Secure Computing

Maart 2016 JAARGANG 5

Veel lees(r)plezier

(NB: met Ctrl+ scrolwieltje 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

Secure Computing

Snel index

Klik op een link voor snelle toegang tot het artikel.

Om terug te keren naar de snel index klikt u onderaan de pagina op Index

Bronnen oa:

Security.nl, PCMweb, ZDnet, Webwereld, Comptable, Bits of Freedom, Cops in Cyberspace, De Digitale Revolutie, PCwereld, PCpro, Clikx, Peppermunt.net, PrivacyNieuws, HackInfo, HardwareInfo, Bright, Computerworld. Tweede Kamer

De Wet computercriminaliteit III moet de opvolger worden van twee voorgaande wetten, met de voor de hand liggende namen ‘Wet computercriminaliteit’ en ‘Wet computercriminaliteit II’.

Wet computercriminaliteit III - Schipperen tussen veiligheid en privacy

De eerste wet in deze reeks is geïntroduceerd in 1993 en voegde een aantal nieuwe bepalingen toe aan onder andere het Wetboek van Strafvordering en het Wetboek van Strafrecht. De noodzaak voor de wet kwam toen voort uit ‘de voortschrijdende toepassing van informatietechniek’. De steeds groter wordende rol van de computer zou vragen om passende en effectieve regelgeving. Om dit te bereiken werden enkele nieuwe bevoegdheden en definities ingevoerd, waaronder de strafbaarstelling van ‘computervredebreuk’.

De Wet computercriminaliteit II volgde in 2006 na een lange parlementaire behandeling. Er lag al een voorstel voor een nieuwe wet in 1999, maar onder andere Europese ontwikkelingen maakten het noodzakelijk om dit voorstel ingrijpend te herzien. Een van deze ontwikkelingen was het Cybercrime-verdrag, dat in 2001 door Nederland werd ondertekend. De Memorie van Toelichting spreekt over ‘informatietechnieken die zich op stormachtige wijze verder ontwikkelen’ als het gaat om de noodzaak van de nieuwe wetgeving. In het bijzonder zouden ‘nieuwe technologieën die het mogelijk maken om computers aan elkaar te koppelen’ opnieuw om vernieuwde regels vragen.

Deze wet voerde enkele nieuwe bepalingen in, bijvoorbeeld over denial of service-aanvallen. Daarnaast werd het strafbaar om opzettelijk en wederrechtelijk een computersysteem binnen te dringen, zelfs als daarbij geen enkele beveiliging wordt doorbroken. Daardoor vond een verbreding plaats van de definitie van het begrip ‘computervredebreuk’. Onder de huidige wetgeving zijn ook het aftappen, opnemen, bekendmaken en misbruiken van computergegevens strafbaar.

Doel van deze achtergrond is een overzicht te bieden van de belangrijkste wijzigingen die het Wetsvoorstel computercriminaliteit III met zich meebrengt. De nadruk ligt op zowel de bestaande als de nieuwe bevoegdheden en het artikel is daarmee geen uitputtende behandeling van het wetsvoorstel, dat op 22 december 2015 bij de Tweede Kamer is ingediend.

Geautomatiseerd werk

Centraal in de discussie staat het begrip ‘geautomatiseerd werk'. Zeer kort door de bocht worden hiermee apparaten bedoeld die op een netwerk zijn aangesloten, waaronder computers, smartphones en routers. Zoals we zullen zien is de precieze betekenis van het begrip al enkele keren gewijzigd, maar de definitie volgens de huidige wetgeving is te vinden in 'Artikel 80sexies' van het Wetboek van Strafrecht:

"*Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen*."

Dit is nogal breed geformuleerd, om het zacht uit te drukken, en de Memorie van Toelichting is al niet veel specifieker. Daarin staat dat het gaat om ‘computers, netwerken van aan elkaar verbonden computers en geautomatiseerde inrichtingen voor telecommunicatie’. Om de reikwijdte van het begrip toch wat in te perken wordt daar echter bij vermeld dat systemen die uitsluitend bestemd zijn voor de opslag van gegevens of om te functioneren zonder interactie met hun omgeving er niet onder vallen. Een elektronisch klokje valt er dus niet onder, zo staat in de toelichting.

In de conceptversie van de Wet computercriminaliteit III die bij de internetconsultatie werd aangeboden, was deze definitie haast onveranderd. Het recentste voorstel, dat nu bij de Tweede Kamer ligt, bevat echter een heel andere definitie:

"*Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er een of meer op basis van een programma automatisch computergegevens verwerken*."

Dit is een kopie van een deel de definitie van de term ‘informatiesysteem’ uit de Europese richtlijn over aanvallen op informatiesystemen uit 2013. In de Memorie van Toelichting bij het wetsvoorstel wordt gesteld dat de definitie daarmee wordt verruimd. Een usb-stick bijvoorbeeld zou niet onder de definitie vallen, totdat hij wordt aangesloten op een apparaat dat op basis van een programma automatisch computergegevens verwerkt, bijvoorbeeld een computer. Daarnaast roept de term ‘samenhangend’ enige vragen op, omdat niet duidelijk is in hoeverre dat verschilt van ‘verbonden’.

Bestaande bevoegdheden

De bevoegdheden van opsporingsambtenaren zijn op dit moment gebaseerd op de eerdergenoemde wetten computercriminaliteit I en II. Om de nieuwe bevoegdheden uit het wetsvoorstel te kunnen beoordelen, is het nuttig om de huidige bevoegdheden in kaart te brengen. Hieronder vind je een greep uit de belangrijkste. Deze zijn te vinden vanaf art. 125i Sv.

Onder andere een opsporingsambtenaar mag bij doorzoeking van een plaats ook onderzoek verrichten op computers die via een netwerk met elkaar in verbinding staan. Daar valt bijvoorbeeld een externe harde schijf onder als deze via het netwerk toegankelijk is. Bij deze ‘netwerkzoeking’ mogen vervolgens gegevens vastgelegd worden. Destijds werd deze bevoegdheid 'de meest vergaande bevoegdheid tot onderzoek in geautomatiseerde werken’ genoemd. Ze mag dan ook alleen worden ingezet als dat noodzakelijk is en het vermoeden bestaat dat er relevante gegevens gevonden kunnen worden. Deze opsporingsbevoegdheid strekt zich overigens niet uit tot computers die zich in het buitenland bevinden, want dat zou in strijd zijn met het internationale recht.

Bron: Tweakers / Sander van Voorst

Als er versleutelde gegevens worden aangetroffen, kan een decryptiebevel worden afgegeven om de gegevens te ontsleutelen. Dit bevel mag echter niet aan de verdachte worden gericht. Ook kan een Officier van Justitie bepalen dat gegevens die tijdens een doorzoeking worden aangetroffen ontoegankelijk worden gemaakt voor zover dat nodig is voor het beëindigen van strafbare feiten en om nieuwe inbreuken te voorkomen.

Daarnaast mag een opsporingsambtenaar bij de verdenking van een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert ook communicatie aftappen. Dit moet bij voorkeur gebeuren met medewerking van de aanbieder van het netwerk of de dienst, maar dat is geen vereiste. Ook hierbij is het mogelijk om een decryptiebevel af te geven. In de Telecommunicatiewet is bovendien geregeld dat aanbieders van netwerken en diensten verplicht zijn mee te werken aan een afluisterbevel, en dat zij hun netwerken en diensten alleen aan gebruikers mogen aanbieden als deze aftapbaar zijn.

Een andere bevoegdheid is het vorderen van gegevens. Hiermee kan een opsporingsambtenaar verkeersgegevens van een gebruiker opvragen bij een aanbieder. Een andere term voor 'verkeersgegevens' is 'metadata'. In Nederland is de Wet bewaarplicht telecommunicatiegegevens op 11 maart 2015 buiten werking gesteld, dus is het maar de vraag of een aanbieder op dit moment aan een dergelijk verzoek kan voldoen.

Het wetsvoorstel

Het huidige wetsvoorstel werd op 2 mei 2013 gepubliceerd. Er is ook een internetconsultatie gehouden, die sloot op 1 juli 2013. Het voorstel introduceert regelgeving die opsporingsambtenaren, waaronder de politie, van nieuwe bevoegdheden moet voorzien.

'Hackbevoegdheid'

Zo wordt de bevoegdheid gecreëerd om op afstand heimelijk binnen te dringen in geautomatiseerde werken, ook wel ‘hackbevoegdheid’ genoemd. Deze is te vinden in art. 126nba van het wetsvoorstel. Deze bevoegdheid kan worden verleend aan een ambtenaar van politie of marechaussee. Daarnaast kan een ambtenaar van een bijzondere opsporingsdienst ervan gebruikmaken. Hieronder vallen bijvoorbeeld de Belastingdienst en de Sociale Inlichtingen- en Opsporingsdienst. De bevoegdheid is dus niet beperkt tot gebruik door de politie.

Vereist is dat het geautomatiseerde werk in gebruik is bij de verdachte. Gegevens van de verdachte die op een server van een derde zijn opgeslagen mogen dus niet zomaar benaderd worden. Om die server binnen te dringen zou dan een apart bevel nodig zijn. Wel is het mogelijk om van het ene geautomatiseerde werk ‘door te stappen’ naar een ander geautomatiseerd werk, zolang dat maar is omschreven in het oorspronkelijke bevel.

De opsporingsambtenaar mag vervolgens gegevens vastleggen voor zover dat nodig is voor het onderzoek. Hieronder valt het kopiëren van gegevens. De ambtenaar mag in tegenstelling tot de huidige situatie ook servers benaderen die zich in het buitenland bevinden. Als duidelijk is dat de server zich in een ander land bevindt, moet daarvoor wel eerst een rechtshulpverzoek aan dat land worden gedaan, maar onder de juiste, nog op te stellen voorwaarden moeten opsporingsambtenaren zelfstandig kunnen optreden.

Concreet biedt de Memorie van Toelichting enkele voorbeelden van de inzet van deze bevoegdheid, waaronder:

"1. De verdachte maakt veelvuldig gebruik van cryptocontainers of complete versleuteling van de harde schijf. Nadat in het geautomatiseerde werk is binnengedrongen kan het wachtwoord worden afgevangen zodat bij latere vastlegging van de gegevens de cryptocontainer kan worden geopend."

"2. Het binnendringen van een computer waarvan alleen het Tor-adres bekend is, om het IP-adres vast te stellen teneinde een bevel tot het aftappen en opnemen van communicatie aan de aanbieder te kunnen afgeven."

Om deze handelingen te kunnen uitvoeren kan er gebruikgemaakt worden van spyware. Zo kan een keylogger worden ingezet om het wachtwoord als in het eerste voorbeeld af te vangen.

Ontoegankelijk maken

De tweede nieuwe bevoegdheid betreft een aanpassing van de bestaande bevoegdheid tot het ontoegankelijk maken van gegevens, zodat het ook mogelijk wordt om aanbieders van communicatiediensten te bevelen om bepaalde gegevens ontoegankelijk te maken. Normaal gesproken kan dit ook via een notice and takedown-procedure. De bevoegdheid om het bevel af te geven wordt dan ook alleen ingezet als er onenigheid met de aanbieder bestaat.

Waarborgen

Voordat de hackbevoegdheid kan worden ingezet moet er een schriftelijk bevel worden uitgevaardigd. Dit kan worden gedaan door een officier van justitie. Vervolgens wordt dit bevel getoetst door een rechter-commissaris.

De hackbevoegdheid mag ingezet worden bij misdrijven met een gevangenisstraf van vier jaar of meer. Als er bij het heimelijk binnendringen gegevens veiliggesteld worden of ontoegankelijk worden gemaakt, moet het gaan om een misdrijf waar minimaal acht jaar gevangenisstraf op staat. De gevolgen voor de persoonlijke levenssfeer van de verdachte zijn immers groter bij het toepassen van deze bevoegdheid. In beide gevallen moet het gaan om een misdrijf dat een ernstige inbreuk maakt op de rechtsorde.

Het is ook mogelijk de bevoegdheid in te zetten bij misdrijven waarvoor 'geen gevangenisstraf van acht jaar of meer is gesteld, maar die worden gepleegd met behulp van een geautomatiseerd werk en waarbij er een duidelijk maatschappelijk belang is bij de beëindiging van de strafbare situatie en de vervolging van de daders'. Dat is het geval bij onder andere het aanbieden van kinderpornografie, het verleiden van minderjarigen tot ontucht en 'andere ernstige delicten waarbij het gebruik van een geautomatiseerd werk instrumenteel is en de inzet van deze bevoegdheid op basis van een afweging van belangen en met inachtneming van de proportionaliteit en subsidiariteit aangewezen is'.

Het voornemen om de bevoegdheid tot onderzoek in een computer of netwerk in te zetten moet ook worden voorgelegd aan de Centrale Toetsingscommissie van het Openbaar Ministerie.

Nemo tenetur

In de conceptversie van het voorstel was sprake van een regeling die het mogelijk zou maken een decryptiebevel af te geven aan de verdachte. Deze heeft de definitieve versie van het wetsvoorstel echter niet gehaald. Dit heeft te maken met het 'nemo tenetur'-beginsel, waaruit voortvloeit dat een verdachte niet kan worden geacht mee te werken aan zijn eigen veroordeling. Het afgeven van een decryptiebevel aan de verdachte zou rechtstreeks ingaan tegen dit beginsel en daarmee in strijd zijn met de rechtsbeginselen. Ook de Raad van State liet in een advies weten dat het voorgestelde bevel niet door de beugel kan.

De nieuwe bevoegdheden zijn nodig om de anonimiteit van daders op te heffen. Dat zou met de huidige bevoegdheden niet mogelijk zijn en het zou daarom voor daders op dit moment te eenvoudig zijn om zich op internet te verschuilen. Hij voegt daaraan toe dat bij delicten met een geringe pakkans, zoals internetcriminaliteit, blijkt dat deze een grote groei doormaken. Wel zou het door het wetsvoorstel voor de politie aantrekkelijker kunnen worden om de bevoegdheden voor andere delicten dan internetcriminaliteit in te zetten.

De nieuwe wet wordt verder noodzakelijk gevonden vanwege ‘de ontwikkelingen op het gebied van de informatie- en communicatietechnologie’. Drie ontwikkelingen spelen daarbij de hoofdrol: versleuteling van gegevens, het gebruik van draadloze netwerken en cloudcomputingdiensten.

Wat de versleuteling van gegevens betreft noemt de Memorie van Toelichting voorbeelden als schijfversleuteling door Truecrypt, en e-mailversleuteling door Google en Microsoft of met tools als pgp. Ook WhatsApp, Twitter, Skype en Tor worden genoemd als diensten die het lastig maken om communicatie te onderscheppen en af te tappen. De huidige bevoegdheden zouden niet voldoende zijn om versleutelde gegevens in te zien. Zo zou het vastleggen van gegevens en het afgeven van een decryptiebevel aan een derde vaak niets opleveren, omdat aanbieders van communicatiediensten zelf vaak geen mogelijkheid tot ontsleuteling hebben. Dit kan bijvoorbeeld te maken hebben met end-to-end-encryptie, waarbij communicatie al op de apparaten van gebruikers wordt versleuteld. Een aanbieder kan deze communicatie niet zomaar ontsleutelen.

Daarnaast zou het gebruik van draadloze netwerken het aftappen van informatie moeilijker maken. Een verdachte zou meer mogelijkheden hebben om een internetverbinding tot stand te brengen, bijvoorbeeld in een restaurant, op de camping of in de trein. Het zou niet wenselijk of mogelijk zijn om al die mogelijke toegangspunten af te tappen, maar door de computer of het netwerk van de verdachte binnen te dringen zou dat ook niet meer nodig zijn.

Ten slotte zouden particulieren en bedrijven steeds meer gebruikmaken van ‘cloudcomputingdiensten’. Als voorbeelden worden onder andere Dropbox, Google Docs en Megaupload genoemd. Het probleem dat bij deze diensten ontstaat, is dat bestaande bevoegdheden als de netwerkzoeking en het bevel om gegevens te verstrekken vaak niet toereikend zouden zijn. Dat heeft ermee te maken dat door gebruik van smartphones en laptops niet duidelijk is waar een gegevensdrager zich bevindt. Bovendien zou vaak niet vaststaan bij welke aanbieder gegevens zijn opgeslagen en zouden veel aanbieders in het buitenland zitten. Ook zou de wettelijke definitie van ‘aanbieder van een telecommunicatiedienst’ niet direct op alle aanbieders van toepassing zijn, bijvoorbeeld niet op ‘bulletproof hosting providers’. Het gevolg daarvan is dat er geen wettelijk bevel kan worden afgegeven.

Kritiek

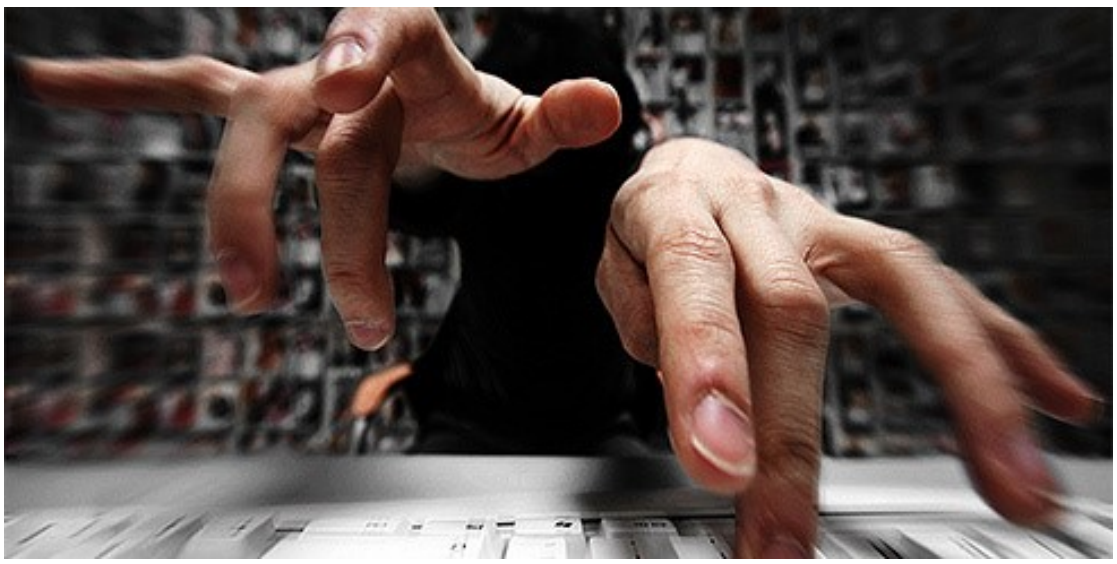
Vooral de voorgestelde hackbevoegdheid heeft heel wat stof doen opwaaien in Nederland. Ton Siedsma van de stichting voor digitale burgerrechten Bits of Freedom stelt tegenover Tweakers dat de wet in vergelijking met andere landen zeer ver gaat. Zo mag er in Frankrijk alleen worden meegekeken op het scherm van de verdachte en kunnen opsporingsdiensten bijvoorbeeld geen webcam aanzetten. Verder mogen in Duitsland alleen gegevens worden vastgelegd, en dat slechts onder strikte voorwaarden. Er moet namelijk sprake zijn van 'lichamelijk letsel, levensgevaar of gevaar voor de vrijheid van personen' of van 'algemeen gevaar voor goederen, dat een bedreiging oplevert voor het voortbestaan van de staat of de mensheid'. Ook zou de bevoegdheid in Nederland door slechte afbakening veel te breed kunnen worden ingezet, waardoor vrijheden van burgers in het geding komen.

Daarnaast baart het hem zorgen dat er in de Memorie van Toelichting staat dat de nieuwe hackbevoegdheid kan leiden tot besparingen, doordat de inzet van deze bevoegdheid andere vormen van politie-inzet kan vervangen. Over de waarborgen zegt hij dat de toetsing door de Centrale Toetsingscommissie met een korreltje zout moet worden genomen. Dit heeft ermee te maken dat deze commissie, anders dan bij de AIVD, onderdeel is van het Openbaar Ministerie en dus ook een opsporingsbelang heeft. Tot slot zou de reikwijdte van de wet niet zijn ingeperkt naar aanleiding van de kritiek die tijdens de internetconsultatie naar voren kwam en zou de noodzaak niet verder zijn onderbouwd. Deze mening wordt gedeeld door onder andere de Nederlandse Orde van Advocaten.

Ook het CBP, nu Autoriteit Persoonsgegevens geheten, was kritisch over het voorstel. Zo zou de nieuwe bevoegdheid 'ongekend omvangrijk' zijn en daarmee gevolgen kunnen hebben voor de privacy van veel burgers die niet als verdachte kunnen worden aangemerkt. In het advies van de privacywaakhond komt eveneens naar voren dat de onderbouwing van de noodzaak van de bevoegdheid gebrekkig is en dat er betere waarborgen nodig zijn.

Het vervolg

Het wetsvoorstel is op dit moment ingediend bij de Tweede Kamer, waar het in een commissie zal worden behandeld. De verschillende fracties kunnen dan schriftelijk commentaar leveren. Na deze schriftelijke voorbereiding wordt het voorstel tijdens het plenaire debat in de Tweede kamer mondeling besproken en kan de minister de inhoud ervan verdedigen. Tijdens dit proces is het mogelijk om wijzigingen aan te brengen. Als het voorstel vervolgens is aangenomen, gaat het naar de Eerste Kamer, waar eveneens een schriftelijke behandeling en een debat volgen. In deze fase kan het voorstel alleen nog aangenomen of verworpen worden; wijzigingen zijn dan niet meer mogelijk. Wordt het voorstel aangenomen, dan treedt het daarna in werking als wet.



Bron: Tweakers / Sander van Voorst

Cybercriminelen hebben zich vorig jaar meer gericht op het stelen van persoonsgegevens en identiteiten dan het jaar ervoor.

PERSOONSGEGEVENS
DAAR ZIJN WE ZUINIG OP

Criminelen richten zich meer op diefstal van persoonsgegevens

In totaal zijn er in 2015 707,5 miljoen gegevens gestolen. Er waren vorig jaar 1.673 gemelde inbraken op computersystemen. Dat blijkt uit de jaarlijkse rapport Breach Level Index, dat dinsdag is gepubliceerd door het Nederlandse veiligheidsbedrijf Gemalto.

Volgens de onderzoekers hebben de criminelen zich veel meer gericht op het stelen van persoonlijke informatie. Bij 53 procent van de inbraken waren criminelen op zoek naar persoonsgegevens. In 2013 en 2014 werden vooral financiële gegevens en creditcardinformatie gestolen. 2014 was daarnaast een recordjaar met meer dan een miljard gestolen gegevens bij grote en kleine inbraken. In 2015 werden in theorie elke seconde 22 computerbestanden gestolen. Dat is in totaal 39 procent minder dan het jaar ervoor, maar er zijn wel veel meer persoonsgegevens buitgemaakt.

Grote inbraken

Vorig jaar zijn er 46 grote inbraken geweest waarbij meer dan een miljoen gegevens werden gestolen. Van 47 procent van alle inbraken is onduidelijk hoeveel informatie de criminelen hebben buitgemaakt.

De meeste schadelijke inbraak had plaats bij de Amerikaanse verzekeraar Anthem. Daar zijn 78,8 miljoen klantgegevens gestolen.

Op de tweede plek staat een hack bij de Turkse overheid, waarbij 50 miljoen identiteitsgegevens werden gestolen. Een Koreaans farmaceutisch bedrijf behaalde een derde plek met 43 miljoen gestolen persoonsgegevens.

Andere noemenswaardige hacks zijn die op de Amerikaanse overheidstak voor personeelsgegevens (22 miljoen gestolen persoonsgegevens) en het Amerikaanse Experian, waar 15 miljoen gegevens werden gestolen.

Versleuteling

In slechts 4 procent van alle inbraken werd er versleutelde informatie gestolen. Dat is zorgwekkend, stelt het veiligheidsbedrijf, omdat versleuteling juist dient als extra beveiliging.

De meeste informatie, 43 procent van alle gestolen gegevens, werd gestolen bij overheden. De gezondheidssector heeft het meest te maken gehad met inbraken, namelijk 22 procent van het totaal.

Van de 1.673 gemelde inbraken werden er 964 door cybercriminelen gepleegd. In slechts 33 gevallen was de inbraak door een overheid gesteund of uitgevoerd. Bij die inbraken is wel veel informatie buitgemaakt, namelijk 107,7 miljoen gegevens.

Bron: Nu.nl/Tech

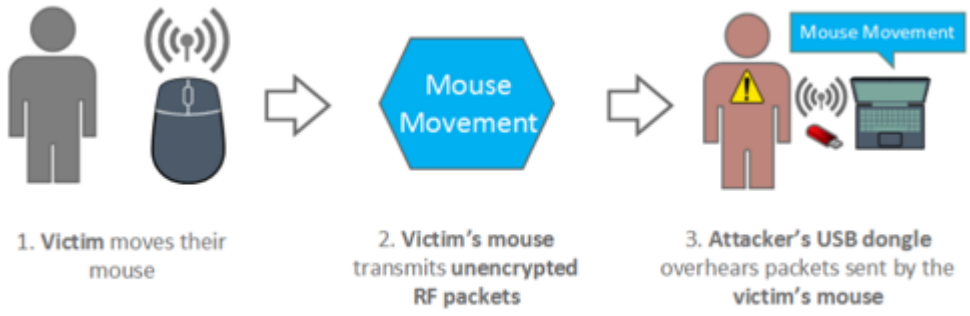
Onderzoekers hebben een kwetsbaarheid in draadloze muizen en toetsenborden ontdekt waardoor de apparaten tot een afstand van 100 meter zijn te hacken en kunnen worden gebruikt om computers met malware te infecteren of als springplank voor verdere aanvallen te gebruiken.

Draadloze muis op afstand van 100 meter te hacken

Het probleem is aanwezig in de draadloze usb-dongels die de toetsenborden en muizen gebruiken om via radiofrequenties met de computer te communiceren. De meeste communicatie tussen de toetsenborden en dongels is versleuteld, maar bij de muizen wordt helemaal geen encryptie voor de draadloze communicatie toegepast. Een aanvaller die binnen 100 meters van de usb-dongel aanwezig is kan de radiosignalen tussen de muis en de computer onderscheppen. Vervolgens kan de aanvaller het signaal door een eigen signaal vervangen en zo kwaadaardige pakketten versturen. Deze pakketten doen zich voor als toetsaanslagen, in plaats van muisklikken.

Onderzoeker Marc Newlin van beveiligingsbedrijf Bastille vertelt tegenover Threatpost dat het mogelijk is om op deze manier in 10 seconden een rootkit te installeren. Voor het uitvoeren van de aanval volstaat een usb-dongel van 15 dollar en 15 regels Pythoncode. De aanval is zowel tegen Linux, Mac als Windows te gebruiken. "Alle computers vertrouwen hun toetsenborden, omdat mensen toetsenborden gebruiken. Het overnemen van het toetsenbord is dus eigenlijk de ultieme hack", zegt Chris Rouland, oprichter van Bastille. De problemen zijn aanwezig in de muizen van zeven bedrijven, namelijk Microsoft, HP, Gigabyte, Amazon, Logitech, Dell en Lenovo.

MouseJack (video), zoals de aanval door Bastille wordt genoemd, vereist wel dat een aanvaller in de buurt van zijn slachtoffer is en op het scherm kan meekijken. Volgens beveiligingsexperts is het risico van een succesvolle aanval dan ook klein. Logitech heeft inmiddels een firmware-update uitgebracht. "Meer dan de helft van de muizen kunnen niet worden geüpdatet en zullen dus geen patch ontvangen. En zullen waarschijnlijk ook niet worden vervangen. Zodoende zullen er overal kwetsbare apparaten zijn", merkt Rouland op.



Attacker Identifying a Victim's Mouse or Keyboard

If necessary, the attacker now force-pairs a fake keyboard with the victim's dongle.

Attacker Force-Pairing a Fake Keyboard with the Victim's Dongle

Fraudehelpdesk en grote Nederlandse providers hebben een belangrijke tip voor iedere mobiele-telefoongebruiker: neem telefoontjes van een vreemd buitenlands nummer niet op en bel vooral niet terug.

Wangiri fraude

ワン切り
wan-gi-ri

De laatste maanden zijn zogenoemde wangiri-fraudeurs actiever geworden in Nederland. In januari en februari van dit jaar kreeg de Fraudehelpdesk al meer meldingen binnen over deze soort fraude dan over heel 2015. Het gaat om telefoonnummers uit verre landen, zoals Afghanistan en Madagaskar. Als je opneemt of terugbelt, moet je flink wat geld neertellen.

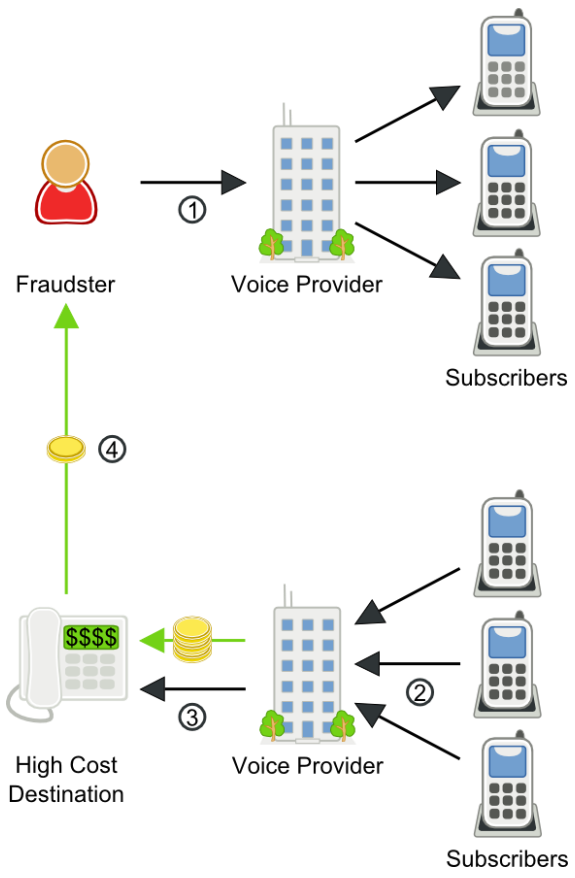
De nummers die rondgaan zijn buitenlandse servicenummers, vergelijkbaar met de 0900-nummers die wij in Nederland kennen. Iemand heeft die geregistreerd en bepaalt zelf wat het tarief is. Dat kan in het buitenland soms veel hoger zijn dan in Nederland. Op die manier verdienen fraudeurs dus aan hun belletjes. Met programma's halen ze nummers van websites als telefoongids.nl en die bellen ze dan. Dat kost ze niets, omdat het met computers gebeurt..

Het gaat om telefoonnummers uit verre landen, zoals Madagaskar en Afghanistan. Mensen melden bijvoorbeeld dat ze worden gebeld omdat er een postpakket voor ze zou klaarstaan. Iemands telefoon rinkelt één keer, waarna de oproep wordt afgebroken. Op deze wijze kost het de fraudeur geen geld. Op het schermpje is te zien dat er een oproep gemist is, met een onbekend telefoonnummer erbij. Wie dat nummer belt, wordt verbonden met een duur betaalnummer en is dus geld kwijt. Het kan ook gaan om een sms'je met de vraag om te bellen.

Om hun slachtoffers zo lang mogelijk aan de lijn te houden, hebben de fraudeurs meerdere trucjes. Eén daarvan is het gebruik van een bandje. Als je terugbelt lijkt het alsof de kiestoon overgaat, maar in werkelijkheid is er allang opgenomen. De toon die je hoort, is dus vooraf opgenomen en wordt op dat moment afgespeeld.

Wanneer je terugbelt dan hoor je niks, maar er wordt wel een verbinding tot stand gebracht waar kosten aan verbonden zijn. Je hoeft je geen zorgen te maken dat je gehackt bent, dit is niet mogelijk. Heb je toch opgenomen, dan zijn daar geen kosten aan verbonden. Dit gebeurt pas als je zelf terugbelt.

Wangiri komt uit het Japans. Wan komt van het Engelse telwoord one en verwijst naar die ene keer dat de telefoon rinkelt. Giri verwijst naar de afbreking van de oproep en komt van kiru, het Japanse woord voor 'snijden', dat ook in harakiri (letterlijk 'buiksnijding') zit.



Bron: Fraudehelpdesk

Het kiezen van een bepaalde computernaam kan helpen bij het voorkomen van een ransomware-infectie.

Ransomware vermijdt computers met bepaalde namen

Althans, in het geval van de PadCrypt-ransomware. Deze ransomware blijkt namelijk computers met bepaalde computernamen te vermijden, wat onderzoek door onderzoekers moet bemoeilijken.

PadCrypt werd onlangs ontdekt en kwam in het nieuws omdat het over een chatfunctie beschikt, zodat slachtoffers met de makers kunnen communiceren. Een andere eigenschap waardoor PadCrypt het nieuws haalde is het aanbieden van een uninstaller, wat een unicum voor ransomware zou zijn. Via het verwijderprogramma kan de ransomware van de computer worden verwijderd. De versleutelde bestanden blijven echter versleuteld.

De makers van PadCrypt hebben een nieuwe versie uitgebracht, die allerlei "verbeteringen" bevat. Zo is de chatfunctie aangepast, alsmede de decryptietool als het losgeld van 300 euro is betaald. Daarnaast is er een blacklist van computernamen toegevoegd. Volgens het forum Bleeping Computer is dit bewust gedaan om onderzoek door onderzoekers te voorkomen. Zodra de malware de computernamen "PLACEHOL-", "MALTEST", "TEST-PC", "BEA-CHI", "BRBRB" en "VMSCAN" tegenkomt, zal de malware stoppen met werken.

Het vermijden van computers met bepaalde namen is niet nieuw. In 2009 vermeed de Bredolab Trojan computers met de computernaam "SANDBOX". Ook werden systemen niet besmet als er een gebruiker met de gebruikersnaam USER, user, CurrentUser of Sandbox werd aangetroffen. In het geval van een CryptoLocker-variant die vorig jaar werd ontdekt ging het in totaal om 13 computernamen, waaronder ook "SANDBOX", waardoor de malware de infectie staakte. Een jaar eerder was het de Neutrino-worm die bij de computernaam "SANDBOX", alsmede "MALTEST", "TEQUILABOOMBOOM", "VIRUS" en "MALWARE" stopte met werken.

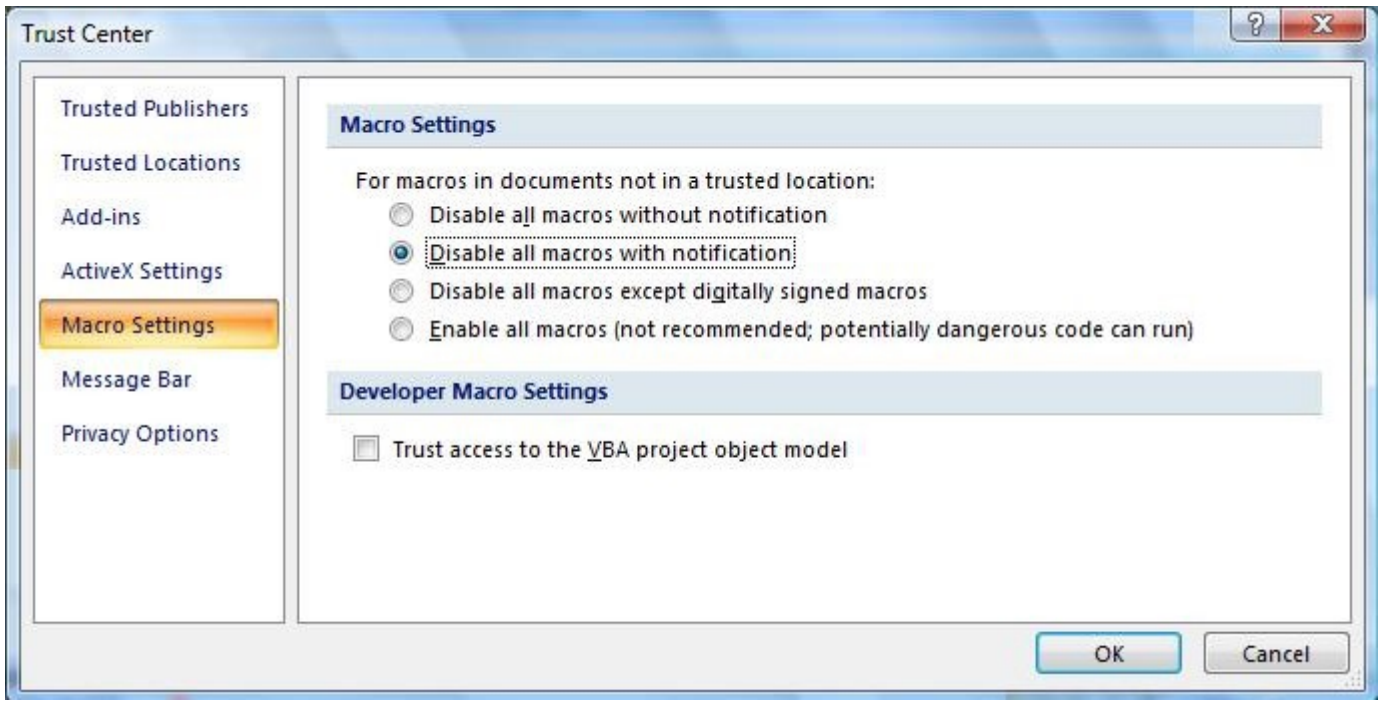
Microsoft heeft gebruikers van Office gewaarschuwd voor het risico van macro's in documenten en adviseert om standaard alle macro's die niet over een digitale handtekening beschikking uit te schakelen.

Microsoft waarschuwt voor risico van macro's in Word

Macro's laten gebruikers verschillende veelgebruikte taken automatiseren.

Het gebruik van macro's is echter ook een populaire aanvalsmethode voor computercriminelen. Macro's in Word-documenten worden onder andere gebruikt door ransomware. Een nieuwe ransomware-variant genaamd Locky verspreidt zich op deze manier en is zeer succesvol. Volgens Microsoft zijn er wereldwijd tal van computers die door Locky besmet zijn geraakt. De malware gebruikt Word- en Excel-documenten waaraan een macro is toegevoegd. In het geval een document over een macro beschikt toont Office een beveiligingswaarschuwing aan de gebruiker dat macro's zijn uitgeschakeld.

Vanwege misbruik door malware in het verleden besloot Microsoft macro's standaard uit te schakelen. Via de waarschuwing kan de macro via één muisklik weer door de gebruiker worden ingeschakeld. In het geval van veel ransomware downloadt de macro vervolgens de ransomware en installeert die op de computer. Om een infectie op deze manier te voorkomen adviseert Microsoft dan ook om macro's uit te schakelen. Alleen digitaal ondertekende macro's zouden moeten worden toegestaan. Dit kan via het Vertrouwenscentrum van Office worden ingeschakeld. Het is ook mogelijk om macro's geheel uit te schakelen, waarbij de gebruiker al dan geen melding krijgt.



Bron: Nu.nl/Tech

West-Europa is de afgelopen dagen opgeschrikt door een nieuwe, agressieve ransomware-variant: Locky. Maar wat is het precies, en hoe voorkom je besmetting?

Dit is wat je moet weten over Locky-ransomware

Beveiligingsspecialist ESET geeft antwoord. Locky is zogenoemde 'ransomware'. Dat is kwaadaardige software die je bestanden onbruikbaar versleutelt. Voor de 'sleutel' moet je de cybercriminelen betalen. Dat is ook bij Locky het geval. Door Locky versleutelde bestanden zijn alleen weer bruikbaar na betaling van een halve tot wel een hele bitcoin per bestand. Dat staat met de huidige wisselkoers gelijk aan zo'n 200 tot 400 euro. Er zijn zelfs prijzen gesignaleerd van maar liefst 10 bitcoins: 4000 euro!

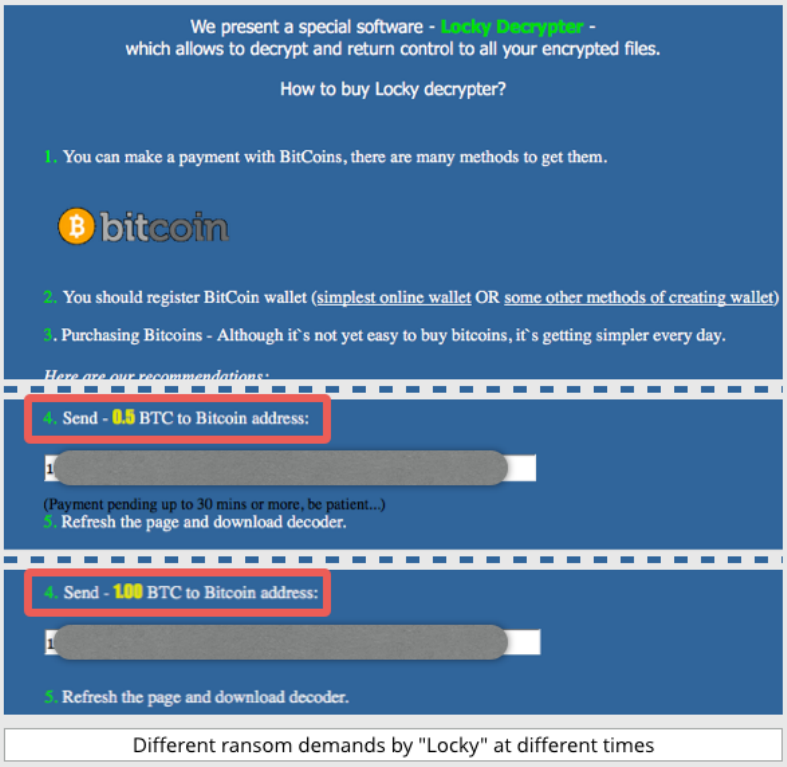
Hoe komt Locky 'binnen?
Locky komt binnen als een e-mail, waarin de verzender je vertelt dat je openstaande rekeningen hebt staan. De mail bevat een bijlage, de zogenaamde factuur. Dat is doorgaans een Word-bestand, in sommige gevallen is het een Javascript-bestand (.js) verstopt in een zip-file. Open je het Word-bestand, dan vraagt Word direct om macro's in te schakelen. Dit is een cruciale stap: ga je ermee akkoord, dan activeert dat de malware en versleutelen je bestanden tot een onleesbare brij tekens. Nooit doen dus!

Welke bestanden lopen gevaar?
Locky versleutelt een hele lijst aan bestanden die voldoen aan bepaalde criteria: afbeeldingen, video's, Office-bestanden, maar ook bronbestanden. Ook snapshot-bestanden, waarmee je je Windows-systeem naar de staat van een bepaald moment kunt herstellen, ontkomen niet aan Locky. Daarnaast zoekt het naar bestanden op gedeelde netwerkmappen, aangekoppeld of niet.

Hoe herken ik besmetting?
Locky verwisselt na het versleutelen je achtergrondafbeelding met een boodschap waar je de ontsleutelings software kunt downloaden. Zie je deze boodschap, dan ben je zeker besmet.

Hoe krijg ik mijn bestanden terug?
De beste manier is door het terugzetten van een back-up. Heb je die niet, dan is er momenteel helaas geen andere methode voorhanden, behalve met de speciale software die de cybercriminelen tegen betaling beschikbaar stellen.

Hoe voorkom ik besmetting met Locky?
• Verwijder verdachte e-mails direct;
• Open nooit bijlagen van verdachte e-mails;
• Macro's in Office zijn standaard uitgeschakeld. Dat is niet voor niets. Activeer nooit macro's in Office voor bijlagen uit e-mails, tenzij je zeker weet dat de macro valide is;
• Werk je systeem regelmatig bij, het liefst zo snel mogelijk na het verschijnen van een update;
• Maak gebruik van beveiligingssoftware en werk deze regelmatig bij;
• Geef jezelf en andere gebruikers niet meer gebruiksrechten dan strikt noodzakelijk. Zo verklein je de kans dat malware door verhoogde rechten snel om zich heen kan grijpen of dieperliggende delen van je systeem kan aantasten.



Different ransom demands by "Locky" at different times

Bron: Nu.nl/Tech

Niet alle IS-leden zijn zich voldoende bewust van de gevaren van het internet. Een nieuwe helpdesk moet de terroristen ook online uit de klauwen van overheidsdiensten houden.

Nieuwe helpdesk leert gevaren van het internet aan IS-leden

Eind vorig jaar raakte bekend dat terreurgroep IS een 24-uur helpdesk heeft om terroristen te helpen met onder andere encryptie. Uit een nieuw rapport blijkt echter dat IS zijn 'online diensten' naar een nieuw niveau heeft getild.

"In het verleden werd technische informatie en hulp verspreid via forums die met paswoorden werden beschermd. Het gemak waarmee IS-leden tegenwoordig aan informatie kunnen geraken, is alarmerend, met name wanneer deze informatie wordt gedeeld via private en beschermde kanalen," staat te lezen in het rapport dat met The Hill werd gedeeld.

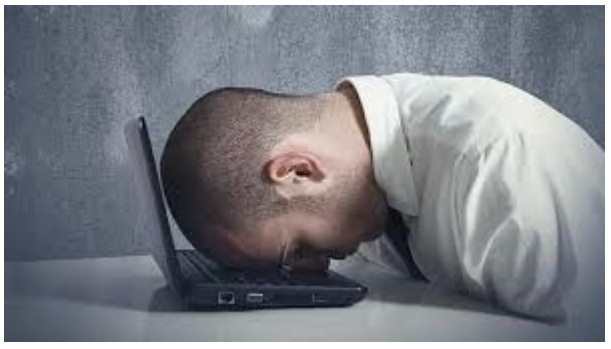
Electronic Horizon Foundation

De geüpgradede helpdesk wordt bemand door een groep IS-leden die de Electronic Horizon Foundation (EHF) wordt genoemd en op 30 januari werd opgericht. De EHF is volgens IS het antwoord op de strengere online controle die door het westen wordt uitgevoerd. Daarom zullen IS-leden instructies krijgen over hoe ze aan dergelijke controles kunnen ontsnappen.

"Het wordt tijd dat we elektronische bewaking het hoofd bieden, onze leden waarschuwen voor de gevaren van het internet en hen ondersteunen met tools en instructies. Hierdoor wordt voorkomen dat IS-leden beveiligingsfouten maken die kunnen leiden tot bombardementen en hun dood," staat te lezen in een aankondiging van IS.

Bron: Nu.nl/Tech

Pas op als een onbekende vrouw op facebook je vraagt om ‘even de broek omlaag’ te doen.



Sextorsion neem toe

Volgens het NRC is er een hausse in het aantal sextortion-gevallen. Eigenlijk willen die vrouwen maar één ding: geld.

De krant schrijft dat mannen worden ‘overspoeld’ door onbekende vrouwen die ‘staan te popelen’ om vrienden te worden. Ze komen uit Engeland of de VS maar schrijven erbarmelijk Engels, ze zijn voor PSV én voor Feyenoord, ze vinden The Revenant een gave film – en hun accounts zijn hooguit een week oud.

Na wat gechat en geflirt volgt snel de vraag of de webcam áán kan. ‘Even laten zien wat je hebt hangen’. Wie er in trapt, wordt afgeperst. ‘Ze zei: laat ‘m eens zien en toen vroeg ze vijfduizend euro’.

Bij Helpwanted.nl zien ze een enorme stijging van deze meldingen. ‘Het is elke dag raak’ – in 2015 370 meldingen, twee keer zo veel als in 2014, en in jan/feb van 2016 al tachtig. Terwijl veel mannen niet eens durven te melden. De politie zegt ook niet te weten hoeveel aangiftes er gedaan zijn. ‘Deze vorm van sextortion wordt niet apart geregisteerd’, aldus een woordvoerder. ‘Wij focussen op kwetsbare doelgroepen, zoals jongeren’.

Interpol spreekt overigens van honderdduizenden gevallen wereldwijd. Talinay Strehl van Helpwanted.nl adviseert nooit te betalen. ‘Als ze geloven dat er niets te halen valt, dan gaan ze vaak snel door naar de volgende prooi’. Ze vermoedt dat er georganiseerde bendes actief zijn, ‘de accounts leiden vaak naar Ivoorkust, Ghana en soms Marokko’. Facebook zelf zegt dat je nooit vriendschapsverzoeken moet accepteren van mensen die je niet kent …

Het Amerikaanse Vice had onlangs een prachtig verhaal waarom het zo moeilijk is om die sextortionists te vinden: twee mensen die elkaar niet kennen, geen van tweeën weet of de ander de waarheid spreekt of is wie die zegt te zijn, in verschillende landen ook nog eens; agenten en rechercheurs die soms wel en soms niet meewerken maar vaker niet eens weten hoe het allemaal in elkaar zit, technologisch gezien, en die ook nog eens een moreel oordeel vellen over je seksuele escapades met vreemden, aan wie je dan ook nog de foto’s moet laten zien van je eigen lijf – enfin, een paradijs voor afpersers.

Bron: NRC

In

Jongeren maken zich naar eigen zeggen vaak schuldig aan cybercrime, maar cijfers van de politie om dit te bevestigen ontbreken.

Jongeren zeggen zich vaak aan cybercrime schuldig te maken

Dat blijkt uit de tweejaarlijkse Monitor Jeugdcriminaliteit (MJC) van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Veiligheid en Justitie (WODC).

Cybercrime wordt door het WODC onderscheiden in cyber- en gedigitaliseerde delicten. In het eerste geval gaat het om zaken als hacken of het uitvoeren van DDoS-aanvallen. In het tweede geval gaat het om traditionele delicten die online worden gepleegd, zoals onlinebedreiging of het niet leveren van spullen die via een webwinkel zijn gekocht maar wel betaald. In deze editie van de MJC is voor het eerst ook uitgebreid onderzoek gedaan naar de mate waarin jongeren zijn betrokken bij cybercrime.

Statistieken

Politie- en justitiestatistieken bieden echter weinig informatie over het aantal jeugdige verdachten en strafrechtelijke daders van cybercrime. De informatie die beschikbaar is geeft volgens het WODC geen goed landelijk beeld van het aantal jeugdigen dat cybercrime pleegt. Uit ander onderzoek blijkt dat er sprake is van een forse onderregistratie van cybercrime door jeugdige daders in justitiële registraties. Een andere reden waarom nog weinig bekend is over daders van cybercrime is dat aangiften van cybercriminaliteit wel door de politie worden geregistreerd, maar dat deze niet zonder meer kunnen worden gekoppeld aan andere opsporingssystemen van de politie.

Op basis van zelfrapportage is er wel informatie over jongeren die cybercrime plegen. Het percentage jongeren dat zegt zich hier aan schuldig te maken is het hoogst onder de minderjarigen en het laagst onder de twaalfminners. Van de minderjarigen in 2015 zegt 31% in het voorafgaande jaar één of meerdere onlinedelicten te hebben gepleegd, bij de jongvolwassenen is dit 28% en bij de twaalfminners 10%.

Minderjarigen zeggen relatief vaker betrokken te zijn bij cybercrime dan jongvolwassenen. Vorig jaar rapporteerde respectievelijk 22% en 14% betrokken te zijn geweest bij één of meerdere gedigitaliseerde delicten over het voorafgaande jaar. Jongvolwassenen zijn relatief vaker betrokken bij cyberdelicten dan minderjarigen. In 2015 rapporteerde respectievelijk 22% en 17% betrokkenheid bij cybercrime in het voorafgaande jaar. Hoewel zelfgerapporteerde cybercrime onder jongeren aanzienlijk is, kan het WODC niet zeggen of sprake is van een verschuiving van offline- naar onlinedelicten.

Bron: Nu.nl/Tech

Er zijn maar weinig mensen die hun privacy niet belangrijk vinden. Toch durven we al eens privégegevens te grabbel gooien op Facebook.

Verbeter je privacy op Facebook

Weet jij wie je Facebook-posts en –foto's kunnen bekijken? Slechts weinig mensen kunnen hier met zekerheid 'ja' op antwoorden. Het volledig uitpluizen van je Facebook-instellingen neemt dan ook al snel enkele uren in beslag. Gelukkig bestaat er een manier om de klus een stuk sneller te klaren. Facebook voorziet namelijk enkele binnenweggetjes om je instellingen op een eenvoudige manier up-to-date te houden. Niet alle informatie is echter even duidelijk en door het continu nemen van binnenwegen, mis je ook enkele belangrijke instellingen. Door onderstaande stappen te volgen, kan je toch alle belangrijke privacy-instellingen aanpassen op slechts tien minuten tijd.

Uniek paswoord

De eerste tip die we je willen meegeven, gaat niet zozeer over privacy, maar is daarom niet minder van belang. Indien je hetzelfde wachtwoord op verschillende sites gebruikt, wordt het voor een hacker namelijk stukken eenvoudiger om het te kraken. Ga daarom naar het tabblad 'Algemeen' in het instellingenmenu om je Facebook-profiel van een nieuw en uniek paswoord te voorzien.

Advertentievoorkeuren

Velen weten dit niet, maar je kan beperkingen opleggen aan de advertenties die je op Facebook ziet. Wanneer je naar 'Advertenties' in het instellingenmenu gaat, zal je hiervoor drie opties terugvinden. Lees de uitleg bij deze instellingen grondig door om een geïnformeerde beslissing te kunnen nemen. De laatste optie is met name interessant indien je last hebt van een vloedgolf aan advertenties over een onderwerp waarin je niet geïnteresseerd bent. Deze instelling laat je namelijk toe de onderwerpen waarover Facebook denkt dat je advertenties wilt zien, te verwijderen. Ben je een fervente scout en krijg je de laatste tijd reclame over Chiro? Verwijder deze jeugdbeweging dan onmiddellijk uit de lijst.

Oude apps

Wanneer je wederom naar de linker kolom in het instellingenmenu gaat, zal je 'Toepassingen' zien staan. Dit submenu herbergt alle apps die je hebt geïnstalleerd en een link met Facebook hebben. Indien hier apps tussen staan die je niet langer gebruikt, kan je deze best verwijderen. Dit doe je door één voor één over de apps met je cursor te bewegen en telkens op het kruisje te klikken.

Tijdlijn en tags

Ook onder 'Tijdlijn en Tags' zijn er enkele interessante instellingen terug te vinden. Heb je liever niet dat vrienden naar believen dingen op je tijdlijn kunnen plaatsen? Ontneem hen dan dit recht volledig, of kies ervoor de berichten na te kunnen lezen alvorens ze definitief online verschijnen. Je kan in dit menu ook controleren wat anderen kunnen zien op je tijdlijn en instellen of je tags wilt controleren die anderen aan jouw foto's of over jou hebben toegevoegd.

Facebook-app

Ben je een fervente gebruiker van de Facebook-app, dan kan je ook daar alle instellingen naar je hand zetten. Hiervoor dien je rechts-bovenaan op het icoontje met drie horizontale streepjes te duwen. Scrol naar beneden tot je 'Privacy snelkoppelingen' tegenkomt. In dit submenu kan je enkele instellingen snel raadplegen, maar ook de volledige lijst met instellingen tonen door op 'Meer instellingen' te duwen. Om via de mobiele app links met toepassingen die je niet langer gebruikt, te verwijderen, dien je naar 'Apps' te gaan. Kies daarna 'Aangemeld via Facebook' en klik de app aan die je wilt ver-wijderen. Onderaan zal je 'App verwijderen' zien staan.

Toegang beperken

Onder de sectie 'Privacy' bevindt zich het merendeel van de instellingen die met je privégegevens te maken hebben. In het menu met maar liefst zeven verschillende instellingen kan je best de tweede en derde optie negeren. Deze bevatten namelijk een zodanig grote hoeveelheid data dat je urenlang bezig zal zijn met deze uit te spitten. De andere dien je daarentegen wel grondig te bestuderen. Hierin staat onder andere wie je posts mag bekijken, of mensen je Facebook-account op basis van je telefoonnummer kunnen opzoeken en of zoekmachines je profiel kunnen vinden.

Bron: Nu.nl/Tech

Nederlanders hebben vergeleken met andere Europeanen het minst last van computervirussen.

Het blijft oppassen met virussen

Dat blijkt uit cijfers van statistiekbureau Eurostat. Maar dat betekent niet dat we relaxed achterover kunnen leunen. Nederland is een gewild doel voor internetcriminelen, waarschuwt security researcher Jornt van der Wiel.

Zes procent van de Nederlandse computergebruikers werd vorig jaar getroffen door een virus of een andere computerinfectie, terwijl het gemiddelde in de Europese Unie op 21 procent lag. In 2010 had nog 23 procent van de Nederlanders te kampen met een computerinfectie.

,,Uitstekend nieuws'', reageert internetdeskundige Danny Mekic'. Hij ziet verschillende oorzaken voor de goede cijfers. ,,Nederlanders lopen voorop in Europa qua technologie. Daarnaast hebben Nederlandse bedrijven een voorsprong qua internetveiligheid. Zo laten banken hun klanten met scanners en codes inloggen, terwijl hun Duitse collega's nog met een inlognaam en een wachtwoord werken.'' Ook is het een voordeel dat Nederland klein en dichtbevolkt is, waardoor computernieuws zich razendsnel verspreidt.

Ransomware

,,De cijfers van Eurostat zijn lastig te verklaren'', reageert Van der Wiel, werkzaam bij antivirusbedrijf Kaspersky Lab. Volgens hem zijn de cijfers tegenstrijdig met het feit dat in Nederland juist de meeste pogingen worden ondernemen met ransomware. Bij dit type virus wordt iemands computer na besmetting 'vergrendeld' en moet het slachtoffer losgeld betalen om zijn bestanden te bevrijden.

Vermoedelijk weten veel mensen niet dat hun computer is geïnfecteerd met een virus. ,,Vroeger ging men amateuristisch te werk en bewoog de muis ineens de verkeerde kant op. Tegenwoordig gaat het er veel professioneler aan toe en valt een computerinfectie minder op.'' Volgens Van der Wiel is het gros van de aanvallen afkomstig uit Rusland en Oekraïne en zijn de criminelen vooral op geld uit.''

,,Rusland is een enorm land waar je je kunt verstoppen'', verklaart Mekic'. ,,Er is in dergelijke Oost-Europese landen veel computerkennis en er heerst een goede ICT-economie. Bovendien hebben de recente ontwikkelingen in die regio criminaliteit in de hand gewerkt. Voor internetcriminaliteit is relatief weinig nodig, maar het levert des te meer op.''

Spam

,,Nederland is een gewild doel voor internetcriminelen'', vertelt Van der Wiel. ,,Nederlanders zijn welvarend en redelijk digitaal: ze krijgen dagelijks veel mails en doen veel meer aan telebankieren dan elders in Europa.'' Via linkjes en spam is intussen al menig computer met een virus geïnfecteerd.

Ook Mekic' ziet Nederland als een gewillig mikpunt. ,,Nederland is een land met veel internetverkeer en daardoor interessant voor criminelen. Een andere reden waarom zij het op Nederland gemunt hebben, is dat er hier weinig capaciteit is om bijvoorbeeld ransomware op te sporen.''

Mekic' ziet toch dat het beleid van de Nederlandse overheid en de bankenwereld zijn vruchten afwerpt. ,,De enorme strijd met criminelen lijkt succesvol. Er is een continue aandacht voor deze technologie. Ik reis veel en ik zie dat computers en internet veel meer een issue zijn in Nederland dan in andere landen. Er wordt hier veel aandacht besteed aan het updaten van computers. Zo gebruiken nog maar weinig mensen Windows XP.''

		2010	2015
1.	Macedonië	68%	71%
2.	Kroatië	33%	41%
3.	Hongarije	46%	36%
4.	Portugal	37%	33%
5.	Frankrijk	34%	29%
	(...)		
26.	Noorwegen	28%	13%
27.	Ierland	15%	11%
28.	Slowakije	47%	9%
29.	Tsjechië	26%	8%
30.	Nederland	23%	6%
	EU	31%	21%

Bron: Nu.nl/Tech

Het grote marktaandeel en de 1,4 miljard dagelijkse gebruikers zijn een uitstekende voedingsbodem voor hackers om geld af te persen bij geïnfecteerde toestellen.

Ransomware wordt heel gevaarlijk voor Android in 2016

In een recent rapport van Bitdefender doet de beveiligingsfabrikant het risico van Android uit de doeken. Het besturingssysteem Android staat hoog aangeschreven bij hackerorganisaties voor een gloednieuwe golf aan ransomware in 2016. Het dominante marktaandeel (82,2% in Q2 2015) en het hoge aantal actieve dagelijkse gebruikers (1,4 miljard) is een perfecte voedingsbodem om geld te verdienen middels afpersing.

Pincode veranderd

Ransomware op Android logt de gebruiker meestal automatisch uit, met de melding dat je geld moet betalen om opnieuw in te loggen. Een penibele situatie waar je niet aan moet toegeven, maar vele gebruikers doen dat meestal wel omdat ze niet weten hoe ze hun toestel naar fabrieksinstellingen kunnen terugzetten zonder in te loggen. Enkel op die manier kan je kosten voorkomen.

Een simpel voorbeeld verandert de pincode van het lockscreen en zorgt er tegelijk voor dat het niet kan worden gestopt via het taakbeheer. Exact dezelfde manier wordt nu ook gebruikt door hackers om pc-gebruikers af te persen door de malware telkens mee te laten opstarten.

Encryptie

Bestanden encrypteren en onbruikbaar maken tot er wordt betaald komt nog niet voor op Android, maar Bitdefender verwacht dat het niet lang meer zal duren tot ook die praktijk wordt toegepast. Oplossingen voor dat probleem zijn een stuk complexer, met automatisch verlies van bestanden als gevolg.

Hoe krijg je ransomware binnen op Android? Het meeste komt binnen via malafide mobiele advertenties. Ze kopen advertentieruimte bij correcte websites om hun bereik te vergroten, en om de valstrik subtieler te maken. In 2015 vielen 4,35% van alle Android-toestellen in de val van ransomware. Er wordt verwacht dat dat aantal in 2016 flink de hoogte in zal schieten. Antivirus installeren kan helpen, maar let vooral op wat je allemaal aantikt op het scherm en blijf weg van valse websites of bijlages in mails die niet betrouwbaar zijn.

Bron: ZDnet

Eén misstap op het internet kan ertoe leiden dat al je bestanden worden versleuteld. Malwarebytes Anti-Ransomware kan je gelukkig tegen zulke ransomware beschermen.

Zo geef je ransomware geen kans

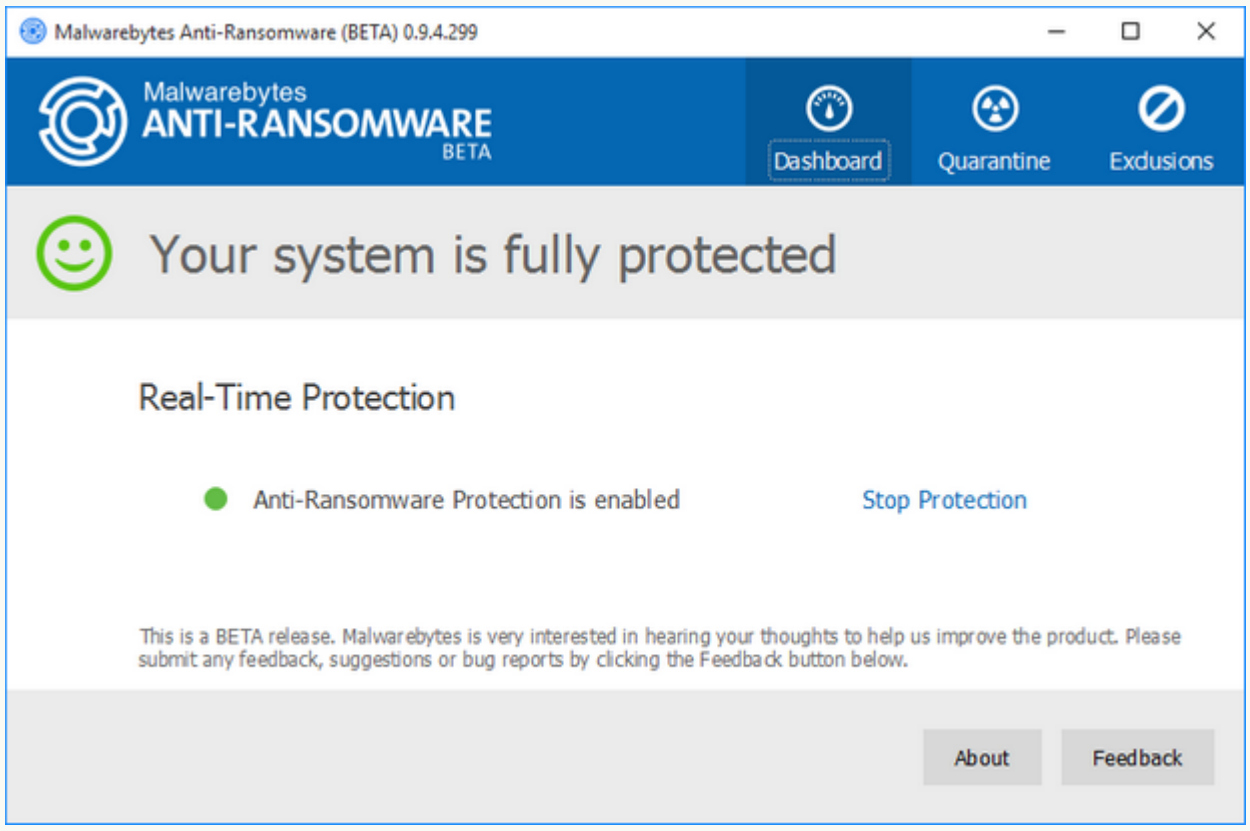
De voorbije jaren is ransomware een veel gezien kwaad geworden. Eenmaal de malware op je computer geraakt, zal het zich razendsnel doorheen je bestanden bewegen en deze één voor één encrypteren. Voor onfortuinlijke slachtoffers zit er vaak niets anders op dan losgeld te betalen om hun files terug leesbaar te laten maken. Hierdoor is het verspreiden van ransomware een erg winstgevende zaak en proberen cybercriminelen met name bedrijven in de val te lokken.

Vorig jaar bracht Kaspersky al een tool uit die je kan gebruiken om je bestanden gratis te redden eenmaal je slachtoffer bent gevallen aan een vorm van ransomware. Deze tool werkt echter niet in alle gevallen en kan niet voorkomen dat je bestanden worden versleuteld.

Malwarebytes Anti-Ransomware

Vandaar dat Malwarebytes nu met een eigen applicatie op de proppen komt. Anti-Ransomware zal net als een antivirusprogramma op de achtergrond op je computer draaien. Eenmaal het programma kwaadwillige code in de gaten krijgt, zal de malware onmiddellijk een halt worden toegeroepen. Hierdoor zullen CryptoLocker, CryptoWall, of CTBLocker niet langer in staat zijn om je bestanden te versleutelen. Ook zal Anti-Ransomware je beschermen tegen nieuwe vormen van ransomware.

Voorlopig is Anti-Ransomware verkrijgbaar als bèta. Iedereen kan het programma echter al downloaden en installeren, maar Malwarebytes waarschuwt wel dat er nog bugs aanwezig kunnen zijn in hun tool.



Bron: MalwareBytes

Kaspersky Labs Anti-Malware Research Team heeft een van de gevaarlijkste Android-bankieren trojans ooit gedetecteerd.

Acecard-trojan: gebruikers van 30 miljoen bank- en betaalapps lopen risico

De Acecard-malware is in staat om gebruikers van bijna 50 verschillende online financiële applicaties en diensten aan te vallen en kan de beveiligingsmaatregelen van de Google Play Store omzeilen.

Tijdens het derde kwartaal van 2015 ontdekte Kaspersky Lab een ongewone toename van het aantal mobiele bankieraanvallen in Australië. Dit zag er verdacht uit en al snel werd ontdekt dat de belangrijkste reden voor deze stijging toe te schrijven was aan een enkele bankierentrojans: Acecard.

De Acecard-trojanfamilie maakt gebruik van vrijwel alle momenteel beschikbare malwarefunctionaliteiten - van de diefstal van tekst- en spraakberichten van banken, tot overlays op officiële app-vensters met valse berichten die de officiële inlogpagina simuleren in een poging om persoonlijke informatie en accountgegevens te stelen. De meest recente versies van de Acecard-familie kunnen de client-toepassingen van zo'n 30 bank- en betaalsystemen aanvallen. Aangezien deze trojans op commando een overlay kunnen plaatsen op een applicatie, kan het totale aantal aangevallen financiële toepassingen veel hoger zijn.

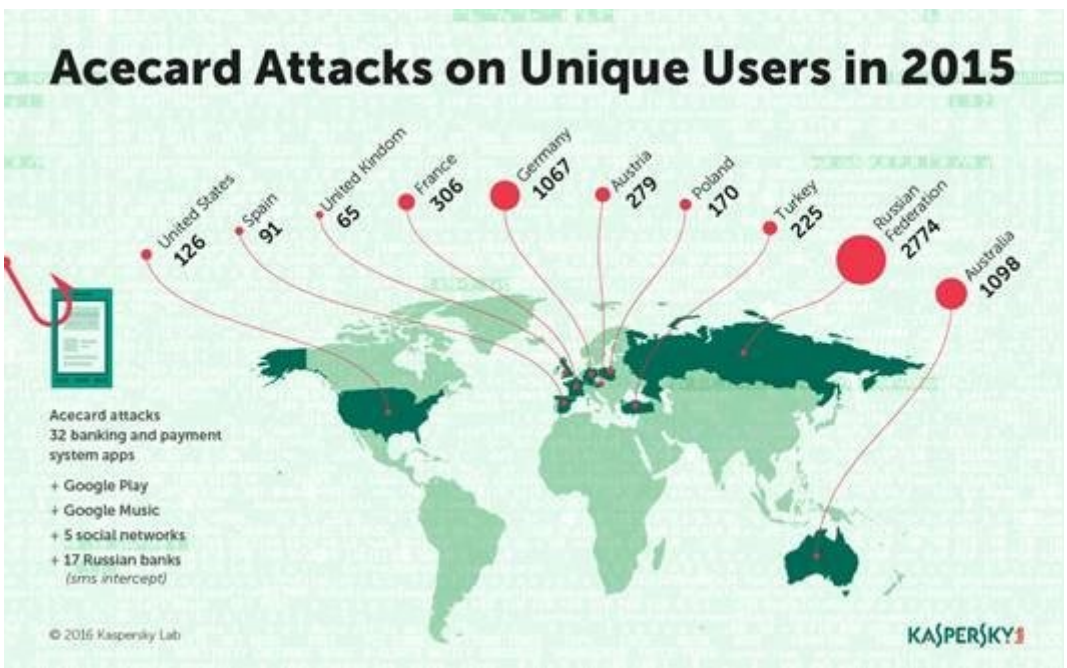
Behalve bij bankierapps kan Acecard bij de volgende toepassingen een overlay met phishing-vensters plaatsen:

- Chatdiensten: WhatsApp, Viber, Instagram, Skype;
- Sociale netwerken: Facebook, Twitter, VKontakte, Odnoklassniki;
- De Gmail-client;
- De PayPal mobiele app;
- Google Play en Google Music-toepassingen.

De malware werd voor het eerst ontdekt in februari 2014, maar vertoonde geruime tijd vrijwel geen tekenen van kwaadaardige activiteiten. Dit alles veranderde in 2015, toen onderzoekers van Kaspersky Lab een piek ontdekten in het aantal aanvallen: in de periode mei-december 2015 werden meer dan 6.000 gebruikers aangevallen door deze trojan. De meesten van hen waren woonachtig in Rusland, Australië, Duitsland, Oostenrijk en Frankrijk. Gedurende de twee jaar van observatie waren Kaspersky Lab-onderzoekers getuige van de actieve ontwikkeling van de trojan. Ze registreerden meer dan 10 nieuwe versies van de malware, elk met een veel langere lijst van kwaadaardige functies dan de vorige.

Google Play ligt onder vuur

Mobiele apparaten werden meestal besmet na het downloaden van een kwaadaardige toepassing die zich voordeed als een legitieme. Acecard-versies worden meestal verspreid als Flash Player of PornoVideo, hoewel soms ook andere namen worden gebruikt in een poging om zich voor te doen als nuttige en populaire software.



Bron: Kaspersky Labs

Whitepages herkent onbekende telefoonnummers, en waarschuwt je wanneer niet Microsoft of je bank maar een fraudeur aan de lijn hangt.

Laat je smartphone automatisch fraudeurs blokkeren

Whitepages kan je gerust de Witte Gids van weleer op steroïden noemen. De applicatie helpt je automatisch om onbekende telefoonnummers te herkennen, en waarschuwt je bovendien wanneer een inkomende oproep wel eens van een persoon met duistere intenties kan komen. De app zit geïntegreerd in je smartphone, en kijkt naar de telefoonnummer van een inkomende oproep. Die nummer wordt vervolgens vergeleken met een steeds groeiende wereldwijde database van meer dan anderhalf miljard telefoonnummers.

Spambescherming

De integratie van Whitepages in een smartphone zorgt er voor dat je op je standaard-belapplicatie te zien krijgt wie je via je telefoon te pakken wil krijgen. De app bevat een steeds groter wordende lijst van nummers die geassocieerd worden met spam of fraude. Dat wordt dezer dagen steeds belangrijker. Phishing, waarbij criminelen je wachtwoord te pakken proberen te krijgen om je zo geld te ontfrutselen, gebeurt immers niet uitsluitend online.

Je zou niet de eerste zijn die een telefoontje ontvangt van iemand die zich uitgeeft als werknemer van je bank of van Microsoft. Dergelijke frauduleuze telefoontjes onderscheiden van de echte is niet altijd even eenvoudig, en daar wordt de meerwaarde van Whitelist duidelijk: als een inkomende oproep niet van een anonieme nummer komt, maar van ‘Fraude’, dan zal je minder geneigd zijn om de leugenaar aan de andere kant van de lijn te geloven.

Samen veilig

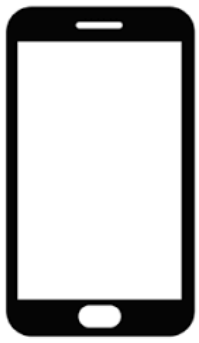
Natuurlijk kan een spammer van nummer wisselen wanneer hij merkt dat zijn pogingen tot misleiding steeds vaker bot vangen. Ook dan kan Whitepages helpen: wie fraude detecteert kan met een druk op de knop aangeven dat zijn huidige gesprekspartner niet te vertrouwen is. Op die manier kan je collega-gebruikers helpen.

Je krijgt (hopelijk) niet iedere dag telefoon van criminelen, en dat weten ze bij Whitepages ook. De app helpt je verder om snel zaken en winkels dichtbij te vinden, vanuit de telefoon-app. Daarmee kan je de app nog het best vergelijken met een hybride combinatie van de Witte en Gouden Gids, verwerkt in je telefoon met een neusje voor malafide bellers.

Whitepages is te downloaden als afzonderlijke app via de Play Store.

Bron: Nu.nl/Tech

Tweedehands smartphones zitten nog altijd vol privégegevens, zoals pikante foto's, e-mails en tekstberichten.



Onderzoek: tweedehands smartphones vol privégegevens

Dat stelt anti-virusbedrijf Avast, dat 20 tweedehands smartphones onderzocht. Het ging om smartphones die in New York, Parijs, Barcelona en Berlijn via een pandjeshuis waren gekocht.

Via gratis herstelsoftware wisten de onderzoekers nog allerlei gegevens te vinden. Het ging om meer dan 1200 foto's, 200 naaktfoto's, 149 foto's van kinderen, meer dan 300 e-mails en tekstberichten, een pornovideo, meer dan 260 Google-zoekopdrachten, waarvan 170 naar porno zochten, drie facturen en een arbeidscontract. Ook kon van twee toestellen de identiteit van de vorige eigenaar worden vastgesteld.

Fabrieksreset

De pandjeshuizen lieten de onderzoekers weten dat bij alle telefoons er een fabrieksreset was uitgevoerd en de gegevens van de vorige eigenaar waren verwijderd. Bij twaalf toestellen bleek dit niet het geval te zijn. Van de telefoons waar een fabrieksreset was uitgevoerd, bleek dat de helft nog steeds persoonlijke gegevens bevatte. Dit kwam omdat de smartphones een oudere Android-versie gebruikten waarbij de fabrieksreset niet goed werkt. Sommige eigenaren hadden hun bestanden zelf verwijderd en geen fabrieksreset uitgevoerd, terwijl anderen helemaal geen gegevens hadden verwijderd of de reset uitgevoerd.

Bij twee van de telefoons was de vorige eigenaar zelfs vergeten om bij Gmail uit te loggen, waardoor de nieuwe eigenaar op zijn account kon inloggen om vervolgens e-mails te lezen en te versturen. Volgens Avast zijn nieuwere Android-smartphones behoorlijk veilig als het om de fabrieksreset gaat, maar worden gebruikte telefoons met oudere Android -versies waarvan de reset niet goed werkt nog steeds verkocht. Gebruikers krijgen dan ook het advies om alle bestanden op de telefoon te overschrijven voordat die wordt verkocht.

In een recent rapport van Bitdefender doet de beveiligingsfabrikant het risico van Android uit de doeken. Het besturingssysteem Android staat hoog aangeschreven bij hackerorganisaties voor een gloednieuwe golf aan ransomware in 2016.

Gevaar voor afpersing reëel op Android

Het dominante marktaandeel (82,2% in Q2 2015) en het hoge aantal actieve dagelijkse gebruikers (1,4 miljard) is een perfecte voedingsbodem om geld te verdienen middels afpersing.

Pincode veranderd

Ransomware op Android logt de gebruiker meestal automatisch uit, met de melding dat je geld moet betalen om opnieuw in te loggen. Een penibele situatie waar je niet aan moet toegeven, maar vele gebruikers doen dat meestal wel omdat ze niet weten hoe ze hun toestel naar fabrieksinstellingen kunnen terugzetten zonder in te loggen. Enkel op die manier kan je kosten voorkomen.

Een simpel voorbeeld verandert de pincode van het lockscreen en zorgt er tegelijk voor dat het niet kan worden gestopt via het taakbeheer. Exact dezelfde manier wordt nu ook gebruikt door hackers om pc-gebruikers af te persen door de malware telkens mee te laten opstarten.

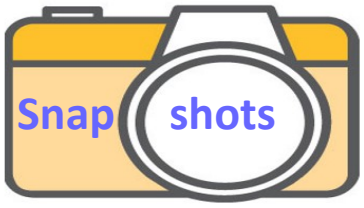
Encryptie

Bestanden encrypteren en onbruikbaar maken tot er wordt betaald komt nog niet voor op Android, maar Bitdefender verwacht dat het niet lang meer zal duren tot ook die praktijk wordt toegepast. Oplossingen voor dat probleem zijn een stuk complexer, met automatisch verlies van bestanden als gevolg.

Hoe krijg je ransomware binnen op Android?

Het meeste komt binnen via malafide mobiele advertenties. Ze kopen advertentieruimte bij correcte websites om hun bereik te vergroten, en om de valstrik subtieler te maken. In 2015 vielen 4,35% van alle Android-toestellen in de val van ransomware. Er wordt verwacht dat dat aantal in 2016 flink de hoogte in zal schieten. Antivirus installeren kan helpen, maar let vooral op wat je allemaal aantikt op het scherm en blijf weg van valse websites of bijlages in mails die niet betrouwbaar zijn.

Bron: Security.nl



In de VS al een groot succes, ook bij politie en brandweer: de ‘burenapp’ Nextdoor. Vergelijkbaar met Whatsapp maar dan met woonadres erbij. Nextdoor toont ‘een kaartje met huisjes en je ziet precies wie in welk huisje woont’, waar je in ‘een gewone appgroep niet altijd ziet wie er mee doet en waar ze wonen’. In de VS zijn al 90 duizend buurten op de app actief. Tamar van de Paal van Nextdoor zegt dat Nederland het eerste land buiten de VS is waar de app wordt getest. In tachtig Nederlandse buurten, onder meer in Capelle aan den IJssel. Nextdoor wil politie en brandweer in Nederland voorlopig nog niet toelaten.

———————————————————

In 2015 is het aantal mensen en ondernemers dat werd opgelicht via internet, bijna verdubbeld. De Fraudehelpdesk kreeg 3625 meldingen, tegen 1887 in 2014. De meeste slachtoffers kochten iets op Marktplaats maar kregen dat niet geleverd. De melders gingen in 2015 voor 12,2 miljoen euro het schip in, in 2014 werd nog 8 miljoen schade gemeld. Volgens de helpdesk meldt 10 tot 13% van de slachtoffers dit bij de helpdesk. ‘De werkelijke cijfers over aantallen slachtoffers en schadebedragen liggen dus aanzienlijk hoger’.

———————————————————

Meer dan drieduizend automobilisten stonden deze week in ‘de grootste file ooit’ op de M25 in Surrey. Ze kwamen opdagen na een oproep op facebook om te parkeren op een groot terrein langs die snelweg. ‘Surviving the Nightlife’ was opgezet door ene Gareth Field, als een geintje natuurlijk. Maar het werd zo druk dat de politie zich genoodzaakt zag enkele op- en afritten te sluiten. Via facebook en andere media riepen politie én Field daarna dat het geen zin had om nog te komen; de honderden automobilisten die al onderweg waren, kwamen geen meter verder. Wat behalve tot enthousiasme bij de organisatoren, vooral tot ergernis leidde bij mensen die in de file stonden.

———————————————————

Met tips uit een Whatsapp-groep heeft de politie twee inbrekersweten te pakken. De twee (30 en 35, uit Spijkenisse) waren in Arnhem over een schutting geklommen. Omwonenden appten de politie die ter plaatse ging en de mannen wist te arresteren.

———————————————————

Na een hausse in de verkoop van Lego, heeft de politie Heemstede nu foto’s met Lego-dieven op internet gezet. Dit ‘zware opsporingsmiddel’ is volgens de politie nodig om een eind te maken aan de diefstallen. Lego is populair en blijkt veel waard te zijn, aldus het bericht. Het wordt zelfs als betaalmiddel gebruikt, bijvoorbeeld door verslaafden. Een junk die Lego pikte bij een speelgoedwinkel, betaalde er zijn harddrugs mee. De dealer verkocht het speelgoed vervolgens voor veel geld op Marktplaats.

———————————————————

Het chatten over seks met kinderen moet strafbaar worden. Dat schrijft justitieminister Ard van der Steur aan de Tweede Kamer. Hij wil de hele zedenwetgeving moderniseren, zeker met het oog op de moderne communicatiemiddelen. Van der Steur wil de plannen in het najaar hebben uitgewerkt. De bewindsman reageert ermee op onderzoek door de Rijksuniversiteit Groningen in opdracht van het Wetenschappelijke Onderzoek- en Documentatiecentrum (WODC). Daaruit werd geconcludeerd dat 'verschillende vormen van digitale ontucht met kinderen een duidelijke plaats moeten krijgen' in de wetgeving. De gevolgen van digitale ontucht kunnen heel groot zijn. Het kind kan er immers helemaal in verstrikt raken. Van der Steur vindt straf op zijn plaats als een kind 'in een belevingswereld wordt getrokken waar het niet in thuis hoort''. In 2012 bleek al uit onderzoek onder ouders dat een meerderheid voor het strafbaar stellen van seksueel getinte gesprekken online is. Bijna 90 procent van de 1000 ondervraagde ouders is van mening dat de overheid op moet treden. Het is de vraag of het nieuwe voorstel dit jaar nog van kracht zal zijn. Een wetsvoorstel moet eerst langs de Tweede en Eerste Kamer voor het van kracht kan worden. Sinds 1 januari 2010 het zogenaamde grooming (digitaal kinderlokken) al strafbaar gesteld. Bij grooming probeert een volwassene online een seks-afspraak te maken met een minderjarige.

———————————————————

Niet alleen op het ‘gewone’ web, maar vooral op het dark web, het deep web of hoe je het ook noemen wil, zijn er ‘cryptomarkets’ waar drugs verhandeld worden. Het European Monitoring Centre for Drugs and Drugs Abuse schrijft in een nieuw rapport dat internet de drugsmarkt net zo veranderd heeft als de boekenmarkt, de muziekwereld en de filmindustrie. Drugs en internet horen bij elkaar als bitcoins bij Tor-netwerken. Nauwelijks verrassend is dat op het web vooral pillen, medicijnen en andere ‘non-controlled substances’ verkocht worden en dat je voor echte ‘illicit drugs’ naar het deep web moet. Dat gaat steeds makkelijker, aldus het rapport: iedereen is 24/7 en overal online en ict-kennis is nauwelijks nog nodig om iets te encrypten of anoniem te browsen.

———————————————————

Uit een lange termijn veiligheidsonderzoek van het CBS blijkt dat Nederlanders zich steeds veiliger voelen. De criminaliteit daalt, de politie telde 29% minder misdrijven en 35% minder verdachten. Met name jongeren pleegden minder misdrijven. Zo daalde het aantal aangehouden verdachten van 12-18 jaar met 64%. Opvallend is dat drie op de tien jeugdigen (12-23 jaar) zeiden dat ze in 2015 wel eens een cyberdelict hebben gepleegd. Het gaat dan niet alleen om ‘relatief onschuldige overtredingen’ (inloggen op iemand anders computer, veranderen van wachtwoorden) maar ook om zwaardere delicten. Twee procent van de tieners (12-18) zei wel eens een DDoS-aanval te hebben uitgevoerd; Een op de vijf bekende een digitaal delict, zoals iemand online bedreigen (8%) of het ongewenst versturen van naaktfoto’s (5%). Het Wodc gaat verder onderzoek doen naar de relatie jongeren-cybercrime, onder meer om te kijken of preventiemaatregelen voor offline-misdrijven ook werken voor online-misdrijven. Volgens Wodc-directeur Frans Leeuw is digitaliteit ‘heel ingewikkeld en gaat het razendsnel’ en zijn jongeren steeds meer online bezig. ‘Niet alleen sociaal maar mogelijk ook asociaal’.

———————————————————

Het Nederlandse ministerie van EZ onderzoekt of er is gefraudeerd bij de verkoop van tickets voor concerten van onder meer Adele en K3. Eerder dit jaar bleek in België dat er massaal identiteitsfraude is gepleegd. De kaartjes gingen op internet soms tien keer over de kop. Omdat veel kaartjes werden aangeboden op Nederlandse websites, belde de Belgische minister van Consumentenzaken met zijn collega Henk Kamp in Nederland. Die heeft nu besloten de zaak te onderzoeken. Kamp benadrukt dat het strafbaar is als bedrijven de tickets kochten en zich daarbij voordeden als privépersonen.

Een aspirant-agent (27, uit Ter Aar) is tot twaalf maanden celstrafveroordeeld, waarvan de helft voorwaardelijk, omdat hij via Skype en Snapchat met minderjarige meisjes bezig was. Nicky V. dwong onder meer een 15-jarig meisje om naaktfoto's en -filmpjes van zichzelf te maken. Hij kreeg zes naaktfoto's en een paar filmpjes, maar toen hij meer vroeg, probeerde het meisje het contact te verbreken. De verdachte zocht vervolgens in politiesystemen naar haar huisadres en stuurde een naaktfoto op. 'Je wilt toch niet dat je ouders dit zien?' Ook al had de verdachte geen fysiek contact met het meisje en claimde hij dat hij de foto's nooit openbaar zou maken, de rechtbank vond hem toch schuldig aan ontucht, afpersing en vervaardiging van kinderporno.

———————————————————-

In Groot-Brittannië heeft de politie binnenkort nieuwe richtlijnen voor sexting. Britse tieners die hun eigen naaktfoto's naar leeftijdgenootjes zenden, worden dan niet meer vervolgd, om te voorkomen dat 'mogelijk miljoenen tieners' worden geregistreerd als sex offender. Het 'vrijwillig uitwisselen van pikant beeldmateriaal' moet het criminaliseren van deze tieners – een strafblad! – voorkomen, maar ook de politie ontlasten, aldus The Mail Online. Sexting is vooral 'a normal part of growing up'. In 2015 werd een Engelse tiener die via Snapchat een piemelfoto naar een 14-jarig meisje stuurde opgepakt, vervolgd en in de politiedatabase opgenomen. De politie zal wel alert blijven, zegt deputy chief constable Olivia Pinkney, op dwang, uitbuiting en andere strafbare feiten maar ook op de motieven van het rondsturen (pesten, wraak). Pinkney, portefeuillehouder jeugd, zegt dat de 'unnecessary criminalisation of young people' voorop staat maar ook dat sexting risicovol blijft. 'Once circulated, the sender loses all control of that image and can cause significant distress when it gets into wider hands'.

———————————————————

Belgen kunnen al tien jaar via de website Police-on-web een internetaangifte doen. De site is nooit erg succesvol geworden: op dit moment zijn er zestien aangiftes per dag. Maar de site blijkt ook nog niet compatibel te zijn. Agenten moeten elke aangifte handmatig overtikken. 'Alsof agenten niets beters te doen hebben', zegt kamerlid Roel Deseyn (CD&V) die een 'grondige opkuis' van de site bepleit. De politie zelf is ook al niet enthousiast over de site. Een vakbondswoordvoerder noemde de site al verbetering vatbaar en korpschef Marc Hellinckx 'kijkt met grote ogen hoe de Nederlandse politie online bezig is'.

———————————————————

Dat adverteerders kunnen profiteren van Facebooks nieuwe reactiebuttons (like, love, haha, wow, sad, angry) leidt natuurlijk geen twijfel. Maar kunnen polities en opsporingsdiensten dat ook? Volgens een bericht op Reveal News wel! Met de zes nieuwe emoji 'determining emotion and sentiment through Facebook could now be exponentially simpler' – zie ook het aantal recente rechtszaken waarin emoji een rol spelen. Sterker nog, schrijft Reveal: hoewel de nieuwe emoji niet specifiek ontworpen zijn voor law enforcement, kunnen ze wel bepalend zijn bij het al dan niet strafbaarstellen of schuldig bevonden worden. Al was het maar omdat nu duidelijker is wel sentiment er achter die emotie zit – mooie extra kolommetjes in een analyse-spreadsheet. Anderen betwijfelen echter de opsporingswaarde. Burgerrechtenadvocaat Lee Rowland bijvoorbeeld, actief bij de ACLU, denkt dat de politie alleen maar méér gaat vastleggen en nog meer data wil gebruiken om bijvoorbeeld profielen mee te bouwen. Hij verwijst naar een zaak waarin een zwarte jongen onterecht werd vastgezet omdat zijn profiel overeen kwam met dat van échte criminelen. Onduidelijk blijft vooral de waarde van (straat- of jongeren)taal en emoties op sociale media. Is een haha-emoji nou echt zo bedoeld of alleen maar cynisch? 'Natuurlijk kun je met emoji dreigingen uiten', zegt Rowland, maar je doet op zich niks illegaals als je online 'your like or love' aangeeft.

———————————————————

Op zoek naar informatie over de zaak-Amzieb doet de politie Amsterdam, behalve een traditioneel buurtonderzoek, ook digitaal buurtonderzoek. Via facebook wordt geprobeerd tips te krijgen. Het lichaam van Nabil Amzieb werd in Zuidoost gevonden, zijn hoofd op de Amstelveenseweg in Zuid. In Utrecht werden de twee auto's gestolen die later uitgebrand zijn. De politie wijst ook op facebook 'nadrukkelijk' op de mogelijkheid om anoniem te melden.

———————————————————

Herkenningstekens op woningen? Onzin, zegt universitair docent en broodje-aap-onderzoeker Peter Burger. Hij reageert op het facebookbericht van het politieteam Kaag en Braassem dat vorige week nog waarschuwde voor deze 'dieventekens'. In dat bericht schreef het politieteam dat er op verschillende woningen 'tekens waren aangetroffen', mogelijk afkomstig van inbrekers. Terwijl iedereen weet, zou kunnen weten, hoort te weten, dat die dieventekens, net als het witte-busjesverhaal over kinderontvoerders, onzin is. De dieventekens stonden in 1923 al in de krant, weet Burger, terwijl er nog nooit een inbreker is ontdekt die zo'n teken neerzette. In heel West-Europa circuleren dit soort berichten al decennialang, maar 'zo werken inbrekers niet'. Volgens Burger is het bericht van de politie verwarrend en worden mensen onnodig bang gemaakt. De politie kan deze geruchten volgens hem simpelweg verifiëren en ontzenuwen. 'Maar nu elke wijkagent een megafoon heeft om het hele land te bereiken' – sociale media – zien we daar ook de nadelen van, zoals het verspreiden van geruchten. 'Mensen delen dit soort berichten massaal. Niet omdat ze weten dat het klopt, maar omdat ze vinden dat delen geen kwaad kan. Agenten handelen vaak niet anders dan gewone burgers en geven ook met de beste bedoelingen onbevestigde waarschuwingen door'. De kracht van sociale media is zo ook de zwakte ervan. 'Het kwaad is al geschied als iets eenmaal online staat'. Terwijl het simpel te controleren is: wie een beetje googlet, snapt de achtergrond. Woordvoerder Liesbeth Voorthuijsen van politie Den Haag zegt dat de tekens in dit bewuste geval door de bewoners zijn aangetroffen. 'Ook al zijn het er maar enkele, we hebben er voor gekozen om bewoners hierop te attenderen'. Volgens haar wil de politie mensen niet bang maken, maar wel alert. 'Door dit facebookbericht kan het ook zo zijn dat we achter de herkomst van de tekens komen'.

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 Hijg 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

Nieuw:

Webinar Computercriminaliteit

Mousejack

Gegijzeld door Ransomware. Wat nu?

Telefonische phishing

Nieuw:

Grooming

Sexting

Webcammisbruik

Bedreigd/gechanteerd

Kinderporno

Nepprofiel

Schatkist

Naslag:

- Handleiding Twitter
- Gebruik tweetraps authenticatie
- Windows 10 installatie
- Online verdwijnen
- Centraal cloudbeheer
- Online kopen
- Cybersecurity 2015
- Stickware
- Netwerk in de knoop
- Slachtofferschap cybercrime en internetgebruik (nieuw)
- Handreiking Cybercrime (nieuw)

Muziek: DoubleYouAB

- Return to TubularBells
- FeddeLeGrand remix
- Faithless Insomnia remix
- ReeAnna2015
- 1.11 Armin
- SummerHardstyle2015
- Summermix2015
- TrancePhonic 2015
- Open Your Eyes 2015 rmx (nieuw)
- MikeOldfieldReborn (nieuw)
- MashedUp2011 (nieuw)
- Heilig rmmstnmix (nieuw, speciaal voor de Rammstein liefhebbers)

Handig

opgeletopinternet.nl

Actuele phishingmails:

klik hier

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

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

Computerwoordenboek

POLITIE Meldpunt internetoplichting

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

MARKTPLAATS: "Wat moet ik doen als ik denk dat ik ben opgelicht?"

Antwoord

1. Wanneer u vooraf betaalt, maar de verkoper het product vervolgens niet levert, adviseren wij het volgende:

Neem eerst nogmaals contact op met de verkoper. Mogelijk is er sprake van een misverstand of wordt het product alsnog geleverd.
Breng in geval van oplichting altijd de Politie op de hoogte (dit kunnen wij niet voor u doen). Zij hebben immers de kennis, expertise en opsporingsbevoegdheden om onderzoek te doen naar strafbare feiten. Wij adviseren u om aangifte te doen bij het Meldpunt Internetoplichting van de Politie via www.mijnpolitie.nl (formulier Melding Internetoplichting).
Wij adviseren u om het formulier zo accuraat en volledig mogelijk in te vullen.
Zorg dat u, wanneer u aangifte gaat doen, alle relevante gegevens bij de hand heeft zoals:

- Uw eigen (contact)gegevens, inclusief uw Burgerservicenummer (BSN).
- De (contact)gegevens van de partij met wie u heeft gehandeld (zoals naam en bankrekeningnummer).
- De gegevens van de transactie, zoals het advertentienummer en de onderlinge communicatie.

Meld oplichting ook altijd aan Marktplaats. Wij nemen dergelijke meldingen zeer serieus en nemen waar mogelijk gerichte maatregelen. Indien u aangifte doet via het formulier Melding Internetoplichting op www.mijnpolitie.nl wordt direct een deel van de informatie die u daar heeft verstrekt door het Meldpunt Internetoplichting aan Marktplaats doorgestuurd.

Cybercrime wetsartikelen

Wetsartikelen voor computercriminaliteit in enge zin

(ruime zin: algehele benamingen / enge zin: specifieke verschijningsvormen)

Voor cybercrime in enge zin zijn de volgende wetsartikelen beschikbaar:

. Artikel 138a WvSr: het binnendringen in een geautomatiseerd werk.

. Artikel 161 sexies WvSr: opzettelijk veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk of werk voor de telecommunicatie.

. Artikel 161 septies WvSr: stoornis in de gang of in de werking in een geautomatiseerd werk of werk voor telecommunicatie door schuld.

. Artikel 350a WvSr: het opzettelijk onbruikbaar maken en veranderen van gegevens.

. Artikel 350b WvSr: het onbruikbaar maken en veranderen van gegevens door schuld,

. Artikel 139c WvSr: het aftappen en/of opnemen van gegevens en

Artikel 139d WvSr: het plaatsen van opname-, aftap- c.q. afluisterapparatuur.

Er zijn geen specifieke wetsartikelen om cybercrime in ruime zin aan te duiden. Voor de hoofddaad worden dezelfde wetsartikelen gebruikt als wanneer de criminele daad niet met ICT zou worden gepleegd.

————————————————————

Haatzaaien.

'Het zaaien van haat of het (opzettelijk) beledigen of discrimineren van een groep mensen wegens hun ras, hun godsdienst of levensovertuiging, hun hetero- of homoseksuele gerichtheid of hun lichamelijke, psychische of verstandelijke handicap, zonder een bijdrage te leveren aan het publieke debat, waarbij ICT essentieel is voor de uitvoering' .

Haatzaaien staat niet als zodanig in het wetboek.

Aan de hand van de geformuleerde definitie kunnen echter de volgende wetsartikelen worden onderscheiden die delicten omschrijven welke vallen onder deze noemer:

- Artikel 147 WvSr: godslastering
- Artikel 90quater WvSr: discriminatie.
- Artikel 137d WvSr: aanzetting tot discriminatie van een bevolkingsgroep.
- . Artikel 137e WvSr: openbaarmaking discriminerende uitlatingen.
- . Artikel 137f WvSr: deelname of steunen van discriminatie.
- . Artikel 137g WvSr: discriminatie in ambt, beroep of bedrijf.
- . Artikel 131 WvSr: opruiing.

————————————————————

Cyberstalking.

'Cyberstalking' is de verzamelnaam voor het stelselmatig lastigvallen van een persoon doorprovocerende uitspraken te doen en/of berichten te plaatsen via online forums, bulletin boards en chatrooms, of de ander als het ware via spyware te bespioneren dan wel voortdurend ongevraagd e-mail en spam te sturen. Er is sprake van een verregaande inbreuk op de privacy van het slachtoffer' .

Relevante wetsartikelen zijn:

Artikel 285b WvSr: belaging.

Artikel 138a WvSr: computervredebreuk.

Artikel 266 WvSr: belediging.

————————————————————

Grooming.

Grooming wordt door het particuliere Meldpunt Kinderpornografie op Internet (MKI) opgevat als het zich op internet anders voordoen (door een volwassene) met het doel om seksueel getinte contacten te leggen met kinderen. Deze contacten kunnen zowel virtueel (seksuele handelingen voor de webcam) als fysiek (een ontmoeting waarbij het kind daadwerkelijk seksueel misbruikt wordt) zijn . Op dit moment is grooming niet strafbaar.

Grooming is echter wel opgenomen in het door Nederland ondertekende, maar nog niet door Nederland geratificeerde EU-verdrag van Lanzarote van 25 oktober 2007, artikel 23 ('Solicitation of children for sexual purposes'), waarin landen zich verplichten om grooming strafbaar te stellen. Grooming is dan het door een volwassene via ICT leggen van contactenmet een jongere met de intentie deze te ontmoeten voor het verrichten van seksuele handelingen, gevolgd door het feitelijk geven van uitvoering aan het tot stand brengen van die ontmoeting. Dat is een aanzienlijk engere uitleg dan het MKI geeft, vooral omdat volgens het verdrag begonnen moet zijn met het realiseren van de ontmoeting ('material acts leading to such a meeting').

————————————————————

Handel in mensen of foute goederen.

Verschijningsvormen:

drugs, geneesmiddelen, vuurwapens en explosieven, mensenhandel- en smokkel, heling.

Kenmerkend bij deze vormen van cybercrime is dat de handel plaatsvindt op of middels ICT

(bijvoorbeeld marktplaats) en dat de betrokken partijen weten dat het gaat om illegale handel.

Relevante artikelen zijn:

Artikel 273a WvSr mensenhandel.

Artikel 416 WvSr opzetheling.

Artikel 417 WvSr opzetheling (gewoonte).

Artikel 274 WvSr slavenhandel.

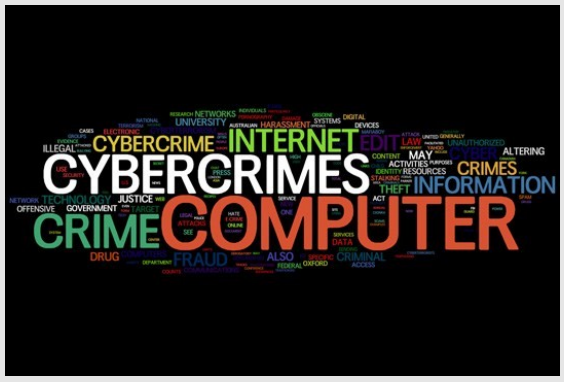
Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



Bij piraterij gaat het feitelijk om illegale handel van allerhande 'cd's, dvd's, films, software en andere producten waarvoor auteursrechten gelden' . De nadruk ligt volgens het KLPD veelal bij eindgebruikers, internetpiraten en vervalsers, en in mindere mate bij gebruikers van licenties (bijvoorbeeld bedrijven) en computerverkopers. In alle gevallen is piraterij echter strafbaar en valt het onder meer onder het Wetboek van Strafrecht, de Auteurswet en de Merkenwet.

Relevante artikelen uit het wetboek van strafrecht zijn:

- Artikel 337 WvSr: handel goederen vervalste merken.
- Artikel 328 WvSr: oneerlijke mededinging.
- Artikel 441a WvSr: heling.
- Artikel 1 AW: auteurswet
- Artikel 31 AW: opzettelijk inbreuk op auteursrecht
- Artikel 31a AW: voorwerp met daarop een inbreuk op auteursrecht
- Artikel 31b AW: beroep maken van inbreuk op auteursrecht

————————————————————————————————-

Kinderpornografie.

Kinderpornografie is in Nederland strafbaar gesteld in artikel 240b Wetboek van Strafrecht.

Kinderpornografie is volgens dit artikel iedere afbeelding - of gegevensdrager die een afbeelding bevat - van een seksuele gedraging waarbij iemand, die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar betrokken is'. Zowel het verspreiden, tentoonstellen, vervaardigen, invoeren, doorvoeren, uitvoeren als in bezit hebben ervan is in Nederland strafbaar. In Nederland is het enkel kijken naar kinderpornografie niet strafbaar.

————————————————————————————————-

Illegale kansspelen.

'Volgens de Wet op de kansspelen (Wok) is er in Nederland een verbod op het aanbieden,

propageren en gebruikmaken van kansspelen waarvoor geen vergunning is verleend. Illegale

kansspelen en gokken op het internet (bijvoorbeeld het online casino) is één van de groei-industrieën

op internet' .

Relevante wetsartikelen zijn:

Artikel 1 Wks: wet op de kansspelen

Artikel 1a Wks: piramidespelen

————————————————————————————————--

E-fraude.

'De essentie van fraude is steeds dezelfde: mensen eigenen zich middels bedrog geld of vermogensbestanddelen toe waarop ze geen recht hebben en tasten daardoor de rechten van anderen aan. Er zijn verschillende begrippen in omloop om de cybervorm van fraude te beschrijven, zoals fraude in e-commerce en internetfraude . 'Bij deze vorm van fraude wordt het internet gebruikt om op oneigenlijke wijze gelden, goederen en diensten te verkrijgen zonder daarvoor te betalen of tegenprestaties te leveren' .

Bij internetfraude wordt er al snel gedacht aan oplichtingen via verkoopsites op internet zoals marktplaats en e-bay. Wij gebruiken de term 'e-fraude' als overkoepelende term. E-fraude is bedrog met als oogmerk het behalen van financieel gewin waarbij ICT essentieel is voor de uitvoering. Fraude staat niet als zodanig in de wet genoemd. Relevante wetsartikelen uit het wetboek van strafrecht zijn:

Artikel 326 WvSr: oplichting.

Artikel 225 WvSr: valsheid in geschrifte.

Artikel 231b WvSr: identiteitsfraude

Artikel 310 WvSr: diefstal.

Artikel 321 WvSr: verduistering.

Artikel 416 WvSr: heling.

————————————————————————