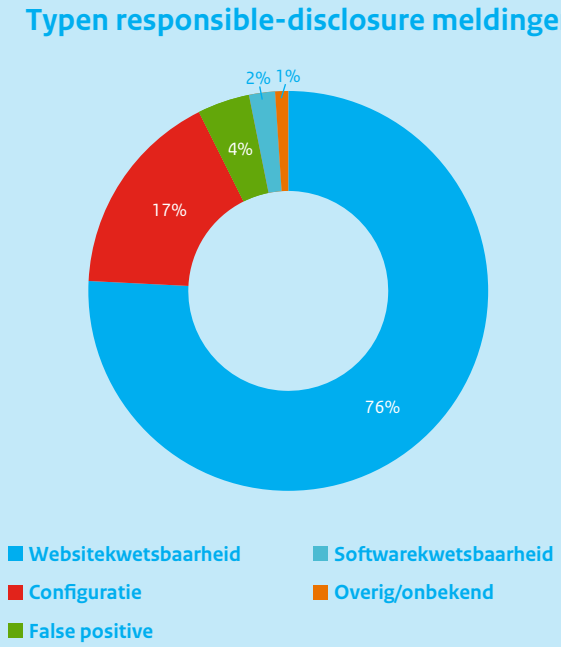
Het NCSC faciliteert het doen van responsible-disclosuremeldingen voor zowel haar eigen infrastructuur als die van de Rijksoverheid en enkele private partijen, het uitbrengen van beveiligingsadviezen voor onze deelnemers en het afhandelen van cybersecurityincidenten. Hierover zijn voor deze rapportageperiode statistieken berekend die hieronder worden gepresenteerd. Door deze statistieken te vergelijken met eerdere rapportageperiodes kunnen trends en overige ontwikkelingen worden geïdentificeerd.

## Responsible disclosure

In de eerste helft van 2013 introduceerde het NCSC een leidraad responsible disclosure en een responsible-disclosurepolicy op de eigen website (https://www.ncsc.nl/security). Met de introductie van responsible disclosure draagt het NCSC bij aan het op een verantwoordelijke wijze melden en afhandelen van kwetsbaarheden in informatiesystemen en (software)producten. Het streven is daarbij om melder en getroffen organisatie altijd rechtstreeks met elkaar in contact te brengen. Het NCSC ontvangt inmiddels meldingen voor kwetsbaarheden in eigen systemen, in systemen van de Nederlandse overheid en in sommige gevallen ook in systemen van private partijen. Onderzoekers blijken het NCSC op dit gebied steeds beter te vinden, vooral sinds september 2013.

In totaal ontving het NCSC in de periode van dit CSBN 95 meldingen; dit waren zowel meldingen voor eigen systemen, als voor overheidssystemen en systemen van private partijen. Niet in alle gevallen bleek er bij onderzoek naar de melding ook daadwerkelijk sprake te zijn van een kwetsbaarheid. In een klein percentage van de gevallen kon de melding niet worden gereproduceerd. Daarnaast bleken diverse onderzoekers vaak dezelfde tekortkomingen te melden, waardoor het totaal aantal meldingen niet representatief is voor het totaal aantal aangetroffen kwetsbaarheden. Figuur 17 toont verschillende types van responsible disclosures en hun respectievelijke aandeel in alle disclosuremeldingen.

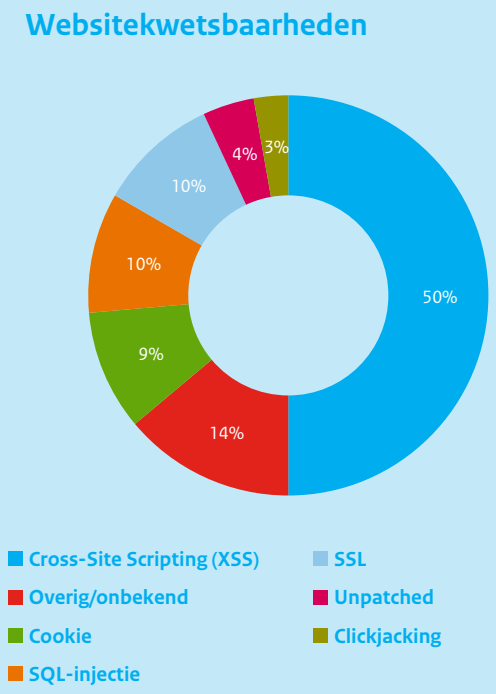
Opvallend vaak (in 76 procent van de gevallen) gaat het bij responsible disclosure om meldingen over kwetsbaarheden in webapplicaties of kwetsbaarheden in de infrastructuur waarop webapplicaties draaien. Daarna volgen configuratiefouten die leiden tot kwetsbaarheden (17 procent). Bij configuratiefouten kan men denken aan onjuist geconfigureerde firewalls en routers of standaard geconfigureerde systemen met bekende wachtwoorden. Verder ontving het NCSC ook meldingen over ongepatchte kwetsbaarheden in software en andere kwetsbaarheden. In 4 procent van de gevallen was er sprake van een false positive.



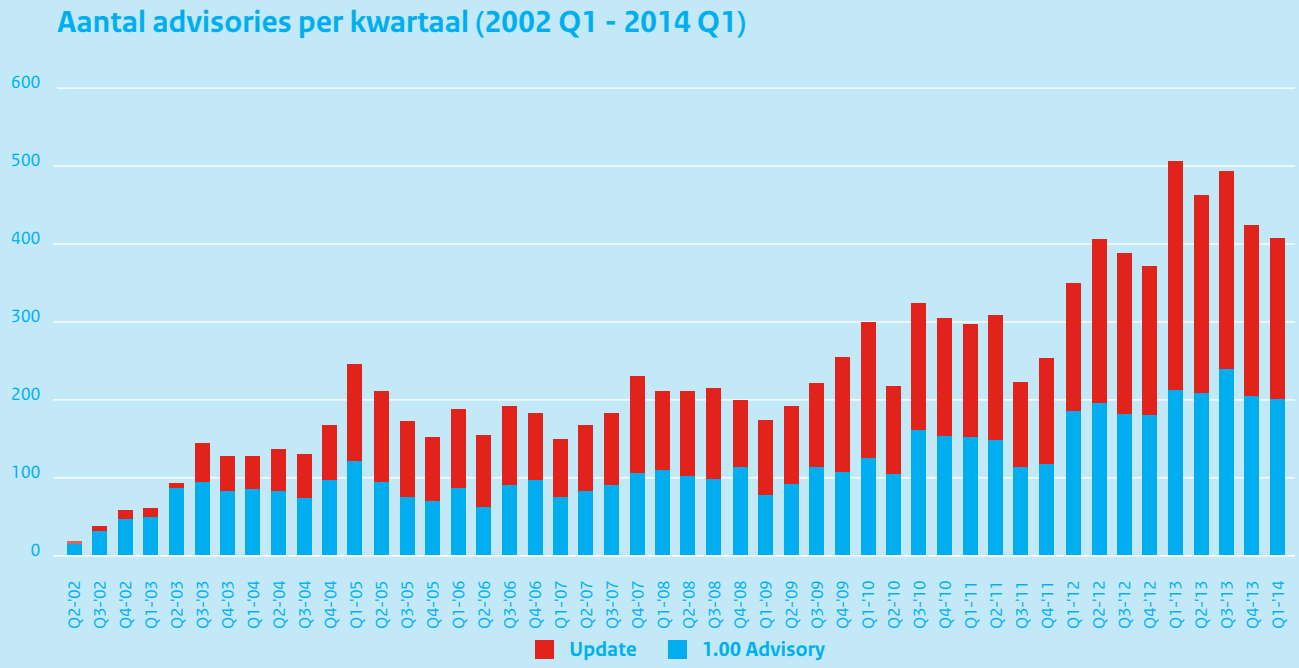

*Figuur 17. Typen responsible-disclosuremeldingen (bron: NCSC).*

**Responsible disclosure in de praktijk**
Een geslaagd voorbeeld van een kwetsbaarheid die via responsible disclosure werd verholpen, is een kwetsbaarheid in Microsoft Internet Explorer. Onderzoeker 'Hoodie22' meldde in september 2013 aan het NCSC misbruik te zien van deze tot dan toe onbekende kwetsbaarheid, die kon leiden tot gecorrumpeerd geheugen en daarmee het uitvoeren van willekeurige code (CVE-2013-3897).[188] [189] Via het NCSC werd de melding geanoniemiseerd doorgezet naar Microsoft, waarna Microsoft in oktober 2013 een patch uitbracht om deze kwetsbaarheid te verhelpen. In de advisory van Microsoft (MS13-080)[190] werd 'Hoodie22' expliciet bedankt voor zijn bijdrage.

Aangezien het overgrote deel van de meldingen in het kader van responsible disclosure kwetsbaarheden in websites betreft, hebben we dit type kwetsbaarheid nader beschouwd (zie figuur 18). Deze nadere beschouwing leert dat het bij de website-kwetsbaarheden in veel gevallen gaat om Cross-Site Scripting (XSS). Het betreft hier de helft van alle kwetsbaarheden die in websites werden gemeld. Daarna volgt ongeveer een gelijk aantal meldingen over achtereenvolgens cookie-instellingen, SQL-injectiemogelijkheden en onveilige SSL-configuraties.

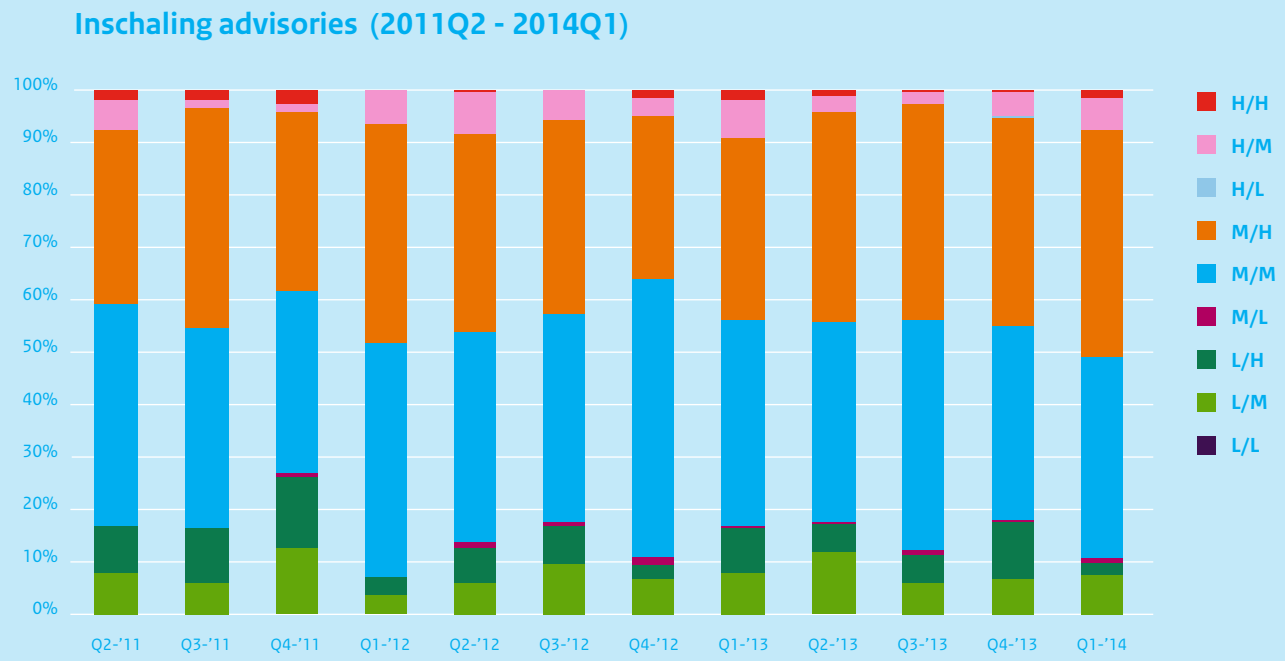



*Figuur 18. Websitekwetsbaarheden (bron: NCSC).*




*Figuur 19. Aantal advisories per kwartaal (2002Q2 - 2014Q1) (bron: NCSC).*

188 https://technet.microsoft.com/en-us/security/bulletin/ms13-080
189 https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2013-0685+1.02+MS13-080+Diverse+kwetsbaarheden+verholpen+in+Microsoft+Internet+Explorer.html
190 https://technet.microsoft.com/en-us/security/bulletin/ms13-080



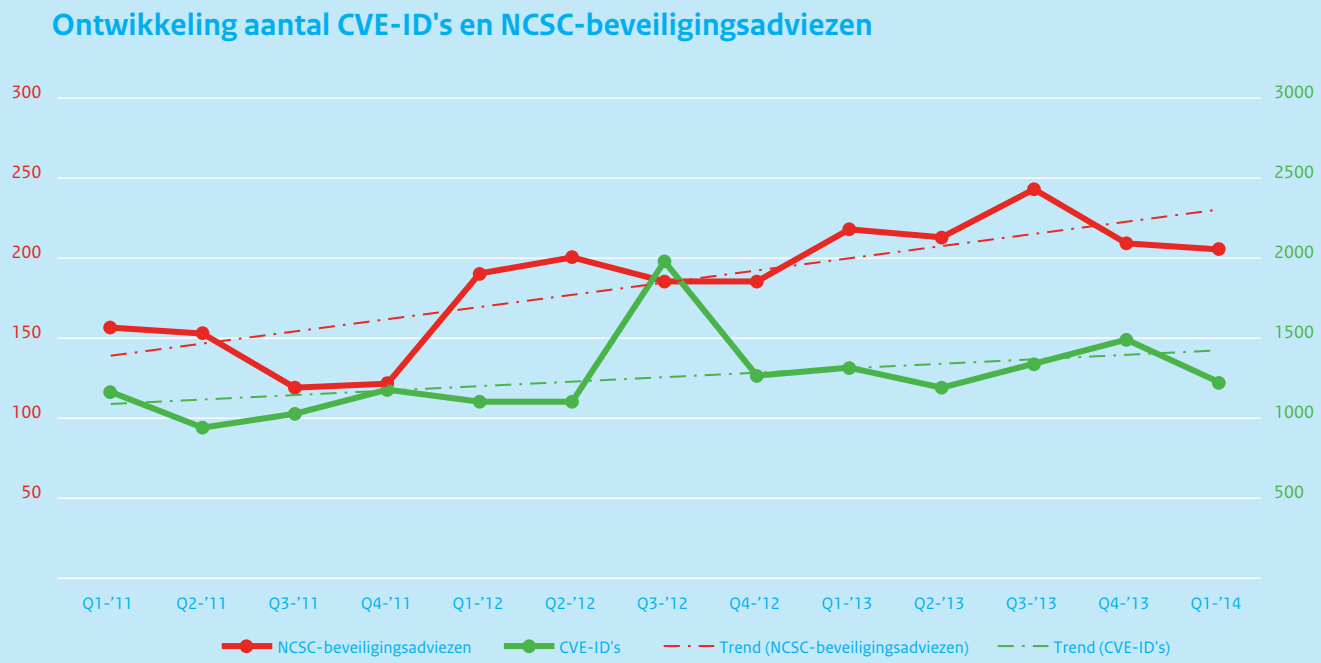

*Figuur 20. Inschaling advisories (2011Q2 - 2014Q1) (bron: NCSC).*

## Beveiligingsadviezen van het NCSC

Het NCSC publiceert beveiligingsadviezen (oftewel advisories) naar aanleiding van software-kwetsbaarheden of geconstateerde dreigingen. In een advisory wordt beschreven wat er aan de hand is, op welke systemen het impact heeft en wat er moet gebeuren om te voorkomen dat een organisatie slachtoffer wordt. Figuur 19 toont het aantal advisories dat het NCSC per kwartaal publiceerde vanaf het tweede kwartaal van 2002 tot en met het eerste kwartaal van 2014. Deze figuur laat zien dat er in de afgelopen rapportageperiode aanzienlijk meer adviezen zijn gepubliceerd dan in de vorige periode.

De beveiligingsadviezen van het NCSC worden ingeschaald op twee elementen. Allereerst op de kans dat de kwetsbaarheid misbruikt wordt. Ten tweede op de schade die optreedt wanneer de kwetsbaarheid misbruikt wordt. De inschaling kent twee criteria: kans en schade. Voor beide criteria wordt, op basis van meerdere aspecten, een niveau geschat: hoog (H), gemiddeld (M) of laag (L). Als er bijvoorbeeld een hoge kans is dat een bepaalde kwetsbaarheid misbruikt wordt maar de schade daarvan laag zou zijn, krijgt het bijbehorende beveiligingsadvies een H/L inschaling. Bovenstaande figuur toont de inschalingspercentages van alle gepubliceerde adviezen vanaf het tweede kwartaal 2011 tot en met het eerste kwartaal van 2014.

In figuur 21 wordt het aantal NCSC-beveiligingsadviezen per kwartaal vergeleken met het aantal CVE-registraties van de National Vulnerability Database (NVD). Het aantal kwetsbaarheden in de NVD is substantieel groter dan die van het NCSC. Om deze in een grafiek op te nemen, worden twee verschillende schalen gebruikt met een factor 10 verschil. De rode lijn toont het aantal NCSC-beveiligingsadviezen en gebruikt de rode schaal aan de rechterkant van de grafiek. De groene lijn toont het aantal NVD-registraties en gebruikt de groene schaal aan de linkerkant van de grafiek. Beide lijnen tonen een algemene trend over de afgelopen rapportageperiode.




*Figuur 21. Ontwikkeling CVE-ID's en NCSC-beveiligingsadviezen (bron: NCSC).*

## Oorzaken van kwetsbaarheden in so□ware

Figuur 22 toont de belangrijkste oorzaken van kwetsbaarheden in software. Sommige kwetsbaarheden zijn aan meerdere oorzaken gekoppeld en sommige kwetsbaarheden zijn aan geen enkele, bekende oorzaak gekoppeld. Bufferoverflow is niet alleen in de afgelopen rapportageperiode, maar al meer dan 25 jaar de meest voorkomende oorzaak. Cross-site scripting (XSS) was ook in de vorige rapportageperiode de op een na meest voorkomende oorzaak. De algemene trend laat zien dat er weinig verandering is in de verhouding van de top 10-oorzaken sinds de vorige rapportageperiode.


*Figuur 22. Belangrijkste oorzaken van kwetsbaarheden (bron: NCSC).*

## Schade van kwetsbaarheden in so□ware

Bij ieder beveiligingsadvies hoort een omschrijving van de mogelijke schade die een kwaadwillende zou kunnen verrichten als het advies niet gevolgd wordt. Om een overzicht te krijgen van deze schade worden adviezen gecategoriseerd op basis van een standaardlijst van schadeomschrijvingen. De categorisatie van de afgelopen rapportageperiode wordt in tabel 7 getoond. Deze tabel toont de schadeomschrijvingen die gekoppeld zijn aan de door het NCSC gepubliceerde beveiligingsadviezen en het percentage dat onder iedere omschrijving valt. Omdat sommige adviezen onder meerdere categorieën kunnen vallen, is de opsomming van alle percentages meer dan 100 procent. Uit deze tabel is duidelijk te zien dat de meeste adviezen te maken hadden met Denial-of-Service (DoS), het uitvoeren van willekeurige code (met gebruikersrechten) en toegang tot gevoelige gegevens. Ook in de vorige rapportageperiode (CSBN-3) vormden deze categorieën de top 3, weliswaar met andere percentages.

| Schadeomschrijving | Percentage |
|---|---|
| Denial-of-Service (DoS) | 45,8% |
| Uitvoeren van willekeurige code (met gebruikersrechten) | 30,6% |
| Toegang tot gevoelige gegevens | 24,0% |
| Verhoogde gebruikersrechten | 20,9% |
| Omzeilen van beveiligingsmaatregel | 13,1% |
| Cross-Site Scripting (XSS) | 11,0% |
| Toegang tot systeemgegevens | 8,4% |
| Omzeilen van authenticatie | 6,3% |
| Manipulatie van gegevens | 5,6% |
| Uitvoeren van willekeurige code (met beheerdersrechten) | 4,4% |
| Spoo□ng | 4,1% |
| Cross-Site Request Forgery (XSRF) | 2,6% |
| SQL-injectie | 1,9% |

*Tabel 7. Schadeomschrijvingen bij NCSC-beveligingsadviezen (bron: NCSC)*

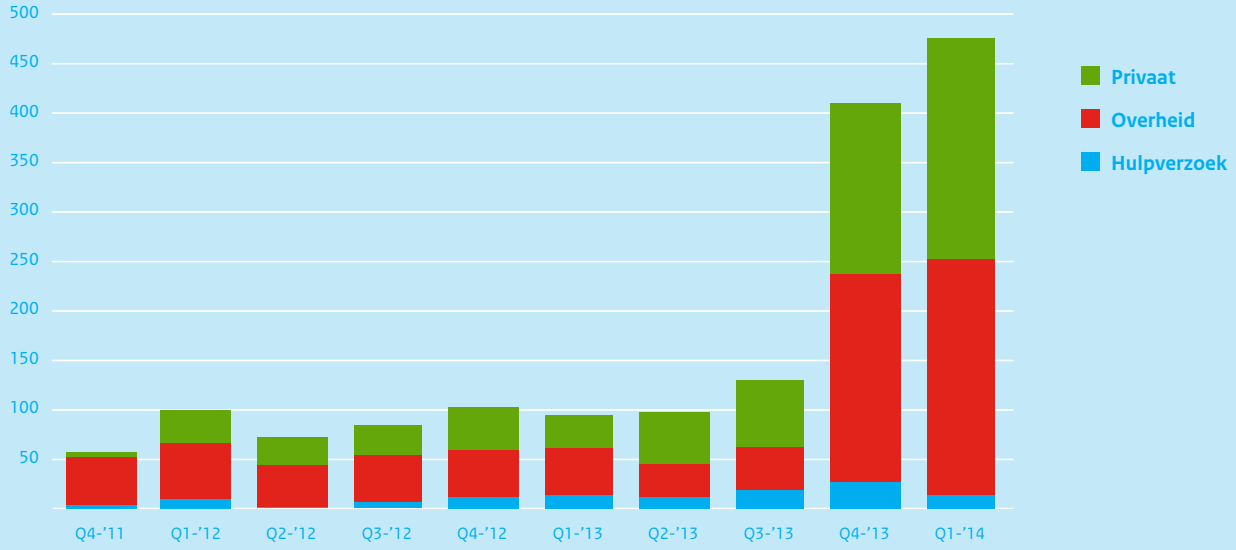
## Incidenten geregistreerd bij het NCSC

Het NCSC ondersteunt overheden en organisaties in vitale sectoren bij het afhandelen van incidenten op het gebied van ICT-veiligheid. In die rol worden bij het NCSC incidenten en kwetsbaarheden gemeld en worden deze ook door het NCSC zelf geïdentificeerd, bijvoorbeeld op basis van diverse detectiemechanismen. Daarnaast acteert het NCSC op verzoek van (inter)nationale partijen richting Nederlandse internetserviceproviders om te ondersteunen bij het bestrijden van cyberincidenten die hun oorsprong vinden in Nederland (bijvoorbeeld vanaf een malafide webserver of vanaf geïnfecteerde pc's in Nederland).

### Aantallen afgehandelde incidenten

Het aantal incidentenmeldingen dat het NCSC in de periode van dit CSBN afhandelde, ligt beduidend hoger dan het aantal in het vorige CSBN. Zoals verderop in dit hoofdstuk staat beschreven, is dit voor een groot deel te verklaren door de automatisering van incidentmeldingen die het NCSC uitstuurt. Figuur 23 toont het overzicht van incidentmeldingen, onderverdeeld naar de sector waarop deze melding betrekking had. Zoals figuur 23 illustreert, is het aantal incidentmeldingen vooral gestegen vanaf het vierde kwartaal van 2013.

## Door NCSC afgehandelde incidenten (Q4-'11-Q1-'14)

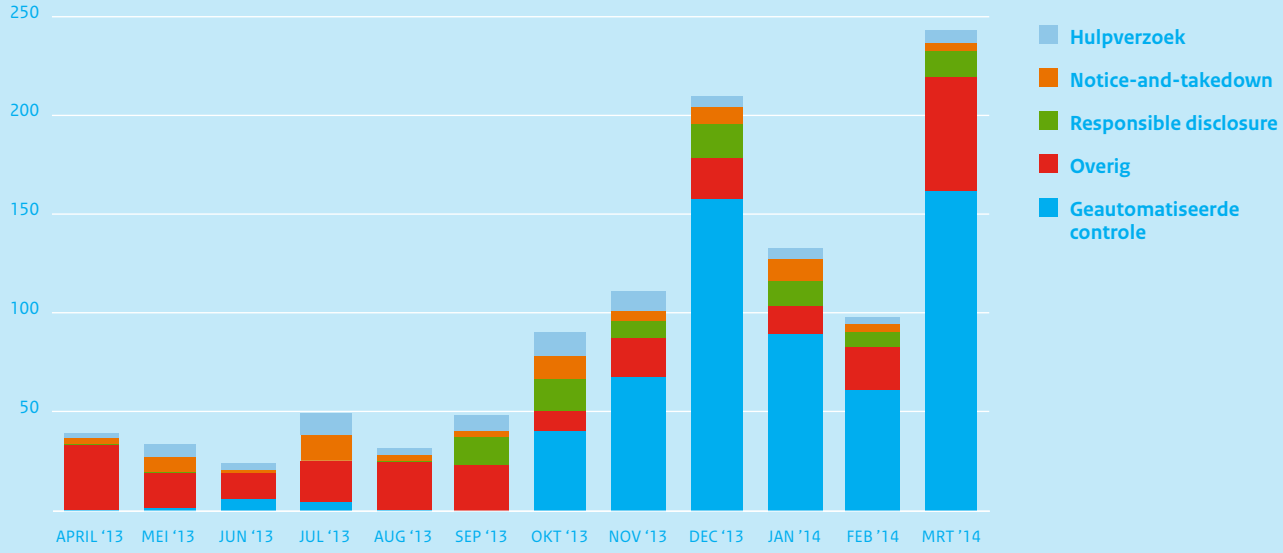



*Figuur 23. Door NCSC afgehandelde incidentmeldingen (inclusief geautomatiseerde controles) (bron: NCSC).*

Om de toename in incidentmeldingen verder te verklaren, is een detaillering van het type incidenten gedurende de rapportageperiode van dit CSBN gemaakt en weergegeven in figuur 24.

In de typering van figuur 24 valt direct op dat het aantal meldingen als gevolg van geautomatiseerde controles sinds oktober 2013 een belangrijk percentage van alle meldingen uitmaakt. Daarnaast worden vanaf september 2013 regelmatig meldingen geregistreerd op

## Detaillering type incidentmeldingen




*Figuur 24. Typen incidentmeldingen voor periode april 2013 tot en met maart 2014 (bron: NCSC).*

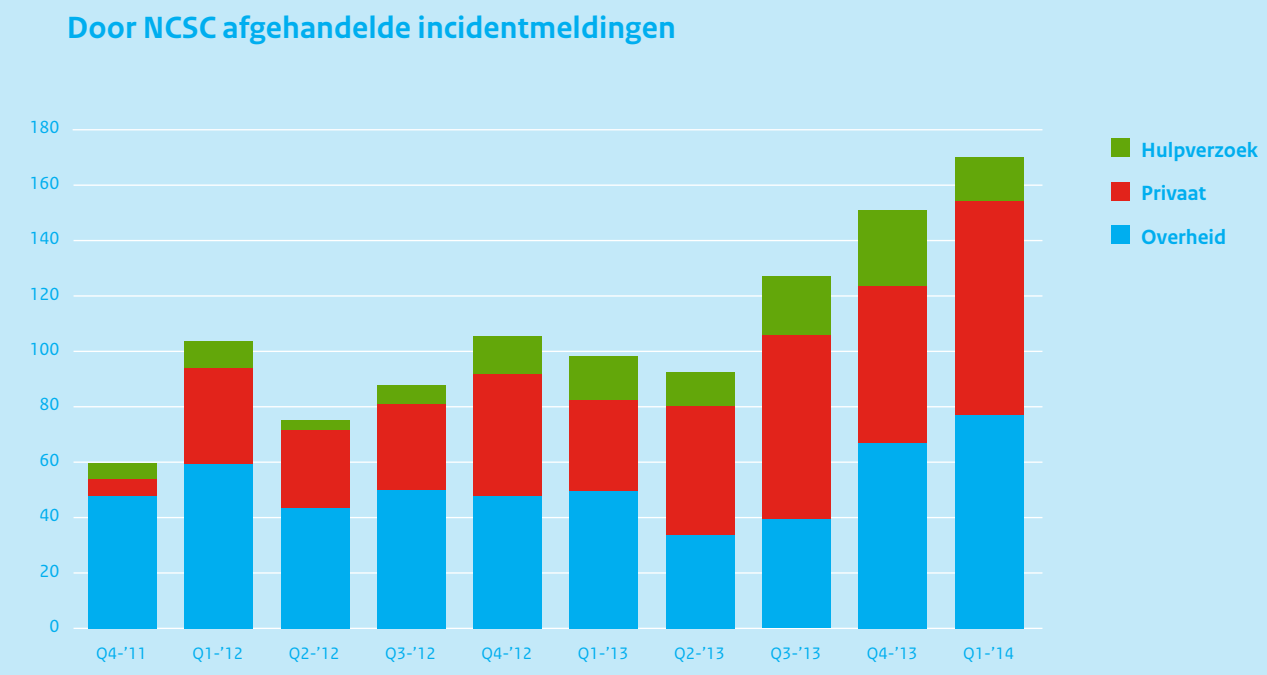
| Categorie | Omschrijving |
|---|---|
| Hulpverzoek | Verzoek van (inter)nationale partijen richting Nederlandse internetserviceproviders om te ondersteunen bij het bestrijden van cyberincidenten die hun oorsprong vinden in Nederland. |
| Notice-and-takedown | Verzoek van een Nederlandse □nanciële instelling bij het bestrijden van phishing-aanvallen die zich richten op deze instelling en hun oorsprong (veelal) vinden in het buitenland. |
| Responsible disclosure | Het op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie verhelpen en openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid. |
| Overig | Alle incidenten die niet onder een van de andere categorieën kunnen worden geschaard. |
| Geautomatiseerde controle | Geautomatiseerde controles van broninformatie (infecties, mala□de systemen) tegen bij NCSC bekende organisaties op basis van IP-adres, AS-nummer en domeinnaam. |

*Tabel 8. Incidenten categorieën.*

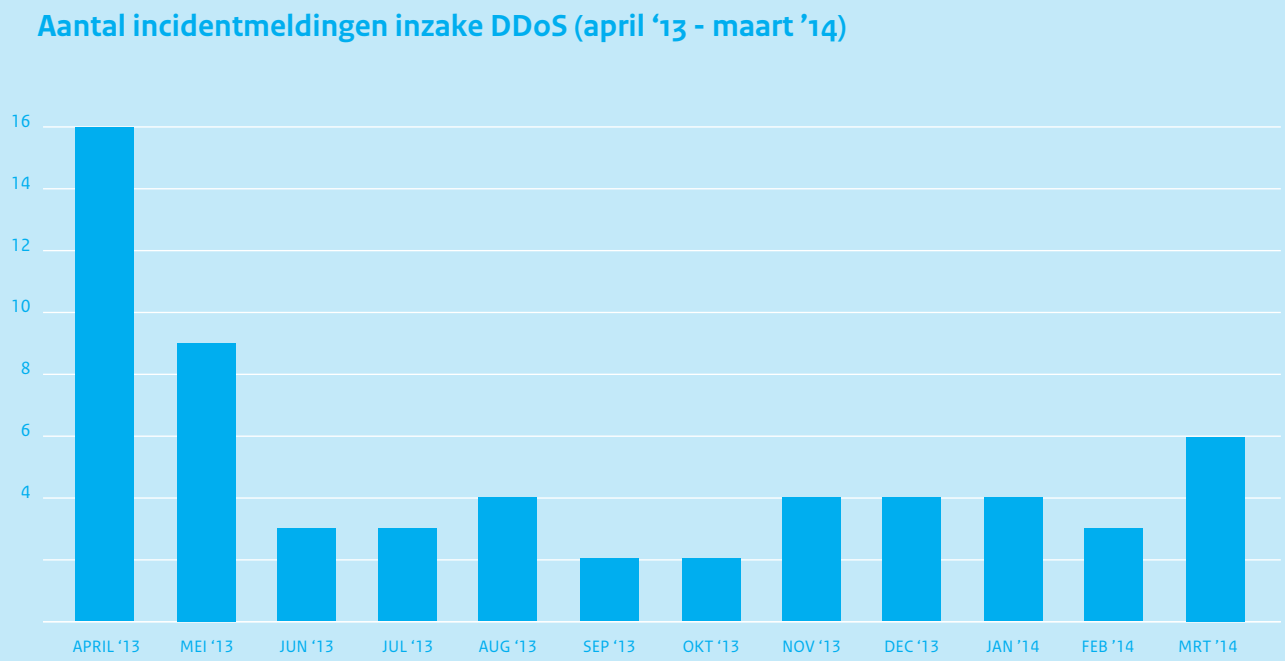
het gebied van reponsible disclosure. Deze twee onderwerpen diepen we daarom in het vervolg van dit hoofdstuk verder uit. Zie tabel 8 voor een beschrijving van de diverse categorieën uit figuur 24.

Om de ontwikkeling van de door NCSC afgehandelde incidentmeldingen over de afgelopen jaren beter in beeld te brengen, is hetzelfde overzicht van figuur 23 nogmaals gegenereerd, maar dan exclusief de geautomatiseerde controles. Het resultaat hiervan is opgenomen in figuur 25, waarin nog altijd een groei in het aantal incidentmeldingen te zien is.

Per kwartaal verwerkt het NCSC dus steeds meer incidentmeldingen. Exclusief de geautomatiseerde controles is dit in de rapportageperiode van dit CSBN opgelopen van 89 in het tweede kwartaal van 2013 tot 163 in het eerste kwartaal van 2014. Opvallend daarbij is dat het aandeel incidentenmeldingen uit de private sector langzaam begint toe te nemen. Terwijl in de periode van het CSBN-3 37 procent van alle incidentmeldingen betrekking had op de private sector, is dit in de periode van dit CSBN gegroeid naar 46 procent van alle meldingen. Een oorzaak hiervan kan liggen in de steeds verdergaande samenwerking van het NCSC met en bekendheid bij




*Figuur 25. Door NCSC afgehandelde incidentmeldingen (exclusief geautomatiseerde controles) (bron: NCSC).*




*Figuur 26. Aantal DDoS-meldingen (bron: NCSC).*

private partijen en de rol die het NCSC vervult bij het afhandelen van responsible-disclosuremeldingen.

Geautomatiseerde controles Zoals al eerder gesteld, vinden veel van de incidentenmeldingen die het NCSC afhandelt hun oorsprong in de geautomatiseerde controles die het NCSC dagelijks uitvoert op basis van de informatie die diverse bronnen aanleveren. Deze informatie matcht het NCSC automatisch tegen bekende IP-adressen, AS-nummers en domeinnamen van organisaties binnen de Rijksoverheid en de vitale sectoren die zich voor deze dienst hebben aangemeld.

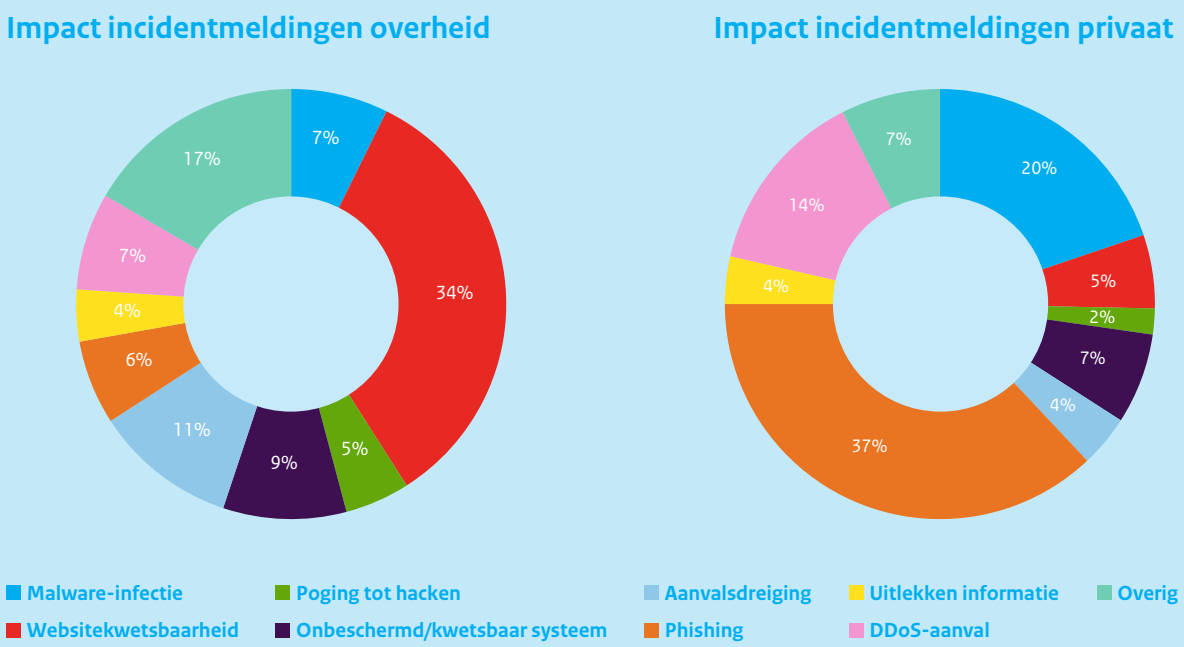
Het aantal incidenten dat voortvloeit uit de geautomatiseerde controles sinds het derde kwartaal van 2013 is substantieel toegenomen. Van de afgelopen rapportageperiode vond meer dan 97 procent van deze incidenten plaats in het vierde kwartaal van 2013 en het eerste kwartaal van 2014. Dit betekent echter niet automatisch dat er veel meer infecties aanwezig zijn in de netwerken van organisaties. Er is een aantal ontwikkelingen geweest die deze toename helpt verklaren:

1 Het aantal organisaties dat zich voor deze dienst heeft aangemeld, is sterk toegenomen. Mede door de oproep van minister Opstelten tot aanmelding voor deze dienst (naar aanleiding van het Pobelka-botnet[191]) is het aantal deelnemende organisaties gegroeid.
2 Het aantal bronnen dat het NCSC gebruikt voor de geautomatiseerde controles is gegroeid, wat leidt tot meer broninformatie.
3 Het uitsturen van incidentmeldingen is steeds verder geautomatiseerd. In sommige gevallen leidt dit tot meer incidentmeldingen. Bij de handmatige controles werden bijvoorbeeld meldingen veelal gegroepeerd en als één incidentmelding aangeboden aan organisaties. In de nieuwe situatie leiden hits van een organisatie op een bron tot één incidentmelding per bron.

DDoS De laatste maanden was er in de media veel aandacht voor de diverse manieren waarop een DDoS-aanval kan worden uitgevoerd. Vooral het gebruik van diverse amplificatietechnieken droeg bij aan de (hernieuwde) populariteit van dit soort aanvallen. Deze populariteit zien wij ook terug in de incidentmeldingen (zie figuur 26). Daar waar tijdens de periode van het vorige CSBN nog maar tien keer melding werd gemaakt van een DDoS-aanval, is dit aantal in de periode van dit CSBN opgelopen naar zestig. Vooral in het begin van de rapportageperiode (april en mei 2013) was dit aantal erg hoog. Vanaf juni 2013 is een stabilisatie van het aantal DDoS-meldingen op rond de vier meldingen per maand zichtbaar.

Nadere detaillering impact In eerdere CSBN-rapporten evalueerden we de ontwikkeling van de impact van incidenten bij de overheid aan de hand van historische cijfers. Door de genoemde groei van incidentmeldingen als gevolg van geautomatiseerde controles zou een vergelijking van de impact gedurende deze CSBN-periode met vorige periodes een scheef beeld opleveren. Daarom is er dit keer voor gekozen om bij de impact vooral te kijken naar de cijfers binnen deze CSBN-periode, exclusief geautomatiseerde controles. In figuur 27 is de impact van incidentmeldingen gespecificeerd voor meldingen over de overheid en over de private sector. Dit laat zien dat het type incidentmeldingen per sector sterk verschilt.

191 h□ps://web.archive.org/web/20130321012513/h□p://www.nu.nl/internet/3210513/alles-gedaan-pobelka-botnet.html Geraadpleegd op 22 mei 2014.




*Figuur 27. Impact meldingen overheid en private sector (bron: NCSC).*

Bij de incidentmeldingen bij de overheid is vooral sprake van kwetsbare websites of een kwetsbare infrastructuur rondom deze websites. Hieronder vallen zaken als onveilige SSL-configuraties, XSS-kwetsbaarheden en onveilige cookie-afhandeling. In vrijwel alle gevallen betrof het hier een responsible-disclosuremelding over een website van de overheid. Bij private partijen vormt phishing de belangrijkste reden van alle incidentmeldingen. «

# BIJLAGE 2 » CYBERSECURITY IN DE VITALE SECTOREN

**Dit jaar zijn voor het eerst gerichte analyses met een aantal vitale sectoren uitgevoerd. Het uiteindelijke doel is om een completer en beter gedi□erentieerd cybersecuritybeeld weer te geven. Deze bijlage presenteert de resultaten van deze eerste sectoranalyses die met medewerking van de ISAC's[192] zijn uitgevoerd. Sommige thema's kwamen in meerdere sectoren terug: ketenintegratie, de rol van persoonsgegevens, de toename van 'customer self care' en de betekenis van uitbesteding en uniforme componenten.**

## Sectoren

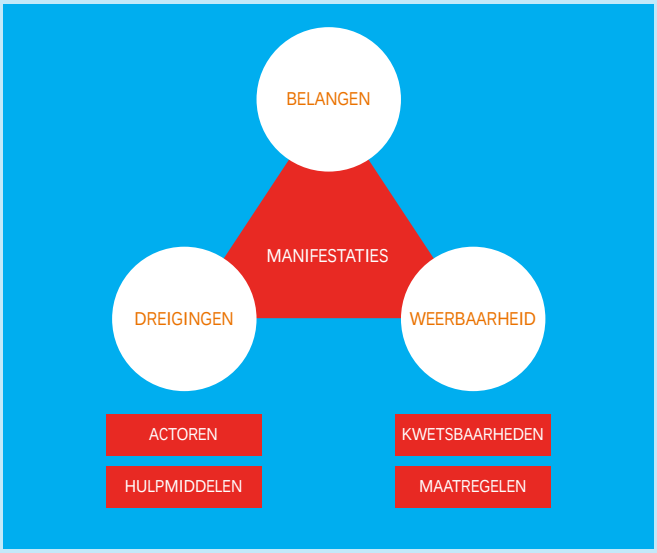
Binnen de volgende sectoren zijn inventarisaties uitgevoerd: Transport (Haven, Luchthaven en Spoor), Telecom, Finance, Energie, Zorg, Water en Managed Service Providers (MSP). De inventarisatie is uitgevoerd aan de hand van de CSBN-driehoek: belangen, dreigingen en weerbaarheid.

In de matrix wordt een overzicht gepresenteerd van de resultaten, waarbij mogelijke verschillen tussen sectoren zichtbaar worden. In de volgende paragraaf wordt een aantal terugkerende thema's gesignaleerd.

## Terugkerende thema's

Ketenintegratie Een terugkerend thema bij veel sectoren is het waarborgen van cybersecurity in ketens van informatiesystemen. De sectoren Water, Energie, Transport en Zorg kennen zowel fysieke productieketens als ketens van informatiesystemen die deze fysieke ketens ondersteunen. Deze ondersteunende ketens worden voornamelijk ingevuld door de telecomsector en door managed service providers (MSP). Deze sectoren kennen dan ook een grote verwevenheid met de andere vitale sectoren.

Afnemers hebben veelal onvoldoende kennis van de inhoud en onvoldoende zicht op alle partijen in de keten om nog de nodige grip op (de cybersecurity-aspecten van) deze ketens te hebben. Uit de analyse komt naar voren dat er behoefte is aan inzicht in de samenhang en werking van deze ketens om deze goed te kunnen beveiligen. Hierbij geven leveranciers van ondersteunende ketens aan dat afnemers er om vragen dat cybersecurity specifiek wordt meegenomen bij het aanbieden van diensten. Enkele sectoren geven aan dat het aanbod aan 'veilige' IT oplossingen achterblijft bij de vraag.




*Figuur 28. Samenhang belangen, dreigingen en weerbaarheid.*

Rol van persoonsgegevens Ten aanzien van persoonsgegevens blijkt uit de analyse dat er tussen verschillende sectoren onderscheid is waar te nemen op het vlak van gevoeligheid. Bescherming van privacy en imagoschade bij het uitlekken van persoonsgegevens leidt bij alle sectoren tot aandacht voor het beveiligen van klant- en persoonsgegevens.

Factuurgegevens worden in de Watersector als gevoelig beschouwd. De gevoeligheid van deze gegevens is van een andere orde dan bijvoorbeeld de gevoeligheid van patiëntgegevens in de zorg. Hierbij gaat het immers om zeer persoonlijke en intieme gegevens. Uit de analyse blijkt dan ook dat naarmate de gevoeligheid hoger ligt er meer aandacht voor de beveiliging van deze gegevens is, zowel qua dreigingen als weerbaarheid.

'Customer Self Care' Zogenaamde 'Customer Self Care'[193]-oplossingen blijken uit de analyse een groeiende ontwikkeling in diverse sectoren. Er is een enorme toename waar te nemen van online portalen waar je als klant je zaken zelf online kunt regelen. Hierbij komt het volgende spanningsveld naar voren.

192 ISAC – Information Sharing and Analysis Center, publiek-private samenwerkingsverbanden waarbij de deelnemers onderling informatie en ervaringen uitwisselen over cyber security.

193 Doe-het-zelf klantportaal waarin klanten zelf hun door een organisatie benodigde persoonsgegevens en afgenomen diensten kunnen bijhouden.

Customer self care-portals hebben twee belangrijke voordelen. In de eerste plaats bieden ze de klant de mogelijkheid om zijn of haar diensten zelfstandig te regelen, zonder daarbij afhankelijk te zijn van de beschikbaarheid (zoals openingstijden) van de leverancier. Daarnaast kunnen online portalen de kosten voor contact met klanten reduceren. Aan de andere kant rijst de vraag hoeveel verantwoordelijkheid je in dit verband bij de klant neer kunt leggen. In de door ons bestudeerde sectoren bieden portalen toegang tot (de instellingen van) diensten die ook voor individuele klanten van belang zijn. Zo zijn er portalen waar je facturen kunt raadplegen en je NAW[194]-gegevens kunt aanpassen, maar ook portalen waar je wijzigingen in contractvormen en afgenomen producten online kunt aanbrengen. Daar komt bij dat de klant meestal beperkte kennis van cybersecurity heeft. Dit vergroot de kwetsbaarheid, waardoor kwaadwillenden mogelijk toegang tot klantgegevens kunnen krijgen. Hieraan kunnen potentieel grote gevolgen verbonden zijn.

Uitbesteding van systeemkennis Zowel afnemers als aanbieders van IT-diensten geven in de sectoranalyse aan dat er toenemende aandacht is voor cybersecurity. Dit geldt zowel bij de uitbesteding van ondersteunende IT processen als de inkoop van COTS[195]-gebaseerde oplossingen. Hier tekent zich een spanningsveld af tussen enerzijds kostenreductie en anderzijds cybersecurity. Bij vitale ICS speelt gebruik van COTS-oplossingen minder.

Een belangrijke reden voor de uitbesteding van ondersteunende IT-processen is kostenreductie. Daar staat tegenover dat de inhoudelijke kennis over de ingekochte producten en diensten bij afnemers vaak afneemt, waardoor ook het gevoel van controle afneemt. Uit de analyse komt naar voren dat afnemers het idee hebben dat leveranciers ‘achterdeurtjes’ inbouwen om op afstand werkzaamheden uit te kunnen voeren, waarvan het overzicht bij de afnemer ontbreekt. Men heeft hierdoor geen zicht meer op eventuele cyberrisico’s.

Bij de inkoop van COTS-gebaseerde oplossingen blijkt kostenreductie eveneens een belangrijk argument te zijn. Een ander voordeel is dat COTS-oplossingen over het algemeen sneller en eenvoudiger te patchen en te onderhouden zijn dan maatwerkoplossingen. In sectoren waar veel gewerkt wordt met specialistische, oudere hard- en software blijkt het lastig om deze te onderhouden. De keerzijde van de medaille is echter dat brede toepassing van COTS-oplossingen voor een homogener landschap zorgt, waardoor potentieel hergebruik van aanvalsmiddelen mogelijk is. Daarnaast vormt een breed toegepaste technologie, waarvan er veel kennis in het publieke domein beschikbaar is, een aantrekkelijk doelwit. «

194 NAW – naam, adres, woonplaats
195 COTS – Commercial O The Shelf , kant-en-klare oplossing, geen maatwerk.

| | Belangen | Dreigingen: actoren | Dreigingen: hulpmiddelen |
|---|---|---|---|
| **Energie** | Steeds a□ankelijker van ICT, besturing zonder ICT vrijwel niet meer mogelijk | Statelijke actoren, cybercrime, hacktivisten (ook politieke organisaties), interne medewerkers, ontevreden klanten, eenlingen/verwarde personen, terugkerende Jihadisten | Malware-as-a-Service, klassieke malware, DDoS, APT, social engineering |
| **Telecom** | Grote verwevenheid met sectoren, daarom zijn belangen van sectoren telecom belangrijk, daarnaast imagoschade van belang | Statelijk, providers niet als doelwit maar als route naar eindgebruikers die doel kunnen zijn; collateral, IP-ranges scannen en toevallig op doel stuiten | DoS-chantage, ransomware, misbruik van organisatienaam, minder mobiele malware dan gedacht |
| **Managed Service Providers** | Meer vraag van klanten naar cybersecurity | Outsourcing naar lagelonenlanden, hoge retentie van medewerkers in lagelonenlanden, (ex)medewerkers | DDoS (vaak niet doordacht, bijvoorbeeld midden in de nacht), social engineering, ransomware minder in zicht op enterpriseniveau |
| **Financial** | Online beschikbaarheid steeds belangrijker voor klanten, mede door afname van het aantal fysieke kantoren | Met name beroepscriminelen, hacktivisten, interne actoren | Malware, phishing, DDoS en APT |
| **Transport (Haven, Luchthaven, Spoor)** | Steeds a□ankelijker van ICT, relatief korte uitval kan langdurige e□ecten hebben | Statelijke actoren, (ingehuurde) hackers, wetgever, cybercrime, onbekende dreiging (wat kunnen anderen met informatie uit transportsystemen) | Man-in-the-Middle-aanvallen gezien op informatielijnen en centrale systemen, meer aandacht voor hacken van vliegtuigen, AIS gevoelig voor manipulatie, keyloggers (zie ook manifestaties) |
| **Water** | Steeds a□ankelijker van ICT, besturing zonder ICT vrijwel niet meer mogelijk | Focus ligt op veiligheid van systemen, niet op actoren; er worden wel eens pogingen gedaan om onderzoeksgegevens te stelen; weinig zichtbare dreiging | In deze categorie zijn geen zaken geduid in de analyse-workshop |
| **Zorg** | Steeds a□ankelijker van ICT, onderzoeks- en patiëntgegevens | Statelijke actoren, commerciële bedrijven, hackers, concurrenten, zorgverzekeraars en eigen medewerkers, vooral gericht op onderzoeks- en patiëntgegevens | Social engineering, bijvoorbeeld op basis van publieke informatie, datagijzeling, botnetbesme□ingen, keyloggers, met name standaard aanvalsmiddelen die tot standaard problemen leiden |

| | Weerbaarheid: kwetsbaarheden | Weerbaarheid: maatregelen | Manifestaties |
|---|---|---|---|
| **Energie** | Uitval door □rmwarefouten van leveranciers, door toepassing COTS-producten aanvalsmogelijkheden homogener geworden | Toename monitoring en detectie, werken aan C-level awareness | Geen grote incidenten geweest |
| **Telecom** | Kwetsbaarheden bij hardwarefabrikanten niet snel opgelost, kwetsbaarheden als gevolg van omslag naar IP-apparatuur | Moeite om security te laten meewegen bij time-to-market-beslissingen, zorgplicht is stok achter de deur | Botnets, malware in het algemeen, scholengemeenschap onder DDoS, Heartbleed hee□ diensten onderuit gedwongen |
| **Managed Service Providers** | Fouten in businesslogica, menselijke/politieke fouten, onaangekondigde publiciteit, SLA a□ankelijk van ketenproviders | Antivirus en andere hulpmiddelen zijn niet onfeilbaar; NDN gaat helpen, maar nog geen garantie; pentesten kan realistischer, goede afspraken om false positives te voorkomen; meer toepassing van IDS-oplossingen | Informatielek na □rmware-upgrade, spearphishing en spam, DDoS bij klanten, onrust en imagoschade door gepubliceerde 0-days |
| **Financial** | Insiderdreiging is toegenomen mede door tijdgeest | Betere monitoring en geoblocking | Malware, phishing, DDoS en APT |
| **Transport (Haven, Luchthaven, Spoor)** | Ketens van diverse IT-leveranciers kennen zwakke plekken | Dit jaar met name nog defensief, beweging naar detectie wordt gezien als mogelijkheid om weerbaarheid te kunnen vergroten | Hacken van de haven van Antwerpen, keyloggers op diverse systemen gevonden |
| **Water** | Veel innovatieve diensten (bijvoorbeeld meldingen van storing) maken gebruik van clouddiensten; bewustzijn is over risico's van outsourcing, geldt minder voor clouddiensten; systemen kunnen worden losgekoppeld van internet zonder fatale gevolgen | Bewustwording personeel, inzet van clouddiensten, investeringen op basis van risicoweging, volwassenheid groeit: toepassing IAM | Geen grote incidenten geweest |
| **Zorg** | Samenwerking in de zorgsector is noodzakelijk, verwevenheid specialistische (vaak legacy-) apparatuur, 'sellerspower' van leveranciers van specialistische apparatuur, volwassenheid op cybersecuritygebied is relatief laag | Toename samenwerking met partijen als SURFnet en NCSC, elk ziekenhuis zijn eigen CERT, externe specialisten ter ondersteuning, juridische maatregelen: privacywetgeving | Insider-incidenten |

# BIJLAGE 3 » AFKORTINGEN- EN BEGRIPPENLIJST

| | |
|---|---|
| **0-day** | Zie Zero-day exploit. |
| **2G/3G/4G** | Verschillende generaties van mobiele communicatie. In Nederland staan deze generaties synoniem voor gsm (2G), UMTS (3G) en lte (4G). |
| **ACM** | De Autoriteit Consument en Markt (ACM) is ontstaan uit de samenvoeging van de Nederlandse Mededingingsautoriteit (NMA), Consumentenautoriteit en Ona□ankelijke Post- en Telecommunicatieautoriteit (OPTA). |
| **Actor** | Een rol die een partij speelt in een ontwikkeling op het gebied van cybersecurity. In veel gevallen gaat het hierbij om een rol die duidelijk aanvallend of verdedigend is, maar dit onderscheid is niet altijd scherp te maken. Een partij kan meerdere rollen spelen, die eventueel gaandeweg ook nog kunnen veranderen. |
| **AIVD** | Algemene Inlichtingen- en Veiligheidsdienst. |
| **APT** | Een Advanced Persistent Threat (APT) is een gemotiveerde (soms geavanceerde) doelgerichte aanval op een natie, organisatie, persoon of groep van personen. |
| **Authenticatie** | Authenticatie is het nagaan of een bewijs van identiteit van een gebruiker, computer of applicatie overeenkomt met vooraf vastgelegde echtheidskenmerken. |
| **Beroepscrimineel** | Zie cybercrimineel. |
| **Beveiligen** | On□rekken aan geweld, bedreiging, gevaar of schade door het tre□en van maatregelen. |
| **Beveiligingsincident** | Een (informatie)beveiligingsincident is een enkele gebeurtenis of serie van ongewenste of onverwachte gebeurtenissen die een signi□cante kans hee□ op het veroorzaken van een ramp, het compromi□eren van de bedrijfsprocessen en een bedreiging vormt ten aanzien van de beveiliging. |
| **Bevoegden** | Diegenen die een geautoriseerde/functionele toegang hebben tot (onderdelen van) het bedrijf, de locatie, het proces, de middelen of informatie. |
| **Bot/Botnet** | Een bot is een geïnfecteerde computer die op afstand, met kwade bedoelingen, bestuurd kan worden. Een botnet is een verzameling van dergelijke geïnfecteerde computers die centraal bestuurd kunnen worden. Botnets vormen de infrastructuur voor veel vormen van internetcriminaliteit. |
| **Botnetbeheerder** | Persoon of organisatie die een botnet onderhoudt en de inzet ervan coördineert. |
| **Bu□erover□ow** | Een bu□erover□ow of bu□eroverloop vindt plaats wanneer een programma of proces meer data in het tijdelijk geheugen probeert op te slaan dan mogelijk is. Het teveel aan data overschrij□ andere geheugen-nadressen en dit veroorzaakt problemen in de werking van het programma of proces. |
| **BYOD** | Bring Your Own Device (BYOD) is een regeling in organisaties waarbij personeel eigen consumentenap-paratuur kan gebruiken voor het uitvoeren van de organisationele taken. |
| **CA** | Een Certi□cate Authority (CA) is, in een PKI-stelsel, een organisatorisch verband dat wordt vertrouwd om certi□caten te maken (genereren), toe te wijzen en in te trekken. |

| | |
|---|---|
| **CBS** | Centraal Bureau voor de Statistiek. |
| **C&C** | Een Command & Control (C&C)-server is een centraal systeem in een botnet van waaruit het botnet wordt aangestuurd. |
| **CERT** | Een Computer Emergency Response Team (CERT) is een team dat primair tot doel hee om incidenten te voorkomen en, wanneer deze toch optreden, adequaat op te treden om de impact ervan te beperken. |
| **Certi caat** | Zie Secure Sockets Layer-certi caat. |
| **Cloud/Clouddiensten** | Een op internet (de 'wolk') gebaseerd model voor systeemarchitectuur, waarbij vooral gebruikgemaakt wordt van So ware as a Service (SaaS). |
| **CNA** | Een Computer Network A ack (CNA) is het militair inze en van o ensieve cybercapaciteiten die tot doel hebben het handelen van de tegenstander te beïnvloeden of onmogelijk te maken. |
| **Compromi ering** | De kennisname dan wel de mogelijkheid van een niet-gerechtigde tot het kennisnemen van bijzondere informatie. |
| **Cookie** | Een cookie is informatie die door een webserver op de computer van een eindgebruiker wordt opgeslagen. Deze informatie kan bij een volgend bezoek van de eindgebruiker aan de webserver weer opgevraagd worden. Cookies kunnen worden gebruikt om gebruikersinstellingen te bewaren en ook om de gebruiker te volgen. |
| **COTS** | Een commercial o -the-shelf (COTS)-oplossing is een kant-en-klaar product, waar geen maatwerk bij wordt geleverd. |
| **CVE** | Common Vulnerabilities and Exposures (CVE) is een unieke gemeenschappelijke identi catie van publiekbekende informatiebeveiligingskwetsbaarheden. |
| **Cybercrime** | Vorm van criminaliteit waarbij een ICT-systeem of de informatie die daardoor wordt verwerkt, het doelwit is. |
| **Cybercrimineel** | Actoren die beroepsmatig cybercrime plegen met hoofdzakelijk geldelijk gewin als doel. Het CSBN onderscheidt de volgende groepen cybercriminelen:<br>» in enge zin, zij die zelf aanvallen plegen (of daarmee dreigen) om geld te verdienen;<br>» criminele cyberdienstverleners, zij die diensten en tools aanbieden waardoor of waarmee anderen cyberaanvallen kunnen uitvoeren;<br>» cyberhandelaren in of -dienstverleners voor gestolen informatie;<br>» criminelen die cyberaanvallen gebruiken voor traditionele criminaliteit. |
| **Cyberonderzoeker** | Actor die op zoek gaat naar kwetsbaarheden en/of inbreekt in ICT-omgevingen om de (te) zwakke beveiliging ervan aan de kaak te stellen. |
| **Cybersecurity** | Het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie. |
| **Data breach/datalek** | Het opze elijk of onopze elijk naar buiten komen van vertrouwelijke gegevens. |
| **DCS** | De Directie Cybersecurity (DCS), waar onder andere het NCSC onder valt, is onderdeel van de NCTV. |

| | |
|---|---|
| **(D)DoS** | (Distributed) Denial of Service is de benaming voor een type aanval waarbij een bepaalde dienst (bijvoorbeeld een website) onbereikbaar wordt voor de gebruikelijke afnemers van de dienst. Een DoS op een website wordt vaak uitgevoerd door de website te bestoken met veel netwerkverkeer, waardoor deze onbereikbaar wordt. |
| **DigiD** | De digitale identiteit van burgers, waarmee ze zich identificeren en authenticeren op websites van de overheid. Zo weten overheidsinstellingen dat ze echt met een bepaalde burger te maken hebben. |
| **DNS** | Het Domain Name System (DNS) is het systeem dat internetdomeinnamen koppelt aan IP-adressen en omgekeerd. Zo staat het adres 'www.ncsc.nl' bijvoorbeeld voor IP-adres '62.100.52.106'. |
| **DNS-hijacking** | Het kapen van een server om DNS-gegevens aan te passen, zodat internetverkeer naar andere bestemmingen kan worden omgeleid. |
| **DNSSEC** | DNS Security Extensions (DNSSEC) is een uitbreiding op DNS waarbij een authenticiteits- en integriteitscontrole wordt toegevoegd aan het bestaande systeem. |
| **Document** | Het begrip document heeft betrekking op brieven, notities, memo's, rapporten, presentaties, tekeningen, foto's, film, kaarten, geluidsopnamen, sms'en, digitale dragers (cd-rom, USB) of enig ander fysiek medium waar informatie op weergegeven kan zijn. |
| **Dreiging** | Het Cybersecuritybeeld definieert doel en dreiging als volgt:<br>» Het hogere doel (intentie) kan zijn het verstevigen van de concurrentiepositie; politiek/landelijk gewin, maatschappelijke ontwrichting, levensbedreiging, et cetera.<br>» Dreigingen in het beeld zijn onder andere ingedeeld als: digitale spionage, digitale sabotage, publicatie van vertrouwelijke gegevens, digitale verstoring, cybercrime en indirecte verstoringen. |
| **Encryptie** | Het versleutelen van informatie om deze onleesbaar te maken voor onbevoegden. |
| **End-of-life** | In de softwarewereld betekent de end-of-life van een product de datum waarop een product niet langer door de leverancier als gangbare software wordt beschouwd. Als software end-of-life is, maakt de leverancier over het algemeen geen updates meer en wordt ook geen ondersteuning meer geleverd. |
| **EMV** | Europay Mastercard Visa (EMV) is een standaard voor betaalkaartsystemen op basis van chipkaarten en chipkaartbetaalterminals. De chipkaart vervangt kaarten met een magneetstrip die makkelijk te kopiëren zijn. |
| **Exploit/exploitcode** | Software, gegevens of opeenvolging van commando's die gebruikmaken van een kwetsbaarheid in software en/of hardware om ongewenste functies en/of gedrag te veroorzaken. |
| **File inclusion** | Aanvalstechniek die voornamelijk bij webapplicaties wordt toegepast, waarbij een gebruiker een bestand met eigen code kan toevoegen om de werking van de applicatie te beïnvloeden. |
| **Gerubriceerde gegevens** | Door een partij en/of eigenaar gewaarmerkte gegevens, inclusief documenten, of materiaal dat beschermd moeten worden tegen ongeoorloofde openbaarmaking en die als zodanig gewaarmerkt zijn in een beveiligingsrubricering. |
| **Gevoelige informatie** | Gegevens over kritieke (vitale) infrastructuur die, wanneer zij openbaar worden gemaakt, zouden kunnen worden gebruikt om plannen te maken en feiten te plegen om kritieke infrastructuurinstallaties te verstoren of te vernietigen. |
| **Gps** | Het Global Positioning System (gps) is een plaatsbepalingssysteem op basis van satellieten met een nauwkeurigheid tot op enkele meters. Gps wordt onder andere gebruikt voor navigatie. |

| | |
|---|---|
| **Gsm** | Global System for Mobile Communications (gsm) is een standaard voor digitale mobiele telefonie. Gsm wordt beschouwd als de tweede generatie mobiele telefoontechnologie (2G). |
| **Hacker/Hacken** | De meest gangbare en de in dit document gehanteerde betekenis van hacker is iemand die met kwaadaardige bedoelingen probeert in te breken in computersystemen. Oorspronkelijk werd de term hacker gebruikt voor iemand die op onconventionele wijze gebruikmaakt van techniek (waaronder so□ware), veelal met als doel beperkingen te omzeilen of onverwachte e□ecten te bereiken. |
| **Hacktivist** | Samentrekking van hacker en activist: personen of groepen die uit ideologische motieven cyberaanvallen van activistische aard plegen. |
| **HTML** | HyperText Markup Language (HTML) is een opmaaktaal voor de speci□catie van documenten, voornamelijk bedoeld voor webpagina's. |
| **Hulpmiddel** | Een techniek of computerprogramma waarmee een aanvaller misbruik kan maken van bestaande kwetsbaarheden of deze kan vergroten. |
| **ICS/SCADA** | Industrial Control Systems (ICS) / Supervisory Control And Data Acqusition (SCADA) zijn meet- en regelsystemen, bijvoorbeeld voor de aansturing van industriële processen of gebouwbeheersystemen. ICS/SCADA-systemen verzamelen en verwerken meet- en regelsignalen van sensoren in fysieke systemen en regelen de aansturing van de bijbehorende machines of apparaten. |
| **Identiteitsfraude** | Het bewust de schijn oproepen dat een kwaadwillende de identiteit van een ander hee□ die niet bij hem hoort. |
| **Incident** | Een (cyber)incident is een ICT-verstoring in de dienstverlening waardoor de te verwachten beschikbaarheid van de dienstverlening geheel of gedeeltelijk is verdwenen, en/of het ongeoorloofd openbaren, verkrijgen en/of wijzigen van informatie. |
| **Informatie** | Een verzameling van gegevens (met of zonder context) opgeslagen in gedachten, in geschri□en (op bijvoorbeeld papier) en/of op digitale informatiedragers (elektronisch, optisch magnetisch). |
| **Informatiebeveiliging** | Het proces van vaststellen van de vereiste kwaliteit van informatie(systemen) in termen van vertrouwelijkheid, beschikbaarheid, integriteit, onweerlegbaarheid en controleerbaarheid alsmede het tre□en, onderhouden en controleren van een samenhangend pakket van bijbehorende (fysieke, organisatorische en logische) beveiligingsmaatregelen. |
| **Informatiesysteem** | Een samenhangend geheel van gegevensverzamelingen en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getro□en voorzieningen voor opslag, verwerking en communicatie. |
| **Integriteit** | Een kwaliteitskenmerk voor gegevens, een object of dienst in het kader van de (informatie)beveiliging. Het is een synoniem voor betrouwbaarheid. Een betrouwbaar gegeven is juist (rechtmatigheid), volledig (niet te veel en niet te weinig), tijdig (op tijd) en geautoriseerd (gemuteerd door een persoon die gerechtigd is de mutatie aan te brengen). |
| **Interne actor** | Individueel persoon of groep in een organisatie die daar van binnenuit cybersecurity-incidenten veroorzaakt. |
| **Internet der Dingen** | Fenomeen waarbij het internet niet alleen wordt gebruikt om gebruikers toegang te bieden tot websites, e-mail en dergelijke, maar om apparaten aan te sluiten die het gebruiken voor functionele communicatie. |
| **IP** | Het Internet Protocol (IP) zorgt voor adressering van datapakke□en, zodat ze bij het beoogde doel aankomen. |

| | |
|---|---|
| **IPv4/IPv6** | IPv4 is een versie van IP met een adresruimte van ruim vier miljard adressen. IPv6 is de opvolger daarvan met 3,4 keer 1038 mogelijke adressen, dat zijn vij□ig miljard keer miljard keer miljard adressen per aardbewoner. |
| **ISAC** | Een Information Sharing and Analysis Centre (ISAC) is een samenwerkingsverband tussen organisaties ten behoeve van het uitwisselen van (dreigings)informatie en gezamenlijke weerbaarheidsverhoging. Het NCSC faciliteert meerdere ISAC's voor vitale sectoren in Nederland. |
| **ISP** | Een Internet Service Provider (ISP) is een leverancier van internetdiensten, vaak simpelweg aangeduid als 'provider'. De geleverde diensten kunnen zowel betrekking hebben op de internetverbinding zelf als op de diensten die men op het internet kan gebruiken. |
| **Kwetsbaarheid** | Eigenschap van een samenleving, organisatie of informatiesysteem (of een onderdeel daarvan) die een kwaadwillende partij de kans gee□ om de legitieme toegang tot informatie of functionaliteit te verhinderen en te beïnvloeden dan wel ongeautoriseerd te benaderen. |
| **Lifecycle-management** | Lifecycle-management is een onderhoudsmethodiek die erop is gericht om systemen gedurende hun gehele levensduur het bedrijfsproces zo optimaal mogelijk te laten ondersteunen. Doel is het verbeteren van de continuïteit en e□ciëntie van productieprocessen. |
| **Lte** | Long Term Evolution; zie 2G/3G/4G. |
| **Malware** | Samentrekking van 'malicious' en 'so□ware', kortom: kwaadaardige so□ware. Malware is de term die tegenwoordig als generieke aanduiding wordt gebruikt voor onder andere virussen, wormen en Trojaanse paarden. |
| **MitM** | Man-in-the-middle (MitM) is een aanvalstechniek waarbij de aanvaller zich tussen twee partijen bevindt, bijvoorbeeld een internetwinkel en een klant. Hierbij doet de aanvaller zich richting de klant voor als de winkel en andersom. Als tussenpersoon kan de aanvaller uitgewisselde gegevens a□uisteren en/of manipuleren. |
| **MIVD** | Militaire Inlichtingen- en Veiligheidsdienst. |
| **NCTV** | Nationaal Coördinator Terrorismebestrijding en Veiligheid, onderdeel van het Ministerie van Veiligheid en Justitie. |
| **NFI** | Nederlands Forensisch Instituut. |
| **OSINT** | Open Source Intelligence (OSINT) is het vergaren van informatie over iemand door openbare bronnen te raadplegen. |
| **OWASP** | Het Open Web Application Security Project (OWASP) is een wereldwijde non-pro□torganisatie, gericht op het verbeteren van de beveiliging van webapplicaties. |
| **Patch** | Een patch (le□erlijk: 'pleister') kan bestaan uit reparatieso□ware of kan wijzigingen beva□en, die direct in een programma worden doorgevoerd om het desbetre□ende programma te repareren of te verbeteren. |
| **Phishing** | Verzamelnaam voor digitale activiteiten die tot doel hebben persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan worden misbruikt voor bijvoorbeeld creditcardfraude, maar ook voor identiteitsdiefstal. Spearphishing is een variant die zich richt op één persoon of een zeer beperkte groep personen in bijvoorbeeld een organisatie, die speci□ek worden uitgekozen op basis van hun toegangspositie om een zo groot mogelijk e□ect te sorteren zonder al te veel op te vallen. |

| | |
|---|---|
| **PKI** | Een Public Key Infrastructure (PKI) is een verzameling organisatorische en technische middelen waarmee je op een betrouwbare manier een aantal zaken kunt regelen, zoals het versleutelen en ondertekenen van informatie en het vaststellen van de identiteit van een andere partij. |
| **RAT** | Een Remote Access Tool (soms Remote Access Trojan, RAT) wordt gebruikt voor het verkrijgen van toegang tot de computer van een doelwit om die op afstand te kunnen bedienen. |
| **Relevantie** | Gee de verhouding weer tussen de verschillende dreigingen, dreigers en doelwi en. Om de verschillende dreigingsniveaus in het CSBN te bepalen worden incidenten, dreigingen binnen de analyses gewogen met de criteria van 'laag', 'midden' en 'hoog'. |
| **Rootkit** | Een stuk so ware dat een aanvaller meer rechten op een computersysteem gee , terwijl de aanwezigheid van deze so ware wordt verborgen voor het besturingssysteem. |
| **Rubricering** | Vaststellen en aangeven dat een gegeven bijzondere informatie is en het bepalen en aangeven van de mate van beveiliging die aan deze informatie moet worden gegeven. |
| **SCADA** | Zie ICS/SCADA. |
| **Scriptkiddie** | Actor met beperkte kennis die hulpmiddelen gebruikt die door anderen zijn bedacht en ontwikkeld, voor cyberaanvallen van baldadige aard. |
| **Skimmen** | Het onrechtmatig kopiëren van de gegevens van een elektronische betaalkaart, bijvoorbeeld een pinpas of creditcard. Skimmen gaat vaak gepaard met het bemachtigen van pincodes, met als uiteindelijk doel betalingen te verrichten of geld op te nemen van de rekening van het slachto er. |
| **Social engineering** | Een aanvalstechniek waarbij misbruik wordt gemaakt van menselijke eigenschappen als nieuwsgierigheid, vertrouwen en hebzucht met als doel vertrouwelijke informatie te verkrijgen of het slachto er een bepaalde handeling te laten verrichten. |
| **Spearphishing** | Zie phishing |
| **SQL-injectie** | Aanvalstechniek waarbij de communicatie tussen een applicatie en de achterliggende database kan worden beïnvloed door de gebruiker, met hoofdzakelijk als doel gegevens in de database te manipuleren of te stelen. |
| **SSL-certi caat** | Een Secure Socket Layer (SSL)-certi caat is een bestand dat fungeert als digitale identi catie van een persoon of systeem. Het bevat tevens PKI-sleutels om gegevens tijdens transport te versleutelen. Een bekende toepassing van SSL-certi caten zijn de met HTTPS beveiligde websites. |
| **Staatsgeheim** | Bijzondere informatie waarvan de geheimhouding door het belang van de Staat of haar bondgenoten wordt geboden. |
| **Statelijke actor** | Er is sprake van een statelijke actor wanneer de actor handelt uit naam van, of een doelwit vormt als zijnde een nationale overheid. |
| **Tablet** | Een draagbare computer waarbij het beeldscherm tevens de belangrijkste invoermogelijkheid is. |
| **Terrorist** | Actor met ideologische motieven die maatschappelijke veranderingen probeert te bewerkstelligen, bevolking(sgroepen) angst wil aanjagen of politieke besluitvorming poogt te beïnvloeden, door toepassing van geweld tegen mensen of het aanrichten van ontwrichtende schade. |
| **THTC** | Team High Tech Crime (Nationale Politie). |

| | |
|---|---|
| **TNO** | Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek. |
| **Tweefactorauthenticatie** | Een manier van authenticeren waarbij twee ona□ankelijke bewijzen voor een identiteit zijn vereist. Dit bewijs kan zijn: kennis over, bezit van of biometrische eigenschappen die de identiteit van de aanvrager bewijst. |
| **UMTS** | Universal Mobile Telecommunications System; zie 2G/3G/4G. |
| **USB** | Universal Serial Bus (USB) is een speci□catie van een standaard van de communicatie tussen een apparaat, in veel gevallen een computer, en randapparatuur. |
| **USB-stick** | Draagbaar opslagmedium dat via een USB-aansluiting aan computers kan worden gekoppeld. |
| **Vertrouwelijkheid** | Een kwaliteitskenmerk van gegevens in het kader van de informatiebeveiliging. Met vertrouwelijkheid wordt bedoeld dat een gegeven alleen te benaderen is door iemand die gerechtigd is het gegeven te benaderen. Wie gerechtigd is een gegeven te benaderen, wordt vastgesteld door de eigenaar van het gegeven. |
| **Webapplicatie** | De term waarmee het geheel wordt aangeduid van so□ware, databases en systemen die betrokken zijn bij het correct functioneren van een website, waarbij de website het zichtbare gedeelte is. |
| **Weerbaarheid** | Het vermogen van personen, organisaties of samenlevingen om weerstand te bieden aan negatieve invloeden op de beschikbaarheid, vertrouwelijkheid en/of integriteit van (informatie)systemen en digitale informatie. |
| **Wi□/Wi-Fi** | Een handelsmerk van de Wi-Fi Alliance. Een apparaat met Wi-Fi kan draadloos communiceren met andere apparatuur tot op enkele honderden meters. |
| **Zero-day exploit** | Een zero-day exploit is een exploit die misbruik maakt van een kwetsbaarheid waarvoor nog geen patch beschikbaar is. |

**Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
T 070 751 55 55 | F 070 322 25 37
www.ncsc.nl | csbn@ncsc.nl

Juli 2014