

Secure Computing

(NB: met Ctrl+ scrolwielje kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen. Via de hyperlinks verkrijgt u nog meer info.)

[W.Bosgra](#)

Taakaccenthouder Digitale Criminaliteit Basisteam Enschede

Snel index

Klik op een link voor snelle toegang . Om terug te keren klik op index onder aan de pagina.

Secure Computing

[Secure Computing website](#)

[Secure Computing op Facebook](#)

[Aktueel](#)

[Over Pokémon, openbare orde, criminaliteit en politie](#)

[Onderzoekers ontwikkelen oplossing voor ransomware](#)

[Politie gaat slachtoffers ransomware helpen](#)

[Microsoft waarschuwt voor ransomware die spontaan voortplant](#)

[De lucratieve handel in IP-adressen](#)

[Overheid gaat burgers voorlichten over wifi-tracking](#)

[Opkomende malware luistert je telefoongesprekken af](#)

[Politie waarschuwt bewoners via Burgernetmail voor inbraken](#)

[Organisaties vrijwel weerloos tegen DDoS-aanvallen](#)

[Aanslagen en sociale media](#)

[Bezoekers 'datingsites' bestookt door nepprofielen](#)

[Meesterbrein achter omvangrijke ceo-fraude opgepakt](#)

[CBS: veel Nederlanders niet handig met software](#)

[Meeste cybercriminelen hebben weinig technische kennis](#)

[Kabinet wil passend antwoord op gebruik encryptie terroristen](#)

[Europese richtlijn voor cybersecurity aangenomen](#)

[Veel veranderd sinds de Snowden-onthullingen](#)

[AVG beste gratis virusscanner voor Mac OS X](#)

Vaste rubrieken

[Snapshots](#) / [Cops in Cyberspace](#) / [Video](#) / [Wetsartikelen](#) / [Handig](#) / [One Drive](#) / [Overzichtstabel cybercrime](#)

AKTUEEL

Secure Computing

Een Nederlandstalige e-mail die op dit moment wordt verstuurd en stelt dat er een pakket niet kon worden afgeleverd bevat in werkelijkheid ransomware. Het bericht is zogenaamd van een transportbedrijf afkomstig en laat de ontvanger weten dat er een pakket niet kon worden afgeleverd. Via een link in de e-mail kan er een document worden gedownload om een nieuwe afspraak te maken. Het gaat om een Word-document met een kwaadaardige macro. Macro's staan vanwege veiligheidsredenen standaard in Microsoft Office uitgeschakeld.

Onderzoekers hebben een nieuwe ransomware-variant ontdekt die op besmette computers een afbeelding van Hitler toont en na een uur allerlei gegevens van de gebruiker verwijderd. In tegenstelling tot crypto-ransomware versleutelt de "Hitler-ransomware" geen bestanden.

Het verwijdert de extensie van alle bestanden in bepaalde directories en vergrendelt de computer. Vervolgens verschijnt er een klok die aftelt. Gebruikers hebben een uur de tijd om via een Vodafone-kaart het gevraagde losgeld van 25 euro te betalen. Gebeurt dit niet, dan laat de ransomware de computer crashen door het proces crss.exe te beeindigen. Dit veroorzaakt een crash of een Blue Screen of Death.

Voor welke gijzelsoftware moet je momenteel het meest oppassen?

Locky

Wat: Locky is ransomware die in Nederland relatief vaak voorkomt en zich volgens ESET 'in snel tempo aan het verspreiden is'. Het virus is in staat verscheidene soorten bestan-

den te versleutelen, waaronder documenten, afbeeldingen en video's.

Hoe: Locky komt binnen via bijlagen in e-mails, die zich vaak voordoen als Word-document. Zodra deze wordt geopend, wordt gevraagd om Office-macro's in te schakelen. Zodra je dat doet, wordt de ransomware uitgevoerd en krijg je de boodschap dat je moet betalen.

Oplossing: Op moment van schrijven is er nog geen manier gevonden om Locky te omzeilen, wanneer een computer eenmaal geïnfecteerd is.

UltraCrypter/CryptXXX

Wat: UltraCrypter is versie 3.0 van CryptXXX en is een afgeleide van CryptoWall. Bestanden worden versleuteld met het RSA-4096-algoritme en krijgen de .crypt-extensie mee. Daarnaast steelt de ransomware je wachtwoorden.

Hoe: UltraCrypter/CryptXXX komt binnen via bijlagen in e-mails, of via links naar websites die een Angler Exploit Kit distribueren.

Oplossing: Wie getroffen is door CryptXXX-ransomware kan een tool van Kaspersky downloaden (.exe) om weer toegang te krijgen tot getroffen bestanden, zonder losgeld te betalen. Helaas werkt de decryptor niet meer sinds de ransomware is omgedoopt tot UltraCrypter.

ZCryptor

Wat: ZCryptor is een van de eerste vormen van ransomware die wordt aangeduid als 'cryptoworm'. Onder meer Microsoft waarschuwt hiervoor.

Hoe: De ransomware kan binnenkomen door macro-exploitatie, nep-installatiebestanden of geïnfecteerde mails, maar is daarnaast vooral notoir omdat het zichzelf kan kopiëren naar gekoppelde usb-apparaten. Op die manier

heeft de gijzelsoftware een veel groter bereik dan we tot op heden gewend waren.

Oplossing: Voor de ZCryptor-worm zijn nog geen oplossingen voor handen. Voorkomen kan echter wel degelijk, bijvoorbeeld door antivirussoftware up-to-date te houden.

TeslaCrypt

Wat: TeslaCrypt was één van de meestvoorkomende vormen van ransomware, totdat de makers ervan opvallend genoeg zelf de handdoek in de ring gooien.

Hoe: Deze gijzelsoftware komt binnen via e-mailbijlagen in .zip-vorm, met daarin een JavaScript-bestand dat TeslaCrypt uiteindelijk binnenhaalt.

Oplossing: Omdat de cybercriminelen de universele sleutel hebben vrijgegeven, kun je onder meer deze tool van ESET gebruiken om weer toegang te krijgen tot je bestanden.

Crysis

Wat: Crysis is een relatief nieuwe vorm van ransomware die veel verschillende bestanden op het oog heeft, en volgens ESET telkens vaker voorkomt.

Hoe: Crysis komt binnen via bijlagen in e-mails of verpakt als een installatiebestand voor ogenschijnlijk onschuldige software. Het kan zich daarnaast verspreiden naar netwerkdrives en verwisselbare schijven. De ransomware nestelt zich diep in het register, geeft zichzelf administrator-rechten en laat 'alleen strikt noodzakelijke systeembestanden ongevoerd'.

Oplossing: Voor Crysis zijn er nog geen oplossingen voor handen. Enkel door losgeld te betalen krijg je weer toegang tot versleutelde bestanden, tenzij het een verouderde variant betreft. Dan kan contact worden gezocht met ESET, zegt het bedrijf.

Alle polities ter wereld hebben het reuze druk met de nieuwste rage.

Over Pokémon, openbare orde, criminaliteit en politie

In Melbourne, Australië werd een overstekende jonge vrouw die naar Pokémon zocht, doodgereden door een man in een gestolen auto;

in San Diego, VS vielen twee mannen van een klif toen ze een zeldzaam Pokémonfiguurtje zochten;

in Antwerpen, België werd een winkelstraat afgesloten nadat een massa Pokémon-jagers daarvan beslag had genomen;

in Roubaix, Frankrijk kregen Pokémon-zoekers slaande ruzie met drugsdealers – ‘dit is ons terrein’.

In Canada schoot een vrouw met een luchtbuik op Pokémon-spelers omdat haar straat in een ‘gym’ was veranderd en tientallen fans in haar voortuin ronddoelden.

Vanuit Engeland komen verhalen over ‘poke-crime’ waarbij Pokémon-zoekers worden beroofd, ‘at gunpoint’, van hun smartphone;

uit Japan komt de waarschuwing toch vooral geen Pokémon te zoeken in de buurt van de kerncentrale in Fukushima.

Uit Rio de Janeiro komen ten slotte al verontrustende berichten van Olympische sporters die zeer teleurgesteld zijn dat er in het Olympische dorp géén Pokémon te vinden zijn. Dat de riolering en de electra het niet doen, akkoord, maar dat er geen Pokémon zijn ...

Kortom, alle polities ter wereld hebben het reuze druk met de nieuwste rage.

Enfin. Hier in Nederland werd een buschauffeur ontslagen die Pokémon speelde achter het stuur van een volle bus. Reizigers hadden gefilmd hoe hij al spelend over de N11 reed. In Zeewolde zocht de politie vorige week urenlang naar een vijfjarig meisje dat op eigen houtje op Pokémon-jacht was gegaan. In Assen werd een jochie van 14 aangehouden die om één uur ‘s nachts op de brommer van zijn vader in de binnenstad op Pokémon-jacht was. recentelijk vonden twee Pokémon-spelers in Den Haag een stervende man. Ze belden de politie maar reanimatie kwam te laat. In Zeist waarschuwde de politie voor de overlast die Pokémon-zoekers veroorzaken. ‘Er ligt opvallend

veel afval in het park’, reden voor agenten om vaker te controleren ‘en zo nodig te bekeuren’.

In de gemeente Stichtse Vecht heeft de politie Pokémon-jagers opgeroepen te helpen in de strijd tegen autoinbrekers – extra ogen en oren: er zijn veel Pokémon te vinden in een buurt waar de laatste tijd veel ingebroken wordt.

De politie Hellevoetsluis heeft verder al spelregels opgesteld voor Pokémon-jagers, zo twitterde wijkagent Remco Hoogstad. Een daarvan is vooral niet te parkeren ‘waar het mag’. De regels komen nadat twee automobilisten zijn bekeurd die een plantsoen inreden omdat hun mobiel aangaf dat ze daar moesten zijn.

Wel heel creatief zijn politiekorpsen in de VS waar ze proberen boeven te vangen met Pokémon. In Smithfield, Virginia zette agent Bryan Miller op facebook dat de zeer zeldzame Ditto op het politiebureau te vinden was. Maar omdat Ditto zo zeldzaam is, ‘kunnen we maar een gelimiteerd aantal mensen toelaten’. Maar op dat lijstje stonden natuurlijk geen gewone burgers; wel mensen met een openstaand arrestatiebevel. Tja.

In New Hampshire werd een soortgelijke grap uitgehaald met de even zeldzame Charizard. Ook hier werden voortvluchtigen uitgenodigd langs te komen. In Detroit had zo’n actie succes. Een gezochte man op een fiets zag niet dat een ‘gym’, waar Pokémon kunnen trainen, feitelijk het politiebureau was. De man werd herkend en gearresteerd.

Van geheel andere orde is het bericht uit Brussel. Daar zijn enkele agenten berispt omdat ze in diensttijd naar Pokémon zochten. Enkele Brusselaars dienden klacht in, zonechef Johan de Becker stelde een intern onderzoek in. ‘Deontologisch kan dit niet’. Ook Belgische media waren kritisch. ‘In België geldt terreurniveau 3 maar de agenten zoeken Pikachu en zijn kompanen’, schreef Het Laatste Nieuws. Uitgezocht wordt in ieder geval of de agenten het met een eigen smartphone deden of met een diensttelefoon ...



Onderzoekers van de Universiteit van Florida hebben een oplossing ontwikkeld om ransomware te stoppen. De oplossing fungeert als een soort van waarschuwingssysteem waarbij de ransomware een aantal bestanden mag versleutelen voordat het wordt gestopt.

Onderzoekers ontwikkelen oplossing voor ransomware

CryptoDrop, zoals de oplossing wordt genoemd, is dan ook niet ontwikkeld om ransomware-infecties op computers te voorkomen. "Ons systeem is een soort van waarschuwingssysteem. Het voorkomt niet dat de ransomware begint .. het voorkomt dat de ransomware alle bestanden kan versleutelen", zegt onderzoeker Nolen Scaife. Gebruikers raken dan alleen een paar documenten of bestanden kwijt, in plaats van alles op de harde schijf. Daarnaast hoeven ze geen losgeld te betalen, gaat Scaife verder.

Tijdens een test met 492 verschillende ransomware-exemplaren van 14 families wist CryptoDrop 100% van de aanvallen te detecteren en te stoppen, waarbij gemiddeld 10 van de 5100 bestanden op de computers werden versleuteld. "Ongeveer een tiende van één procent van de bestanden ging verloren", laat onderzoeker Patrick Traynor weten.

Monitoren

In plaats van de programma's te monitoren die aanpassingen aan bestanden maken, monitort CryptoDrop de bestanden van de gebruiker. Het systeem kan verdachte bestandsactiviteiten herkennen en vervolgens het verantwoordelijke proces stoppen. Hiervoor kijkt het systeem naar drie verschillende hoofdindicatoren, namelijk het overschrijven van bestanden, het verplaatsen van bestanden en het vervangen van bestanden. Ransomware blijkt vaak deze activiteiten allemaal uit te voeren, terwijl dat niet het geval is bij legitieme programma's.

Zodoende kan CryptoDrop zeer snel de ransomware detecteren en stoppen, zonder dat er veel bestanden verloren gaan. Dit zorgt er weer voor dat slachtoffers niet hoeven te betalen en de cybercriminelen achter de ransomware geen inkomsten ontvangen, zodat hun verdienmodel instort en het niet meer loont om ransomware te maken. Het onderzoeksteam heeft inmiddels een volledig werkend prototype voor Windows ontwikkeld en zoekt nu een partner om het op de markt te brengen.



Een speciale website die de Nederlandse politie en Europol samen met twee bedrijven hebben ontwikkeld moet slachtoffers van ransomware helpen.

Politie gaat slachtoffers ransomware helpen

Ransomware is een type virus dat bestanden van gebruikers ontoegankelijk maakt. Pas na betaling kunnen ze weer bij hun bestanden.

Op de website, [No More Ransom](#), kunnen slachtoffers programmaatjes downloaden die ze kunnen gebruiken om hun bestanden weer toegankelijk te maken, zonder dat ze hoeven te betalen.

'Betaal nooit'

Waterdicht is de oplossing niet, benadrukt Europol. Het is dan ook belangrijk dat gebruikers opletten op internet. "En het belangrijkste advies: betaal niet!", zei Steven Wilson van de politie-organisatie tijdens een persconferentie in Den Haag.

De programmaatjes van Europol werken enkel bij gijzelvirussen waarvan onderzoekers de zogenoemde encryptiesleutels hebben kunnen achterhalen. Op dit moment gaat het om vier verschillende ransomware-virussen die onschadelijk kunnen worden gemaakt, waaronder de Shade -, TeslaCrypt- en CoinVault-virussen.

De programmaatjes zijn ontwikkeld in samenwerking met chipfabrikant Intel en beveiligingsbedrijf Kaspersky. "Van oorsprong richt de politie zich vooral op onderzoeken, maar voor de strijd tegen cybercrime is meer samenwerking nodig", aldus Wilbert Paulissen, hoofd van de nationale recherche.

Volgens Paulissen gaat het onderzoek naar ransomware nog steeds door, maar wordt op deze manier het verdienmodel van makers van ransomware verstoord.

Nederland en ransomware

Hoe vaak Nederlanders slachtoffer zijn van ransomware is moeilijk te zeggen. Vorige week bleek echter wel uit onderzoek van Symantec dat Nederland wereldwijd op de vierde plek staat als het gaat om ransomware-besmettingen. Daarbij gaat het echter wel om meldingen bij Symantec; een volledig beeld geeft dat niet.

Ook Nederlandse overheden zijn vaak slachtoffer, blijkt uit cijfers waar het AD melding van maakt. Elke tien dagen wordt een Nederlandse overheidsinstelling aangevallen; het is echter onduidelijk hoe veel van die aanvallen succesvol zijn.



Windows-gebruikers opgelet: een nieuw type ransomware kan je computer versleutelen én zichzelf verspreiden via harde schijven.

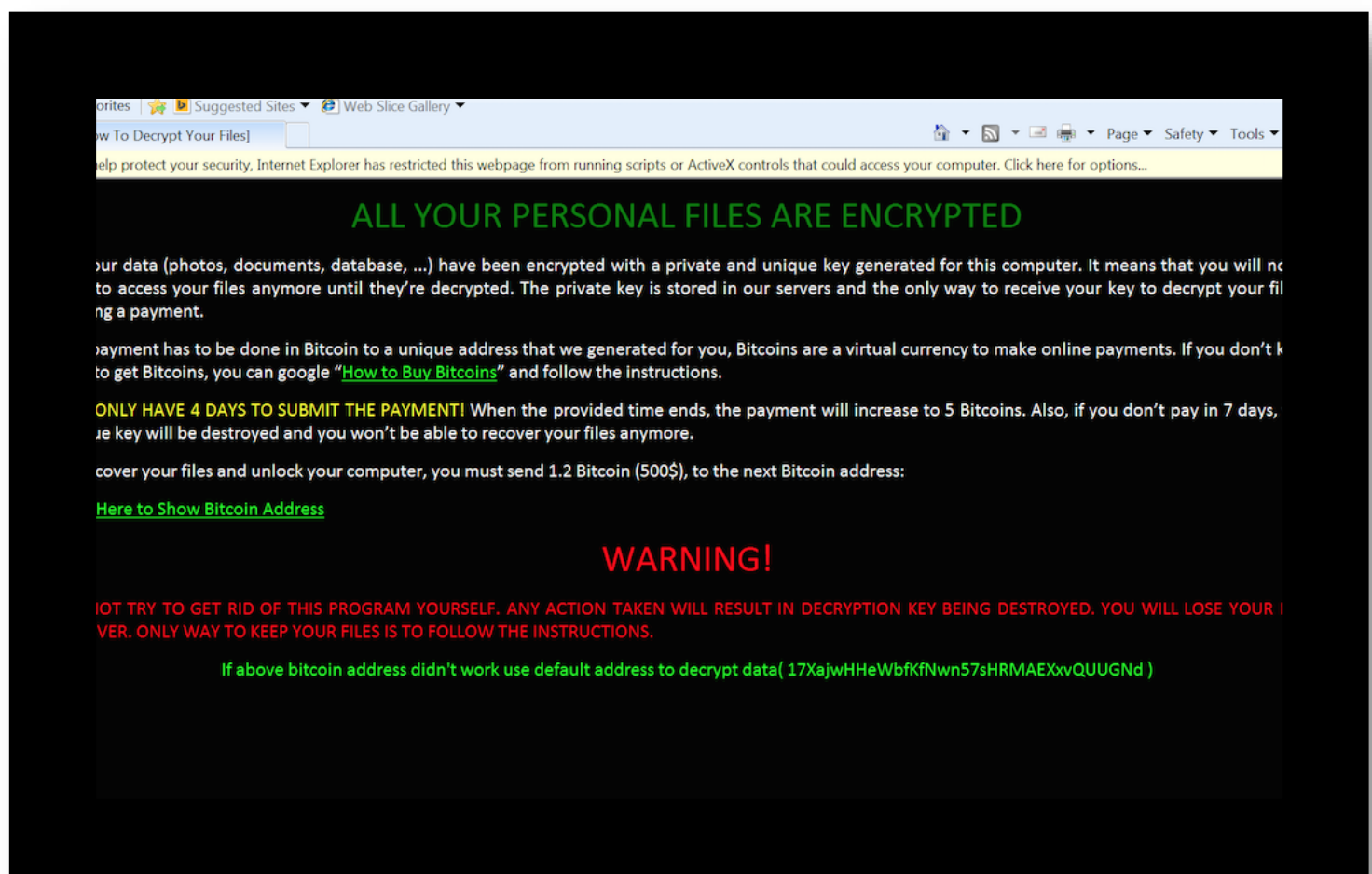
Microsoft waarschuwt voor ransomware die spontaan voortplant

Ransomware volgt meestal een vrij simpel proces, bestaande uit infectie en versleuteling. Systemen worden besmet door het klikken op onveilige links of bestanden, en normaliter kan de malware zich zelf niet van gebruiker tot gebruiker verspreiden. Tot nu: Microsoft ontdekte namelijk een ransomware-type dat zichzelf op eigen basis kopieert.

De ransomware, zCrypt genaamd, plaatst bij infectie een autorun.inf-bestand op verwijderbare harde schijven of een netwerkschijf. Dat maakt het makkelijk om bijvoorbeeld via usb-sticks een hele resem aan systemen te infecteren. Een usb-stick die aangesloten werd op een geïnfecteerde computer en daarna geopend wordt door een ander systeem, zal de malware automatisch overdragen en ervoor zorgen dat zCrypt ook de data op die laatste versleutelt.

Zulke acties doen eerder aan het gedrag van een worm denken en komen in de regel niet voor bij conventionele ransomware. De ontwikkeling brengt nieuwe risico's met zich mee voor het gebruik van verwisselbare harde schijven; niet alleen is ransomware een online gevaar, de bedreiging zet zich op deze manier ook voort buiten het web.

Volgens Trend Micro viseert ZCrypt vooral oudere Windows-versies zoals Windows XP, en Windows 7 en 8. Bijna 90 bestandstypes worden versleuteld, waarna doorgaans 1,2 bitcoin gevraagd, oftewel zo'n 585 euro. Zoals altijd raadt Microsoft aan om systeemupdates zo snel mogelijk uit te voeren, geregeld back-ups te maken en ook antivirus-programma's up-to-date te houden.



Nu de schaarste aan IP-adressen van het oude soort toeneemt, stijgen de prijzen. Dat trekt criminelen aan die IP-adressen kapen om ze voor veel geld door te verkopen.

De lucratieve handel in IP-adressen

Internetbedrijven die willen blijven groeien of providers die nieuwe abonnees krijgen: allemaal hebben ze vroeg of laat behoefte aan nieuwe IP-adressen. Elk apparaat op internet heeft een IP-adres nodig, maar in het IPv4-systeem zijn er slechts 4 miljard adressen beschikbaar. Nieuwe IPv4-adressen zijn daardoor erg schaars geworden, terwijl de overgang naar opvolger IPv6 nog vele jaren duurt. Het gevolg is een levendige handel in IPv4-adressen, schrijft Maarten Reijnders in Bright Ideas. Hij sprak onder meer met Erik Bais van Prefix Broker, dat kopers en verkopers van IP-adressen aan elkaar koppelt.

In 2013 werd er per IP-adres gemiddeld zo'n 5 of 6 euro betaald, in 2014 steeg dat naar 7 tot 8 euro en vorig jaar schommelde de prijs volgens Bais tussen de 9 en 12 euro. Toch leuk als je toevallig nog wat IP-adressen hebt liggen. Zo ontdekte Bais dat de politie in het Engelse Northumbria op een flinke partij ongebruikte IP-adressen zat. "Ze wisten daar helemaal niet dat die IP-adressen van hen waren. Van het geld dat de verkoop opleverde, konden ze het tehuis voor gepensioneerde agenten helemaal opknappen: het werd opnieuw geschilderd, iedereen kreeg een nieuwe tv."

Ook criminelen hebben zich op de IP-adressen gestort. Zo kaapte in 2014 een Bulgaarse bende IP-adressen van het Nederlandse ministerie van Buitenlandse Zaken. De Bulgaren gebruikten de adressen maar tijdelijk, maar andere criminelen nemen IP-ruimte permanent over met als doel om de adressen vervolgens weer door te verkopen. "Nagemaakte documenten, Roemeense notarissen die vervalste stempels zetten: het gebeurt allemaal", vertelt Bais. Aan het Amsterdamse RIPE, dat het overzicht bijhoudt van wie eigenaar is van welke ip-adressen in Europa, de ondankbare taak om te controleren of er geen sprake is van valsheid in geschrifte en poging tot diefstal.



De overheid gaat burgers voorlichten over wifi-tracking, zo heeft minister Kamp van Economische Zaken op Kamervragen van D66 laten weten. Aanleiding voor de vragen was een brief van de Autoriteit Persoonsgegevens waarin winkels en gemeenten werden opgeroepen om zich aan de regels voor wifi-tracking te houden.

Overheid gaat burgers voorlichten over wifi-tracking

Minister Kamp laat weten dat de toezichthouder dit jaar geen onderzoek heeft gedaan naar het gebruik van wifi-tracking in concrete gemeenten en winkels. "Het is dus niet bekend of gemeenten en winkels zich aan de regels houden", aldus de minister. De Autoriteit Persoonsgegevens had van verschillende mensen die zich zorgen over wifi-tracking maken signalen ontvangen, waarop de toezichthouder verschillende gemeenten en winkels een brief stuurde.

Via wifi-tracking kunnen winkels en gemeenten zien waar mensen zich bevinden en hoe ze zich op een bepaalde locatie bewegen. Hiervoor worden locatiegegevens samen met het unieke nummer van een smartphone opgeslagen en verwerkt. Organisaties mogen deze persoonsgegevens volgens de Wet bescherming persoonsgegevens (Wbp) alleen verwerken als zij daar een zogenoemde wettelijke grondslag voor hebben. Organisaties die wifi-tracking inzetten moeten mensen daarnaast informeren over welke gegevens worden verzameld en waarvoor dat gebeurt. Volgens de minister heeft de Autoriteit Persoonsgegevens niet geconstateerd dat gemeenten zich niet aan de regels houden.

D66 vroeg de minister ook of hij bereid is om in campagnes over cyberbewustzijn het uitzetten van wifi en bluetooth mee te nemen, zodat mensen ongewenste tracking kunnen voorkomen. Daarop wijst Kamp naar de website veiliginternetten.nl, waar al allerlei adviezen worden gegeven. "Het thema wifi-tracking zal ook op de website worden opgenomen", laat de minister in zijn antwoord weten. Op de website wordt het uitschakelen van bluetooth al besproken, alleen dan om 'spontaan contact' te voorkomen.



Wetenschappers zijn een nieuw Trojaans paard op het spoor: Spy-Note kan onder andere je berichten lezen en je telefoongesprekken afluisteren.

Opkomende malware luistert je telefoongesprekken af

Security-bedrijf Palo Alto Networks waarschuwt voor een Trojaans paard op Android dat wellicht binnenkort een opmars zal maken. SpyNote, zoals de malware bekendstaat, werd enkele dagen geleden via malafide fora verspreid op het dark web. Wetenschappers verwachten nu dat een breed publiek aan cybercriminelen het trojaans paard in de nabije toekomst zullen inzetten bij aanvallen.

De malware lijkt nog het meest op een RAT, een remote administration tool waarmee iemand op afstand de controle over je toestel kan overnemen. Zo geeft SpyNote de cybercrimineel toegang tot sms-berichten, de camera, gps-locatie, microfoon, en laat het zelfs toe om telefoongesprekken af te luisteren.

Eens de malware geïnstalleerd is, is het moeilijk om ervan af te raken, zegt Palo Alto Networks. SpyNote verwijdert immers automatisch het app-icoontje, zodat het uit het zicht blijft, en downloadt automatisch updates. Vooraleer de installatie kan doorgaan, moeten gebruikers echter zelf de APK downloaden en toestemming geven voor een hele lijst aan eisen.

Gebruikers doen er daarom goed aan om enkel apps te downloaden van betrouwbare uitgevers, zoals de Google Play Store – hoewel ook die niet waterdicht is – en altijd op te letten welke toestemmingen een app vereist. Lijken die onzinnig, is het veiliger om eens te googlen of de applicatie wel veilig is.



De politie is onlangs begonnen om bewoners in de buurt van een inbraak via e-mail te waarschuwen. Het gaat om nieuwe service van Burgernet, genaamd Burgernetmail.

Politie waarschuwt bewoners via Burgernetmail voor inbraken

Deelnemers waarvan het e-mailadres bekend is worden per e-mail ingelicht wanneer er een woninginbraak in hun buurt heeft plaatsgevonden.

In de mail staat waar, wanneer, hoe laat en op welke manier de inbraak heeft plaatsgevonden. Ook geeft Bureau Burgernet preventietips hoe een inbraak die op deze manier is gepleegd in de toekomst voorkomen kan worden. Betrokken deelnemers wordt gevraagd om alle informatie die zij hebben of verdachte situaties die zij zich herinneren door te geven aan de politie. "Om het project te laten slagen is het belangrijk dat er zoveel mogelijk mensen meedoen met Burgernet", zegt John Janse van de recherche.

"Inbrekers slaan na een geslaagde inbraak namelijk vaker toe in dezelfde buurt. De nieuwe service van Burgernet vormt een aanvulling op dit buurtonderzoek. De betrokken bewoners kunnen digitaal antwoord geven met behulp van een invulformulier", aldus Janse. "Vaak denken bewoners dat wat zij gezien hebben, wel niet zo spannend zal zijn. Maar voor de politie kan dat net het ontbrekende puzzelstukje zijn. Meld het dus vooral, dan is de politie op de hoogte van alle mogelijke informatie."

Burgernetdeelnemers die alleen de app hebben gedownload, zijn niet volledig bij Burgernet aangemeld. Hun e-mailadressen zijn niet bekend bij Bureau Burgernet. Wie dit wil kan zijn of haar e-mailadres via de website van Burgernet registreren. De nieuwe service van Burgernet maakt deel uit van het project Waak voor Inbraak. Bij dit project werken bewoners, ondernemers, gemeenten, politie, Openbaar Ministerie, provincie en diverse andere partners samen aan de veiligheid in de eigen omgeving.

BURGERNET
Werket!

Er is vrij weinig dat organisaties kunnen uitrusten tegen ddos-aanvallen. Maar dat wil niet zeggen dat er lijdzaam moet worden toegekeken hoe de servers van je website worden platgegooid.

Organisaties vrijwel weerloos tegen DDoS-aanvallen

Een 'distributed denial of service'-aanval, zoals een ddos-aanval voluit heet, is een aanval die wordt uitgevoerd door zogenaamde botnets. Een botnet is eigenlijk een groot netwerk van geïnfecteerde computers die door kwaadwillenden op afstand kunnen worden bestuurd. Zo kan de computer thuis ook zonder jouw medeweten onderdeel zijn van een botnet. De mensen die een ddos-aanval willen uitvoeren op de servers van een bepaald bedrijf, sturen alle pc's in zo'n botnet, dat kan bestaan uit miljoenen computers wereldwijd, naar de website van dat bedrijf. De servers waarop die website draait, kunnen die enorme vraag niet aan en gaat plat. Dat is in het kort een ddos-aanval.

Risicoanalyse

Eigenlijk kun je je als organisatie nauwelijks wapenen tegen zulke aanvallen. Natuurlijk zijn er technologische maatregelen zoals intrusion prevention, web application firewalls en intrusion protection anti flooding, maar net als met gewone inbrekers geldt: als ze naar binnen willen, komen ze er echt wel in. De technologische maatregelen zijn solide sloten, maar daar heb je bar weinig aan als er iemand met een bulldozer door je veranda rijdt.

Imagoschade

Als de website bedrijfskritisch is, dan is de meest eenvoudige manier om te zorgen voor uptime, het outsourcen naar een hostingpartij. Daarbij kan er ook gekozen worden om de site over meerdere datacenters te verspreiden, zodat er in geval van een aanval uitgeweken kan worden. Maar dat zijn vooral maatregelen om ervoor te zorgen dat je zo weinig mogelijk schade

ondervindt van een aanval. Het zijn geen oplossingen om een aanval tegen te gaan, omdat die er feitelijk niet echt zijn. Zorg ervoor dat je een duidelijk stappenplan hebt, zodat je weet wat er moet gebeuren op het moment dat de bedrijfswebsite ten prooi valt aan een ddos-aanval.

Modern protest

Het aantal ddos-aanvallen stijgt gestaag. Dat is te wijten aan het stijgende belang van internet. Pas de afgelopen jaren is internet voor veel bedrijven bedrijfskritisch geworden. De risico's zijn groter, maar het gewin dus ook. Ddos-aanvallen worden niet alleen uit financieel gewin uitgevoerd, maar er zijn ook steeds meer sociaal-maatschappelijke aanvallen. Een groep als Anonymous laat op zo'n manier heel duidelijk merken aan organisaties wat zij vinden dat correct is en wat niet. Het is een moderne manier van actie voeren, maar met het grote verschil dat niet het ganse land er last van heeft.

In principe hoeft een organisatie een ddos-aanval niet te melden onder de komende EU-wetgeving op gebied van databeveiliging. Feitelijk zijn het twee zaken die los staan van elkaar. Toch sluimert daar een gevaar. Hoe weet een organisatie nu zeker dat het alleen een ddos-aanval was en dat er niet ook iemand binnen is geweest? Bij een ddos-aanval gaat alle aandacht daar naar uit. Als hackers kwaad willen, zouden ze dat met zo'n aanval kunnen verbergen. Het is een theoretische mogelijkheid, maar dat betekent dat in de toekomst ook ddos-aanvallen gemeld moeten worden.



Als al die aanslagen, schietpartijen en massamoorden van de laatste tijd iets gemeen hebben, dan is het wel dat er in al die openbronnen, #osint, sociale media of hoe je ze ook noemen wilt, ongelooflijk veel te vinden is over daders en slachtoffers.

Aanslagen en sociale media

Het blijft fascinerend te zien hoe op twitter, facebook en al die andere netwerken van alles rondgaat: foto's, filmpjes – niets blijft geheim. Of het allemaal klopt, is iets anders maar feit is wel dat we bij alles kunnen 'meekijken'. En dus zien we, via twitter, zowel de Syrische asielzoeker die in Reutlingen een vrouw neerstak, als de machete waarmee hij dat deed. En dus lezen we op zijn facebookpagina dat Mohamed Bouhlel, die met een vrachtwagen in Nice meer dan tachtig mensen doodde, IS-aanhanger werd, naar onthoofdingsfilmpjes keek, online zocht naar informatie over andere aanslagen en al sinds een jaar bezig was met zijn terreurdaad.

En dus weten we (vrijwel) alles over Ali David Sonboly die in München negen mensen doodde bij een McDonalds. Dat hij werd gepest op school, zich uitleefde in gewelddadige videospelletjes en in die games veel chatte over eerdere schietpartijen. Dat hij andere schoolshooters verheerlijkte, online informatie zocht over Breivik én dat hij 'op een donkere afdeling van het internet' de Glock-17wist te kopen waarmee hij zijn actie uitvoerde. En dat hij zijn slachtoffers naar de McDonalds lokte via facebook: onder het alias 'Selina Akim' plaatste Sonboly het bericht dat daar gratis eten werd uitgedeeld. 'Kommt heute um 16 Uhr Meggi am OEZ ich spendiere euch was wenn ihr wollt'.

Maar we weten ook veel over Gavin Long, de ex-marinier die in Baton Rouge, VS drie agenten doodschoot. Op sociale media schreef Long dat 'terugvechten de enige manier is om een bullebak te stoppen', dat hij al maandenlang boos was over de discriminatie van zwarte Amerikanen en dat hij zich online presenteerde als 'spiritueel adviseur'. Dat hij onder het alias Cosmo Setepenra allerlei filmpjes online zette waarin hij zich onder meer Arabieren en Indiërs die 'geen fuck' zouden geven om het lot van zwarte Amerikanen. En weten we dat een van de door Long gedode agenten, Montrell Jackson, vlak voor zijn

dood op facebook schreef dat hij moe en teleurgesteld was als hij aan het werk was.

Ondertussen waarschuwde de politie van München iedereen toch vooral te stoppen met het online verspreiden van beelden van slachtoffers. 'Stop daar mee', in hoofdletters, in twee talen. De tweet was vooral gericht aan de omstanders die op die bewuste vrijdagavond 'gretig en direct' foto's en video's verstuurden vanaf de plaats delict. Het korps adviseerde deze beelden te uploaden naar een speciale politiesite.

De actie was voor hoogleraar Henri Beunders (Erasmus Universiteit) aanleiding te pleiten voor een verbod op het direct openbaar uploaden van zulke beelden. 'Toen de Charlie Hebdo-schutters uit Parijs en hun medeplichtige in de joodse supermarkt waren omsingeld, konden ze via internet precies zien wat de politie op dat moment aan het doen was', zegt Beunders die opmerkt dat 'we' nog steeds niet goed gewend zijn aan wat we wel en niet online moeten zetten. 'Het uploaden van sommige beelden is gewoon veel gevaarlijker dan men denkt'.

Ook privacy speelt hier een rol. Iets langer geleden zagen we ook al hoe een verwarde man van het dak van een brandend pand in Amsterdam afsprong en verscheen er vorige week nog een video waarin iemand vanaf een (ander) dak ruziet met een omwonende. 'Het online zetten van die video geeft een beeld van de dader, maar de dader weet dan ook dat de politie weet waar hij is'. Volgens Beunders moet het OM een proefproces gaan voeren. 'Dat klinkt misschien hard, maar het zijn ook barre tijden'.



Dat de ene datingsite de andere niet is, zal niemand verrassend.
Maar volgens de Fraudehelpdesk zijn er wel erg veel datingsites
waarop alleen maar valse profielen staan.

Bezoekers 'datingsites' bestookt door nepprofielen

De Fraudehelpdesk telt er 'zeker 700'. De sites staan vol met niet-bestaande vrouwen maar vragen wel veel geld voor contact, van 60 cent tot 1 euro per bericht.

Brancheorganisatie Thuiswinkel.org wil daarom dat de politie en de Autoriteit Consument en Markt in actie komen om deze misleiding en fraude aan te pakken. Een van de dubieuze sites is Love2Date.nl waarop gebruiker Jacques in een avond al honderd euro kwijtraakte.

Een woordvoerder van die site verwijst naar de kleine lettertjes waar inderdaad staat dat profielen nep kunnen zijn en dat het bedrijf 'zich uitdrukkelijk het recht voorbehoudt om gesprekken te sturen via zelf gecreëerde profielen'.

Eigen schuld, dikke bult dus? Nee, want de sites adverteren ook met slogans als 'Hier de leukste singles' en 'Vind hier moeiteloos een perfecte match'. Er zijn zelfs gespecialiseerde bedrijven die 'ondernemers' helpen zulke misleidende datingsites op te zetten ... Binnen no time heb je een eigen datingsite met honderden profielen van niet-bestaande vrouwen, zo ondervond de NOS die wat uitprobeerde. Tja.

Het moet daarom veel makkelijker worden hiertegen op te treden, zegt ook voorzitter John Meuffels van het Keurmerk Veilig Daten. 'En als de bestaande wetgeving niet toereikend is, dan moet die worden aangevuld'. De Fraudehelpdesk spreekt van een 'juridisch schemergebied', de ACM zegt al honderd meldingen te hebben over datingsites en het ministerie van Justitie ... zegt dat het niet mogelijk is 'dit soort sites' juridisch aan te pakken zolang identiteitsfraude op internet nog niet echt strafbaar is.



**Hoe herken je ze? 7 tips! (of
sleep de bewuste foto naar
Google afbeeldingen)**

Interpol heeft samen met de Nigeriaanse autoriteiten het meesterbrein achter een omvangrijke fraude opgepakt waarbij honderden bedrijven voor miljoenen dollars werden opgelicht.

Meesterbrein achter omvangrijke ceo-fraude opgepakt

Het gaat om ceo-fraude, ook bekend als business email compromise. Oplichters doen zich in dit geval voor als de directeur of andere bestuurders van een organisatie of bedrijf en sturen vervolgens een e-mail naar iemand van de financiële afdeling.

In de e-mail wordt gevraagd om een groot geldbedrag naar een buitenlandse rekening over te maken. De afgelopen jaren is erop deze manier volgens de FBI 3,1 miljard dollar door de oplichters buitgemaakt. De nu aangehouden man wordt verdacht een bende van minstens 40 mensen te hebben aangestuurd, die duizenden van dergelijke scams uitvoerden. Wereldwijd werden er honderden slachtoffers gemaakt, die meer dan 60 miljoen dollar verloren. Eén bedrijf maakte zelfs 15,4 miljoen dollar over, zo stelt Interpol.

De bendeleider, die onder het alias "Mike" bekendstond, kon na informatie van het Japanse anti-virusbedrijf Trend Micro worden aangehouden. Het onderzoek naar de man begon eind 2014, toen er malware werd onderzocht die bij sommige gevallen van ceo-fraude was ingezet. Dit onderzoek leidde uiteindelijk naar Mike, waarna Trend Micro de informatie met Interpol deelde. Dit leidde eind juni tot de aanhouding van de man.



In vergelijking met inwoners van andere EU-landen kunnen Nederlanders goed overweg met computers en internet, maar de omgang met software is voor veel mensen nog altijd een probleem, aldus het Centraal Bureau voor de Statistiek (CBS).

CBS: veel Nederlanders niet handig met software

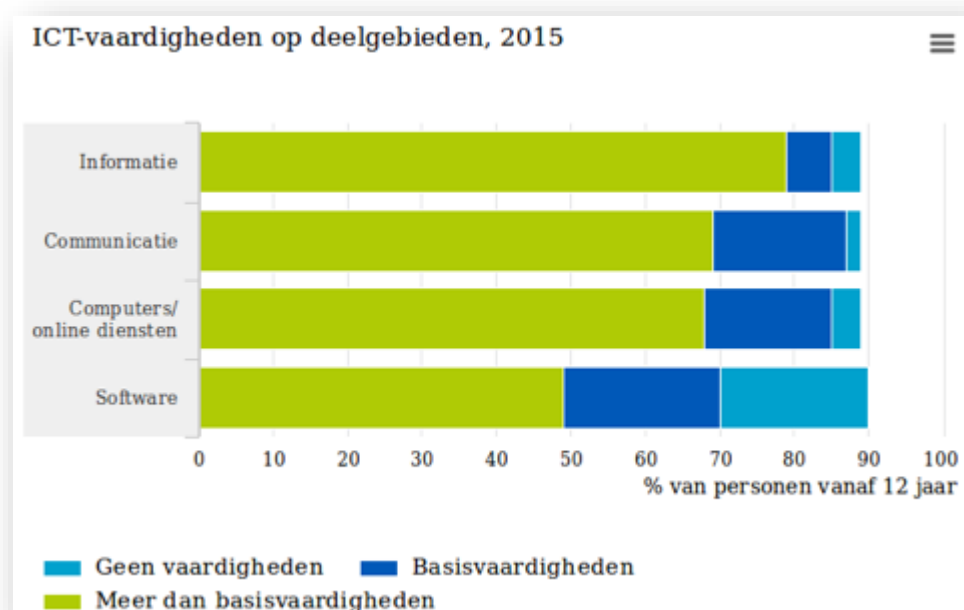
Samen met Luxemburg, Denemarken en Finland behoort Nederland tot de EU-landen waarvan de inwoners relatief veel ict-vaardigheden hebben. Van de 16- tot 75-jarige Nederlanders had vorig jaar ruim 40 procent meer dan basisvaardigheden, tegen minder dan 30 procent in de EU als geheel. Oost-Europese landen en ook Frankrijk en Italië scoren lager dan het Europese gemiddelde. De ict-vaardigheden zijn afgeleid van de antwoorden op de vraag welke computer- en internetactiviteiten men recent heeft uitgevoerd.

Het leeuwendeel van de Nederlanders van 12 jaar of ouder bezit ict-vaardigheden op minimaal basisniveau: in 2015 had ongeveer 30 procent basisvaardigheden en 40 procent meer dan basisvaardigheden in de omgang met computer en internet. Ruim 20 procent had weinig of geen vaardigheden en 10 procent had recent geen internet gebruikt. Wat mensen kunnen met ict verschilt sterk naar leeftijd en opleiding. Zo is het percentage met meer dan basisvaardigheden onder jongeren ruim zes keer zo groot als bij ouderen, en bij hoogopgeleiden bijna drie keer zo groot als onder laagopgeleiden. Tussen mannen en vrouwen zijn de verschillen veel kleiner.

Software

De meeste Nederlanders kunnen goed overweg met informatie en communicatie op internet. Op het gebied van software is dat echter minder: krap de helft beschikte vorig jaar over meer dan basisvaardigheden. Een op de vijf had helemaal geen vaardigheden in de omgang met software. Het gaat bijvoorbeeld om het gebruik van programma's voor tekstverwerking of het maken van presentaties.

Op het gebied van informatie, zoals zoeken via internet, bestanden verplaatsen, en foto's opslaan in de cloud had 80 procent van de Nederlanders meer dan basisvaardigheden. Ook met communicatie (zoals e-mailen, sociale netwerken, bellen via internet) en 'computers/online diensten', bijvoorbeeld online winkelen, apps installeren, online cursus volgen, had een ruime meerderheid vaardigheden die het basisniveau overstijgen.



De meeste cybercriminelen hebben relatief weinig technische kennis, het zijn dan ook een paar honderd internetcriminelen die de grootste dreiging vormen, zo stelt de Britse National Crime Agency (NCA) .

Meeste cybercriminelen hebben weinig technische kennis

Volgens de NCA neemt de dreiging van internetcriminaliteit toe, zoals ransomware en ddos-aanvallen. De reactie van Groot-Brittannië op deze groeiende dreiging schiet echter te kort, aangezien de criminelen voorop lopen, aldus de Britse opsporingsdienst. Die pleit dan ook voor een nauwere samenwerking tussen bedrijven, overheid en opsporingsdiensten om effectiever te kunnen optreden en cybercrime te voorkomen.

De NCA stelt verder dat de meest geavanceerde en grootste cyberdreiging voor Groot-Brittannië afkomstig is van een paar honderd internationale cybercriminelen, die meestal in georganiseerde groepen opereren. "Hoewel de grootste dreiging van deze internationale bendes afkomstig is, hebben de meeste cybercriminelen relatief weinig technische kennis", zo schetst de Britse opsporingsdienst. Deze criminelen zouden via online criminele marktplaatsen de vereiste expertise en tools weten in te schakelen. Daardoor kunnen ook minder ervaren cybercriminelen een groot aantal kwetsbaarheden aanvallen, aldus het rapport.

Bewustzijn

Om de problematiek aan te pakken wordt onder andere gepleit voor het vergroten van het bewustzijn van zowel eindgebruikers als bedrijven. Op dit moment zouden gebruikers namelijk onvoldoende kennis van cybercrime hebben. Veel bedrijven en de meeste eindgebruikers weten bijvoorbeeld niet hoe zich op internet moeten beveiligen en hoe ze een misdrijf moeten melden als het zich heeft voorgedaan.

In veel gevallen zouden slachtoffers namelijk niet eens weten dat ze het slachtoffer van een misdrijf zijn geworden. De NCA spreekt dan ook van een lange termijn uitdaging om mensen te onderwijzen en trainen. Organisaties moeten zich hier dan ook voor blijven inzetten om de gewenste verandering te kunnen bereiken.



Het kabinet wil de komende vijf jaar een "passend antwoord" op het gebruik van encryptie door terroristen. Dat staat in de Nationale Contraterrorismestrategie 2016-2020 die onlangs werd gepresenteerd.

Kabinet wil passend antwoord op gebruik encryptie terroristen

De strategie bouwt voort op de strategie van de afgelopen vijf jaar en is verder gebaseerd op het verwachte dreigingsbeeld voor de komende vijf jaar, alsmede op de kennis en ervaring die de afgelopen jaren zijn opgebouwd.

Volgens het technische rapport waarin de strategie uit de doeken wordt gedaan gaan de ontwikkelingen in het cyberdomein snel.

"Waakzaamheid is geboden, zeker waar het gaat om het opbouwen en benutten van hackvaardigheden en -kennis door jihadisten of toegang tot deze vaardigheden en kennis bij anderen." Het kabinet verwacht dat jihadisten het cyberdomein steeds slimmer, professioneler en georganiseerder zullen gaan gebruiken. "Zij zullen het cyberdomein steeds vaker inzetten als middel voor propaganda, rekrutering, fondsenwerving, onderlinge communicatie en informatie-vergaring voor fysieke aanslagen."

Volgens het rapport zijn algemene ict-vaardigheden en -kennis, zoals op het gebied van sociale media, veilig digitaal communiceren of zoekmachines, hiervoor al vaak voldoende. In andere gevallen, bijvoorbeeld bij illegale informatievergaring uit databases, kunnen hack-

vaardigheden behulpzaam of noodzakelijk zijn. "Deze verdere professionalisering kan er ook toe leiden dat jihadisten het cyberdomein gaan gebruiken als doelwit of als wapen."

De Nationale Contraterrorismestrategie noemt "digitale middelen" dan ook als één van de strategische uitgangspunten voor de komende periode. In de toelichting wordt gesteld dat de overheid de komende jaren een "passend antwoord" heeft op het gebruik van digitale middelen door extremisten en terroristen, zoals sociale media, het 'dark web' en encryptie. Hoe dit antwoord er in de praktijk zal komen uit te zien is niet bekendgemaakt. In januari presenteerde het kabinet nog het kabinets standpunt over encryptie. Daarin werd gesteld dat er op dit moment geen maatregelen tegen encryptie worden genomen.



Het Europees Parlement heeft deze week ingestemd met de Europese cybersecurityrichtlijn over Netwerk en Informatiebeveiliging (de NIB-richtlijn), die gericht is op het creëren van een gemeenschappelijk niveau van netwerk- en informatiebeveiliging binnen Europa.

Europese richtlijn voor cybersecurity aangenomen

De samenwerking tussen de Cyber Security Incident Response Teams in de verschillende lidstaten (zoals het NCSC) vormt hier een belangrijk onderdeel van. Digitale veiligheid houdt zich van nature niet aan de klassieke scheidslijnen van landsgrenzen, waardoor een gezamenlijke aanpak essentieel is. Zo worden bedrijven die aanbieders zijn van zogenoemde "essentiële diensten" met deze richtlijn verplicht om inbreuken in hun informatiesystemen te melden.

De Europese richtlijn treedt in augustus in werking. Aangezien het een Europese richtlijn betreft moeten de regels nog worden omgezet in nationale wetgeving. Lidstaten hebben 21 maanden om de richtlijn om te zetten, plus zes maanden om aanbieders van essentiële diensten aan te wijzen waarvoor de verplichtingen gaan gelden.

Zie hier het persbericht van het Europees Parlement.

Europese investeringen in cybersecurity

Deze week is tevens bekend geworden dat de Europese Commissie 450 miljoen euro steekt in privaat-publieke samenwerking waarmee initiatieven en innovaties op het gebied van cybersecurity worden gestimuleerd. Branches moeten daarmee de beschikking krijgen over een betere beveiliging tegen cybercriminaliteit. Daartoe heeft Euro-

pees Commissaris Günther Oettinger deze week een overeenkomst getekend met de ECSO, de European Cyber Security Organisation. De verwachting is dat de totale investeringen van dit publiek-private samenwerkingsverband in 2020 uitkomen op minimaal 1,8 miljard euro. De Europese gelden zijn afkomstig van het onderzoeks- en innovatieprogramma Horizon 2020, waarmee de Europese Commissie maatschappelijke vraagstukken wil oplossen en er naar streeft om het concurrentievermogen van Europa te vergroten.

De Europese Commissie vindt publiek-private samenwerking van belang, omdat 80 procent van alle bedrijven wel eens problemen met cybercriminaliteit heeft ondervonden en alleen een gezamenlijke aanpak effectief is. Dit sluit aan op de Nederlandse publiek-private aanpak. Het aantal cyberincidenten is vorig jaar met 38 procent gestegen en geen sector is uitgesloten van digitale dreiging, aldus de Europese Commissie. Het is dan ook broodnodig om gezamenlijk innovatieve en veilige technologieën te ontwikkelen die binnen diverse sectoren kunnen worden ingezet, zoals de energiesector, de gezondheidszorg, de transport- en financiële sector.



3 jaar geleden plaatste de Britse krant The Guardian één van de belangrijkste verhalen van het afgelopen decennium: De Amerikaanse inlichtingendienst NSA verzamelde de telefoondata van miljoenen mensen. Ruim 2 jaar lang kwam er steeds meer informatie naar boven over het grootschalig af luisteren door inlichtingen- en opsporingsdiensten.

Veel veranderd sinds de Snowden-onthullingen

Inmiddels zijn we 3 jaar verder, dus is het tijd om de balans op te maken. Wat is er allemaal veranderd sinds het NSA-schandaal?

Het eerste nieuws over het grote af luister-schandaal kwam op 6 juni 2013 naar buiten, door Guardian-journalist Glenn Greenwald. Het bleek het eerste verhaal te zijn in een serie schandalen die een lelijk inzicht gaven in een grootschalige, vaak illegale dataverzameloede van inlichtinge- en opsporingsdiensten. De verhalen waren afkomstig van klokkenluider Edward Snowden. We zijn inmiddels 3 jaar verder na de onthullingen. Op het eerste gezicht lijkt er maar weinig veranderd in de wereld na de Snowden-leaks. De publieke reactie was er wel één van woede, maar ook van onmacht. Wat kun je doen tegen zo'n gigantische organisatie waar zo weinig over bekend is? De grote demonstraties en woedende protesten bleven dan ook uit, en het argument "ach, ik heb toch niets te verbergen" werd steeds vaker geuit. En de NSA? Die verzamelt nog steeds veel informatie.

Toch zijn er wel degelijk veel dingen veranderd, met name in de manier waarop we naar privacy, anonimiteit en bescherming kijken.

Privacy is voor veel bedrijven een steeds belangrijker verkooppunt geworden, met name door de publieke opinie tegen de massasurveillance. Het meest opvallende daarvan is Apple, dat in een juridisch gevecht terecht kwam toen het weigerde een telefoon te ontsleutelen in een onderzoekszaak. Hoewel dat niet direct gerelateerd is aan massasurveillance, laat de ingewikkelde zaak wel zien dat het bedrijf veel waarde hecht aan privacy en anonimiteit. Dat is ook te zien in andere bedrijven zoals Google, dat in Android 6.0 (Marshmallow) de harde schijf van telefoons standaard versleutelt.

Ook andere sociale netwerken doen daaraan mee: Zo geven Google, Facebook en Twitter-

steeds vaker een waarschuwing als er data van een gebruiker wordt opgevraagd.

Van de andere kant is er ook veel stilte bij de bedrijven. Eén van de belangrijkste onthullingen van Snowden was die van het PRISM-programma, waarbij de NSA data kon aftappen bij diensten zoals Outlook en Gmail. Bedrijven als Google en Microsoft, maar ook Facebook, Twitter en anderen, hebben zich nauwelijks hardop uitgesproken tegen de massasurveillance.

Ook onder het publiek is het bewustzijn gegroeid, en steeds meer internetgebruikers weten zich te wapenen tegen surveillance. Dat is te zien in de stijging in gebruik van populaire privacytools zoals Tor, PGP-mail, of Linux-distro TAILS.

Iets meer toegankelijk zijn VPN's, en ook daar is een flinke stijging te zien in gebruik. Volgens onderzoek was er al een jaar na de Snowden-leaks een grote stijging in het gebruik van VPN's te zien. Idem dito voor browserplugins als HTTPS Everywhere, Ghostery of adblockers. Internetters weten zich steeds beter te beschermen.

Ook op veel andere, misschien wat minder duidelijke vlakken is privacy meer in het licht komen te staan. Zo is het makkelijker geworden om je privacyinstellingen op Google te veranderen, een indirect gevolg van de grotere bewustwording van gebruikers.

Dat gebruik van privacy-tools had volgens tegenstanders van Snowden ook een groot nadeel: Terroristen zouden nu weten waar de inlichtingendiensten op zochten, zodat ze nu alleen maar moeilijker te vinden waren. Het was mede daarom dat ex-CIA-directeur Holden zei dat Snowden moest worden opgehangen na de aanslagen in Parijs, omdat die mede door zijn onthullingen niet te voorkomen waren.

Dat bleek echter niet waar. Sterker nog, geen enkele van de terroristen gebruikte ook maar

enige vorm van encryptie tijdens de aanslagen in Parijs. Op de computer van Salah Abdeslam bleken alle plannen over de aanslagen makkelijk toegankelijk opgeslagen, zonder wachtwoorden of versleuteling. Bovendien communiceerden de aanslagplegers met elkaar via (onversleutelde) sms'jes.

Critici van de surveillanceprogramma's, en later zelfs de inlichtingendiensten zelf, durven zelfs verder te gaan door te zeggen dat de massasurveillance de NSA te veel data oplevert. Daardoor is het juist moeilijker om échte daders te vinden. Het programma werkt daarmee vaak juist averechts.

Edward Snowden moest Amerika ontvluchten na zijn onthullingen. Aanvankelijk zat hij in Hongkong, maar inmiddels heeft hij asiel gekregen in Rusland, waar hij nu nog woont. Mocht Snowden ooit terugkeren naar de VS, dan wacht hem een flinke straf. Technisch gezien kan hij voor landverraad de doodstraf krijgen (iets wat de voormalig CIA-directeur prima vindt), maar het Amerikaanse Openbaar Ministerie zegt dat dat niet gebeurt.

Edward Snowden is niet voor iedereen een held. De klokkenluider wordt door de Amerikaanse overheid nog steeds gezien als landverrader die 'levens in gevaar heeft gebracht' - maar ook dat sentiment verandert. Stukje bij beetje heeft Amerika namelijk toe moeten geven dat Snowden wel degelijk een publieke dienst had geleverd.

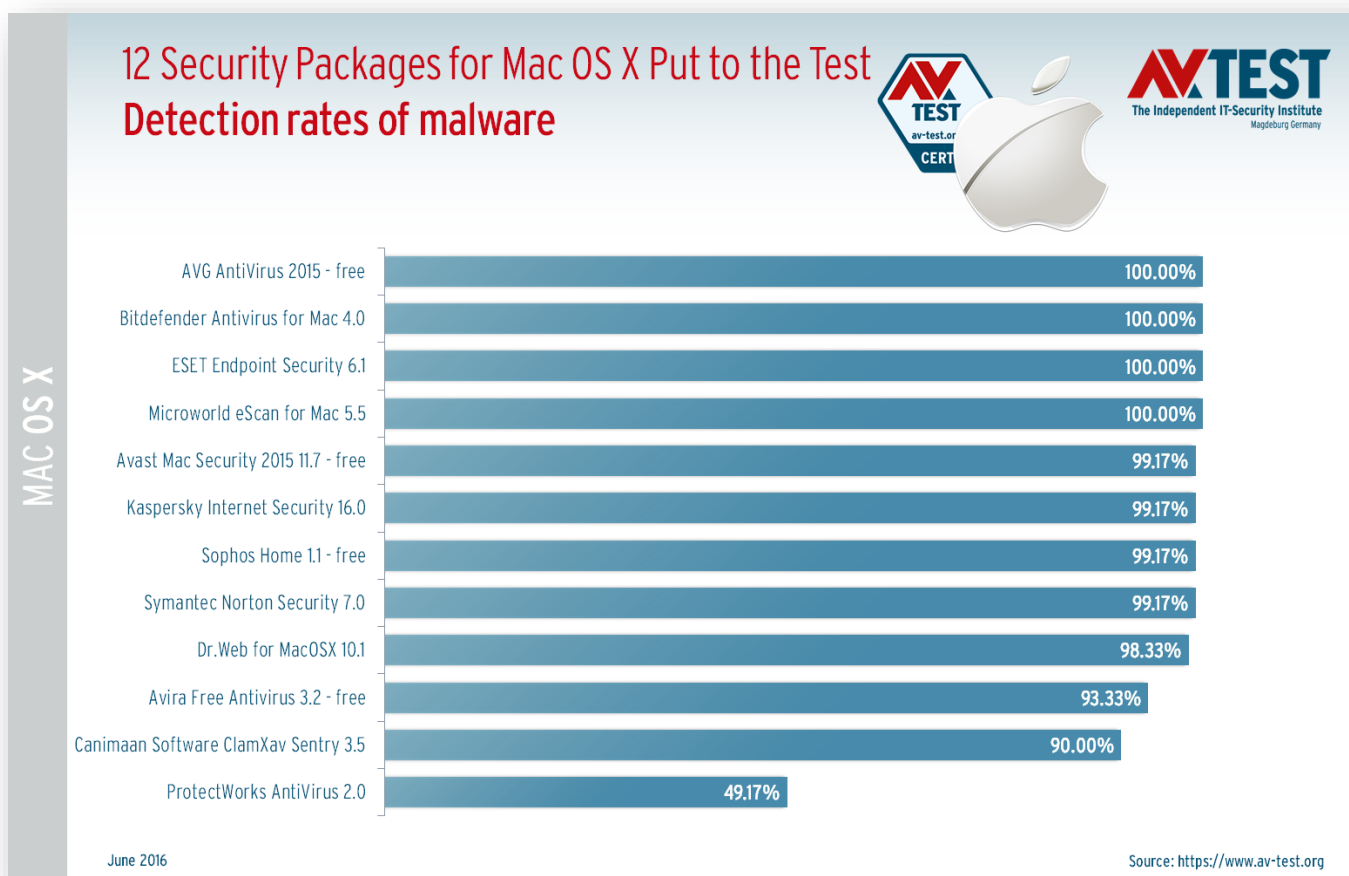
Eigenaren van een Mac die een gratis virusscanner zoeken kunnen het best voor de oplossing van AVG kiezen, zo adviseert het Duitse testlab AV-Test dat 12 virusscanners en security suites voor consumenten testte.

AVG beste gratis virusscanner voor Mac OS X

Dat malware voor Mac nog altijd weinig voorkomt blijkt wel uit de test set. Waar erbij tests voor Windows met duizenden en zelfs tienduizenden malware-exemplaren wordt gewerkt, werden voor de test met Mac-malware slechts 120 exemplaren gebruikt. Slechts 4 van de 12 virusscanners wisten alle malware-exemplaren te detecteren. Het gaat om AVG, Bitdefender, ESET en Microworld. Van de vier is alleen de oplossing van AVG gratis.

Als het om de systeembelasting gaat doen de vier gratis oplossingen die AV-Test testte het minder goed. Bij het downloaden en kopiëren van bestanden zorgt AVG voor een vertraging van 22 seconden. De gratis oplossingen van Avast, Avira en Sophos doen het nog slechter, waarbij Avast het systeem met 220 seconden vertraagt. Bitdefender is de snelste virusscanner en zorgt ervoor dat het downloaden en kopiëren slechts 3 seconden langer duurt.

Verder sloegen de virusscanners geen enkele keer vals alarm bij het gebruik van schone bestanden, ook bekend als false positives. Wie naar een gratis oplossing zoekt krijgt dan ook het advies om voor AVG te gaan, dat 100% detectie met een systeembelasting van zo'n 10% combineert, aldus AV-Test. De beste prestaties worden echter door de betaalde oplossing van Bitdefender neergezet.



Snapshots

Secure Computing

650 Nederlanders hebben vorig jaar hun pinpas naar criminelen gestuurd, waarmee vervolgens 1,8 miljoen euro werd gestolen. Dat blijkt uit cijfers van het jaarverslag van de Betaalvereniging Nederland. Het gaat om de 'pas-opstuurfraude', waarbij criminelen phishingmails versturen.

In de phishingmails wordt de ontvanger verteld dat hij een andere betaalpas krijgt en zijn oude pas moet opsturen. Tijdens het proces wordt op een aparte phishingpagina naar de pincode van het slachtoffer gevraagd. Met de fysieke pinpas en de ingevoerde pincode kan er geld worden opgenomen en luxe goederen worden betaald. Vorig jaar besloten 650 Nederlanders hun pinpas op te sturen waarmee voor 1,8 miljoen euro werd gefraudeerd.

Als onderdeel van verschillende anti-terreurmaatregelen gaat Duitsland de verkoop van anonieme prepaid simkaarten verbieden. Het land volgt daarmee België, dat eerder besloot om de maatregel door te voeren. De Duitse Bondsdag ging vrijdag akkoord met nieuwe anti-terreurmaatregelen, zo meldt het Duitse Heise.

Daardoor moeten mensen die een prepaid simkaart willen kopen zich vanaf volgend jaar juli legitimeren. Volgens het Duitse ministerie van Binnenlandse Zaken maken criminelen en terroristen voor hun communicatie vaak gebruik van anonieme prepaid simkaarten en vormen ze daardoor een groot beveiligingsrisico. De nieuwe maatregel moet dit tegengaan.

Een speciale internet-eenheid van Europol die een jaar geleden werd opgericht om online terroristische propaganda te bestrijden heeft sindsdien duizenden berichten van social media, websites en andere platformen laten verwijderen. In een jaar tijd rapporteerde de Internet Referral Unit van Europol 11.000 berichten aan 31 verschillende platformen. In een grafische weergave van de gegevens wordt echter over 70 verschillende platformen gesp-

roken. In 91% van de meldingen werd de content door de betreffende social media- of internetprovider ook daadwerkelijk verwijderd. Daarnaast heeft de Internet Referral Unit het monitoren van open bronnen en internet verder uitgebreid om de activiteiten van mensensmokkelaars tegen te gaan. Het gaat dan bijvoorbeeld om het laten verwijderen van advertenties die smokkeldiensten aanbieden.

Wie World of Warcraft speelt, kan het doelwit zijn van social engineering-aanvallen, meldt internetbeveiligers GData. De oplichters bernaderen de spelers via de chat van de game en laten ze een specifiek commando uitvoeren waarmee ze een bepaald voorwerp kunnen verkrijgen. Uiteraard wordt er op de achtergrond een script uitgevoerd waarmee de aanvaller de computer van het slachtoffer kan overnemen. GData schrijft dat de scam voorkomen kan worden door geen scriptcode van vreemden in het eigen chatvenster uit te voeren.

De Telegraaf schrijft over de 'zeker vierhonderd Nederlanders' die de afgelopen drie jaar opgelicht werden op datingsites. Een van hen, diabetespatiënt Sander Cirk (41, uit Den Helder), vloog naar China en wachtte twee weken vergeefs op de luchthaven van Changsa op ene 'Alice' die hij twee maanden terug via een datingsite had leren kennen. Alice kwam echter nooit opdagen, Cirk – inmiddels wereldwijd trending topic – belandde zelfs met uitdrogingsverschijnselen in het ziekenhuis. Ook 'Heleen' (46) werd slachtoffer. Ze raakte dertigduizend euro kwijt aan een niet-bestaande man die ze op Badoo.com had ontmoet. 'Hij pushte zo dat ik geld moest overmaken, dat ik het uiteindelijk heb gedaan'. Marlon (56, uit Hilversum) werd ook al opgelicht, dit keer door iemand die zich voordeed als Amerikaans ingenieur. Marlon raakte al haar spaargeld kwijt, 50 mille, maar haar droomman zag ze nooit. 'Ze laten je verliefd worden en daardoor ben je erg kwetsbaar'. Internetliefde wordt vaak

duur betaald, stelt deFraudehelpdesk. Het hoogste bedrag aan datingfraude dat bij de helpdesk bekend is, is van een vrouw die, nog tijdens haar huwelijk, 150.000 euro overmaakte aan een 'Duitse ingenieur op een booreiland'. De afgelopen drie jaar meldden zich bij de Fraudehelpdesk 394 slachtoffers van datingfraude, het topje van de ijsberg. 'De grote meerderheid schaamt zich kapot en doet geen aangifte'.

Van alle door Twitter verwijderde accounts is 96% op Turks verzoek verwijderd. In totaal verwijderde op verzoek van de regering in Ankara 414 twitteraccounts. Daaronder zaten ook accounts van 'kritische' Turks-Nederlandse twitteraars, zo blijkt. Deze twitteraars ontvingen, in een mail van Twitter, het 'blokkadebesluit' van de rechtbank in Ankara. Daarin staat dat de tweets 'terreur verheerlijken' en de staatsveiligheid in gevaar brengen. Mehmet Cerit, hoofdredacteur van Zaman Vandaag, is een van de geblokkeerde twitteraars. Naar eigen zeggen is hij 'alleen maar kritisch' ten opzichte van Erdogan. Hij heeft Twitter om uitleg gevraagd. De Turkse regering liet verder 3000 tweets verwijderen; alle andere landen tezamen niet meer dan 350.

De onlinemarkt voor drugs wordt tegenwoordig geschat op 150 à 180 miljoen dollar. Dat is tien keer zo veel als in 2012, aldus een artikel in The Economist. En één op de tien gebruikers zou wel eens iets online hebben gekocht, meldt het Global Drug Survey. Kortom, een enorme markt. Maar wat kopen die gebruikers dan? Uit 1,5 Tb aan data – 360.000 bestellingen op de darknets Agora, Evolution en Silk Road 2, met een waarde van 50 miljoen dollar – concluderen onderzoekers dat mdma en marihuana het populairst zijn, gevolgd door cocaïne, speed en heroïne.

Cops in Cyberspace

Wie zich op de facebookpagina van het Korps Politie Suriname misdraagt, zal daarvan worden geweerd. De politie schrijft dat 'elke bezoeker die zijn mening uit, als voorbeeld voor anderen zal moeten dienen'. De laatste tijd werd de facebookpagina nogal eens bestookt met 'vulgaire en ongepaste' reacties op berichten en filmpjes. Deze reacties zullen worden verwijderd, de afzenders geblokkeerd.

In 2016 zijn er bij de politie al 15 meldingen geweest van grooming. Onduidelijk is hoeveel slachtoffers er zijn, wel duidelijk is dat de politie zich zorgen maakt. Volgens Hugo van Rosmalen van het Team Kinderporno Politie zijn er voor elk slachtoffer dat aangifte doet, 'nog tientallen andere slachtoffers'. Van Rosmalen roept mensen op om direct aangifte te doen zodra hun kinderen te maken krijgen met groomers. Dat gebeurt nu relatief weinig, mogelijk uit schaamte maar ook omdat veel kinderen 'simpelweg niet doorhebben' dat ze niet met een leeftijdsgenoot te maken hebben terwijl ze aan het chatten zijn. 'De volwassenen die de kinderen benaderen, gaan geraffineerd te werk', aldus Van Rosmalen. Kinderen zijn bovendien goedgeloviger dan volwassenen en trappen sneller in de val. 'Sommige van de meisjes worden zelfs verliefd op die mannen'. Kinderen moet daarom leren dat wat ze offline niet mogen, ook online niet mogen. 'Kinderen zijn altijd en overal online, en bijna elk apparaat heeft tegenwoordig een camera'.

Een man (52, uit Assen) heeft zestig uur werkstraf gekregen voor 'grievende opmerkingen' die hij plaatste onder de blog van een politieagent. De agent beschreef in het blog wat er gebeurde toen hij door een scooterrijder werd aangereden; terwijl hij kermend op de grond lag met een dubbele beenbreuk, stonden omstanders te klappen en te juichen. Op het blog kwamen veel steunbetuigingen; de verdachte schreef echter te hopen dat de agent nooit meer zou lopen. 'Het is een vieze smerige kanker nazi smeris die

mensen bedreigt en aanvalt. Dikke pluim voor diegene die hem heeft aangereden'.

In de tweede helft van 2015 zijn bij Google maar liefst 40 duizend dataverzoeken ingediend, meer dan ooit: het zijn er tienduizend meer dan in de tweede helft van 2014 en vierduizend meer dan in de eerste helft van 2015. In heel 2015 werden zo'n 76 duizend verzoeken gedaan, die betrekking hadden op ruim 81 duizend accounts. De VS zijn koploper (12.500 verzoeken, 79% gehonoreerd). Nederland diende 210 verzoeken in, over 216 Google-account; 69% werd ingewilligd.

De politie heeft, in de strijd tegen internetpesten, de hulp ingeroepen van YouTube-ster Joy (13). Joy is het gezicht van BeautyNezz, een kanaal met 380.000 abonnees. Ze gaat in een filmpje vertellen hoe ze omgaat met 'best nare reacties' en uitleggen hoe naar het is om iemand online te pesten. Joy's filmpjes zijn populair en worden soms meer dan een miljoen keer bekeken.

Nog meer politiefrustratie op facebook: de politie Haarlem beschrijft in detail hoe een arrestant zijn politiecel besmeurde met eten én zijn eigen uitwerpselen. Bij een foto van een met poep besmeurde deur, schrijft de politie 'ook dit helaas mee te maken'. Inclusief hashtags als #ookpolitiewerk en #schijteraan. Het voorval betrof een man die was aangehouden en door een arts was onderzocht. De man was het echter niet eens met de door de arts voorgeschreven medicatie. De cel is, nadat de man weer vertrokken was, door een schoonmaakbedrijf gereinigd. 'De kosten zullen op [de man] worden verhaald', aldus het facebookbericht.

De politie Amsterdam uit op facebook haar ongeloof over het gedrag van omstanders bij een incident op de Groenburgwal. Daar zat een verward meisje, rillend van de kou, op de grond. Niemand hielp het meisje, ze waren allemaal te

druk met filmen. 'Omstanders vonden dit wel grappig om op youtube te plaatsen. Toch was er gelukkig een omstander die dit niet normaal vond en hier wél een melding van heeft gemaakt'. Het meisje bleek te zijn weggelopen uit een psychiatrische instelling en zou zeker een uur langs de gracht hebben gelegen. Ze is overgedragen aan de crisisdienst. De reacties op het facebookbericht van de politie laten zich raden. Waar de een 'schande' roept, zich afvraagt hoe de wereld zo lomp, onpersoonlijk en asociaal geworden is en dat de filmers allemaal 'lafbekken' zijn, zegt de ander nuchter 'welkom in 2016'. Tja. Filmen is gewoon de tijdgeest, zegt Jan van Dijk, hoogleraar nieuwe media in Twente, in Het Parool. 'We zijn steeds meer toeschouwer in plaats van onderdeel van een gebeurtenis. Het beeld is soms belangrijker dan de werkelijkheid die wordt gefilmd'. Neurowetenschapper Ruud Hortensius wijst op het omstandereffect, waarbij de kans op ingrijpen of helpen kleiner wordt naarmate de groep groter is. Mensen maken volgens hem op zulke momenten geen bewuste keuze. Filmen zou wel eens een automatisme kunnen zijn, 'zoals je je telefoon pakt tijdens een verjaardag'. Van Dijk denkt dat filmen ook gebeurt om later te kunnen zeggen dat je er als eerste bij was. De experts wijzen ook op de kansen die filmers bieden: het beeld kan als bewijs dienen, tijdens een misdrijf zelfs afschrikkend werken, en ook voor brandweer en ambulance een heel goed hulpmiddel zijn.



Tek Tok Late Night:

1. [Privacy](#)
2. [Internetvrijheid](#)
3. [Digitale veiligheid](#)
4. [High Tech Crime](#)
5. [Data in onderwijs](#)
6. [Cybersurveillance](#)
7. [Techtrends in onderwijs](#)
8. [Veilig internetten](#)
9. [MKB cyber secure](#)
10. [Cyberellende bij Tek Tok](#)
11. [Standaarden en keurmerken](#)
12. [Operation Higg Tech Crime](#)
13. [Kraak van de Maand](#)

[Doe jij het veilig online](#)

[Malware](#)

[WiFi ontvangst verbeteren](#)

[Internetfraude via de telefoon](#)

[Documentaire: Veiligheid en privacy](#)

[Herken een nep-hotspot](#)

[Gebruik wachtzinnen](#)

[Drive-by-downloads voorkomen](#)

[Hoe herken je een phishing mail](#)

[Beveiligd internetbankieren](#)

[Privacy—ik heb toch niets te verbergen](#)

[Webinar Computercriminaliteit](#)

[Mousejack](#)

[Gegijzeld door Ransomware. Wat nu?](#)

[Telefonische phishing](#)

Nieuw:

[Grooming](#)

[Sexting](#)

[Webcammisbruik](#)

[Bedreigd/gechanteerd](#)

[Kinderporno](#)

[Nepprofiel](#)

Cybercrime wetsartikelen

Secure Computing

[Art. 138ab, lid 1 Sr](#) Hacken: opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk

[Art. 138ab, lid 2 Sr](#) Hacken: overnemen, aftappen of opnemen van gegevens uit een geautomatiseerd werk na binnendringen daarvan

[Art. 138ab, lid 3 Sr](#) Hacken door tussenkomst van een openbaar telecommunicatienetwerk

[Art. 138b Sr](#) Het belemmeren van toegang tot of gebruik van een geautomatiseerd werk

[Art. 139c Sr](#) Het aftappen of opnemen van gegevens (afluisteren)

[Art. 139d, lid 1 Sr](#) Plaatsen van opname-, aftap- of af luisterapparatuur; voorbereidingshandelingen

[Art. 139d, lid 2 Sr](#) Het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen of toegangscode bedoeld om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen

[Art. 139d, lid 3 Sr](#) Zoals in art. 139d, lid 2 Sr, maar met oogmerk gericht op art. 138ab, lid 2 en 3 Sr

[Art. 139e Sr](#) Het bezit en verspreiden van gegevens of een voorwerp waarop gegevens staan die door wederrechtelijk aftappen of opnemen zijn verkregen

[Art. 161sexies Sr](#) Opzettelijk vernielen etc. van een geautomatiseerd werk of werk voor telecommunicatie; voorbereidingshandelingen

[Art. 161septies Sr](#) Vernieling etc. van een geautomatiseerd werk of werk voor telecommunicatie door schuld

[Art. 231b Sr](#) Identiteitsfraude

[Art. 232 Sr](#) Opzettelijk valselyk opmaken, vervalsen, gebruiken, etc. van betaalpas, waardekaart e.d.

[Art. 240b Sr](#) Kinderpornografie

[Art. 248e Sr](#) Grooming

[Art. 273, lid 2 Sr](#) Bekendmaking bedrijfsgeheimen; heling computergegevens ondernemingen

[Art. 273d Sr](#) Schending telecommunicatiegeheim

[Art. 317, lid 2 Sr](#) Afpersing door de bedreiging dat gegevens opgeslagen door een geautomatiseerd werk onbruikbaar, ontoegankelijk of gewist worden

[Art. 326c Sr](#) Het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen

[Art. 350a, lid 1 Sr](#) Opzettelijke vernieling van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

[Art. 350a, lid 2 Sr](#) Het feit gepleegd in lid 1 met tussenkomst van een openbaar telecommunicatienetwerk

[Art. 350a, lid 3 Sr](#) Opzettelijk gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

[Art. 350b, lid 1 Sr](#) Vernieling door schuld van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

[Art. 350b, lid 2 Sr](#) Door schuld gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Overzichtstabel cybercrime

Verschijningsvorm cybercrime	138ab lid 1	138ab lid 2	138ab lid 3	138b	139c lid 1	139d	139e	161 sexies	161 septies	350a lid 1	350a lid 2	350a lid 3	350b lid 1	350b lid 2
• Malware														
Malware maken en/of verspreiden	X					X		X	X	X	X	X	X	X
Malware (Trojaanse paarden) gebruiken	X	X			X			X	X	X	X	X	X	
• Computerinbraak														
Computerinbraak (hacking)	X		X								X			
Computerinbraak vervolghandelingen		X	X		X	X	X	X	X	X	X	X		
Portscan						X								
Spoofing/cache poisoning	X	X		X	X	X	X	X		X	X			
Sniffing					X	X	X			X				
Draadloze netwerken hacken/misbruiken	X	X	X	X	X		X	X		X	X			
Password guessing	X			X		X								
• Website aanvallen														
Veroorzaken open relay									X				X	
Wederrechtelijk open relay gebruiken	X							X		X				
Defacing/vernielen website	X							X	X	X			X	
Defacing/doorleiden internet-verkeer	X							X	X	X				
Cross-site scripting	X	X			X	X	X	X		X			X	
SQL-injecties	X	X						X		X				
• Botnets														
Botnet bouwen en beheren	X	X	X		X					X		X		
• Denial of Service														
DDoS-aanval				X				X		X			X	
• Social Engineering														
Phishing		X			X		X							
Vishing/Smishing		X			X									
• E-mail gerelateerd														
Wederrechtelijk open mail relay gebruiken	X							X	X	X				
Spamming (met DoS tot gevolg)				X				X	X				X	

Handig

Phishing- / valse e-mails melden

ABN AMRO Bank: valse-email@nl.abnamro.com
 ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

ICS- / ABN AMRO creditcards: valse-email@icscards.nl

Actuele phishingmails:

[klik hier](#)

Voor vragen over veilig internetbankieren bij uw eigen bank, kunt u op een van de onderstaande websites terecht.

Websites banken

ABN AMRO	LeasePlan Bank
Argenta	Rabobank
Credit Europe Bank	SNS Bank
Delta Lloyd Bank	Staal Bankiers
DHB Bank	Triodos Bank
Friesland Bank	Van Lanschot Bank
ING Bank	ASN Bank



Controleer vooraf de (bank)gegevens van de verkoper op www.mijnpolitie.nl/miocheck

MARKTPLAATS: veilig handelen



Computerwoordenboek

OneDrive extra's

Naslag:

- Handleiding Twitter
- Gebruik tweetraps authenticatie
- Windows 10 installatie
- Online verdwijnen
- Centraal cloudbbeheer
- Online kopen
- Cybersecurity 2015
- Stickware
- Netwerk in de knoop
- Slachtofferschap
cybercrime en
internetgebruik

Muziek: DoubleYouAB

- Return to TubularBells
- FeddeLeGrand remix
- Faithless Insomnia remix
- ReeAnna2015
- 1.11 Armin
- SummerHardstyle2015
- Summermix2015
- TrancePhonic 2015
- Open Your Eyes 2015 rmx
- MikeOldfieldReborn
- MashedUp2011
- Heilig rmmstnmix

OneDrive