



November 2015

JAARGANG 4

Secure

Computing

Meer en meer wordt er gebruik gemaakt van Twitter. Nog geen Twitter account? In dit nummer leest u hoe dit te realiseren. Kunt u tijdens uw vakantie 'uw volgers' op de hoogte houden.

In bijna elk artikel zijn hyperlinks opgenomen. Klik erop en u ziet meer informatie!



Veel lees(r)plezier

(NB: met Ctrl+ scrolwielje kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen.)



[W.Bosgra](#) Taakaccenthouder Digitale Criminaliteit Basisteam Enschede



Snel index

Klik op een link voor snelle toegang tot het artikel.

Om terug te keren naar de snelindex 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, Klikx, Peppermunt.net, PrivacyNieuws, HackInfo, HardwareInfo, Bright, Computerworld. Tweede Kamer

[Bereid je voor op georganiseerde cybermisdaad](#)

[Stijging van fraude met internetbankieren en skimming](#)

[Minister wil geen aparte autoriteit voor internetfraude](#)

[Europol: privacy gaat ten koste van veiligheid](#)

[Google moet persoonsgegevens afstaan aan BREIN](#)

[Wat betekent de 'Safe Harbor'-uitspraak in de praktijk?](#)

[Kamp: toestemming vragen voor 'supercookies' niet zinvol](#)

[Nieuwe malware neemt heel je browser over](#)

[Android beveiligingslek Stagefright 2.0](#)

[Opnieuw lek gevonden in in besturingssysteem Apple](#)

[Ceo-fraudeurs slaan toen via 'reply-to' optie](#)

[Trap niet in de 'vind ik niet leuk knop' oplichterij op Facebook](#)

[Linuxgebruiker kan zonder virusscanner](#)

[Is het neerzetten van een honeypot strafbaar?](#)

[Hoeveelheid Mac-malware blijft zeer beperkt](#)

[Duitse politie waarschuwt voor kinderfoto's op Facebook](#)

[Toename fraude geldautomaten door lowtechcriminelen](#)

[Verplicht internetdiploma voor Nederlandse kinderen](#)

[Maak je systeem veiliger](#)

[Gehackte USB-stick elektrocutteert je computer](#)

[Kijk tip > Mr Robot](#)

[YouTube teach yourself](#)

[Schatkist](#)

[Snapshots](#)

[Cops in Cyberspace](#)

[Handig](#)

[Wetsartikelen](#)

Een nieuwe post van beveiligingsblogger Brian Krebs richt zich op een groeiende trend in de cybercriminaliteit: samenwerking.

Bereid je voor op georganiseerde cybermisdad

Op de 'normale' georganiseerde misdaad lijkt het allemaal nog niet direct, waarbij lokale groepen een lokale onderwereld domineren, maar een wereldwijd platform waar criminelen hun vaardigheden kunnen delen kan vele malen gevaarlijker zijn.

Enigma

De post richt zich op het nu overleden Enigma hacking forum, dat dient als een goed voorbeeld van de soorten activiteiten waar Krebs voor waarschuwt. Het forum stelde aanstaande hackers in staat om een specifiek detail te plaatsen van de aanval die ze van plan waren uit te voeren – bijvoorbeeld omdat ze door de beveiliging van een bepaald merk en type router moeten komen. Als er in de userbase van het forum iemand met de vereiste vaardigheden, toegang, of connecties aanwezig is, is ad-hoc het cybercriminelenteam daar.

Elke sub-stap in een geslaagde hack kan dus à la carte geassembleerd worden, en wel lands- en socio-economische grenzen overstijgend. En met de onpersoonlijke en verspreide aard van dergelijke fora, kan een Chinese hacker een barrière doorbreken met de hulp van een Italiaanse tiener, die software gekocht heeft van iemand uit Honduras, die draait op een Duitse server.

Dit maakt het niet alleen enorm lastig om cybercriminaliteit te traceren (zowel voordat de misdaad plaatsvindt als daarna), maar betekent ook dat een grote proportie van de aanvallers toegang heeft tot een volledig spectrum van personeel om veilig een klus te klaren. En dat betekent weer meer ondernomen pogingen, en dus absoluut gezien meer succesvolle kraken.

The Samurai

Deze wereld is de moeite waard voor iedereen die in de schaduw werkt – crimineel of anders. Krebs vertelt het verhaal van een Enigma gebruiker die bekend stond als The Samurai, waarvan men nu denkt dat het een Chinese overheidsagent was. The Samurai was geïnteresseerd in het kopen van grote hoeveelheden gestolen informatie – elke informatie – en hij zou direct betalen zonder te zeuren over de prijs. In de criminele onderwereld betekent dat dat hij aankopen doet met het geld van iemand anders – zoals bijvoorbeeld die van de Volksrepubliek.

Niemand, niet eens de mensen die informatie verkochten aan The Samurai, wist zeker wie hij was. Wat natuurlijk de bedoeling is. Dergelijke markten bieden staten (lees: geheime diensten) de mogelijkheid om hun aanvallen op andere staten uit te besteden aan de aldaar actieve criminelen, waardoor ze zichzelf uitsluiten van gevaar. Een ander hacker forum, The Gentleman's Club, postte de aanval op Ashley Madison drie weken voordat de hack in de kranten verscheen. Gerelateerd of puur toeval?

Weet niemand. Maar naar mate dergelijke hacks steeds vaker het nieuws domineren blijven dergelijke vragen hangen. Kunnen we hackers stoppen, zelfs als ze de kracht van crowd-sourcen aanboren met een goedgevulde portemonnee?



De schade door fraude met internetbankieren en skimming is in de eerste helft van dit jaar gestegen ten opzichte van dezelfde periode in 2014, zo blijkt uit cijfers van de Nederlandse Vereniging van Banken. In de eerste zes maanden van dit jaar werd er voor 3,1 miljoen euro via internetbankieren gefraudeerd.

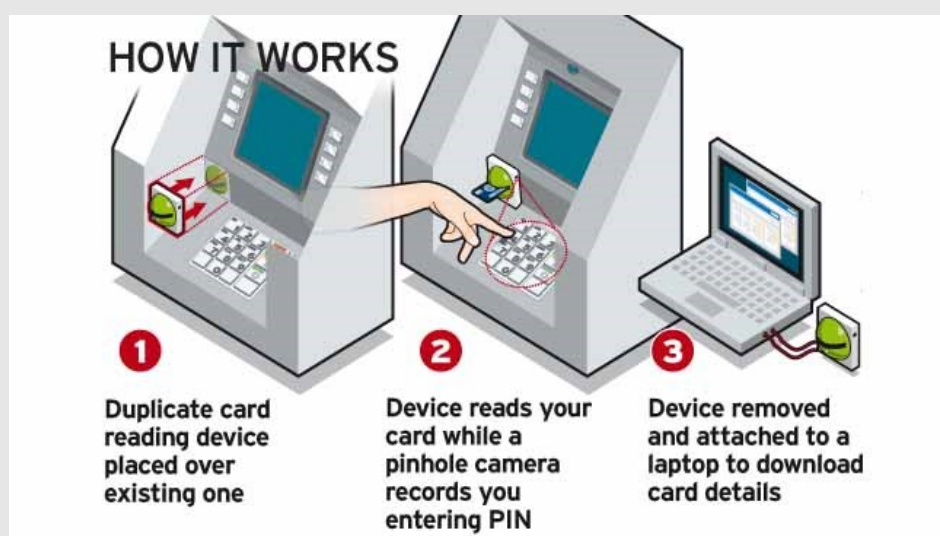
Stijging van fraude met internetbankieren en skimming

In de eerste helft van 2014 bedroeg de schade door fraude met internetbankieren nog 2,1 miljoen euro. Volgens de Nederlandse Vereniging van Banken (NVB) is de stijging te verklaren doordat criminelen hun phishingmethodes "perfectioneren". Phishing veroorzaakt nog altijd de meeste schade. Op deze manier werd in de eerste zes maanden van dit jaar 2,8 miljoen euro gestolen. Een jaar eerder was dat nog 1,7 miljoen euro. Via malware wisten criminelen dit jaar 300.000 euro te stelen. Een daling ten opzichte van de eerste helft van 2014, toen er op deze manier 380.000 euro werd buitgemaakt.

"Doordat phishingmails er steeds professioneler uitzien en minder taalfouten bevatten zijn ze minder makkelijk te herkennen. Ook spelen criminelen vaak handig in op de actualiteit door bijvoorbeeld gebruik te maken van de introductie van nieuwe betaalpassen. In telefoongesprekken waarin criminelen zich voor doen als bankmedewerker wordt vooral geprobeerd om de klant in paniek te brengen zodat ze hun inlogcodes afgeven", aldus de NVB.

Skimming

Ook de schade door skimming steeg in de eerste helft van dit jaar. Het ging om een schadepost van 790.000 euro. Een jaar eerder was dit nog 640.000 euro. Volgens de NVB komt schade als gevolg van skimmen in Nederland nagenoeg niet meer voor. De schade werd vooral veroorzaakt doordat passen buiten Europa werden geskimd terwijl geoblocking was uitgezet. Geoblocking voorkomt dat er buiten Europa met een pinpas kan worden gepind.



Minister Van der Steur van Veiligheid en Justitie wil geen aparte autoriteit voor internetfraude in het leven roepen, zo heeft de minister tijdens het vragenuurtje in de Kamer laten weten. Volgens SP-Kamerlid Gesthuizen wordt er bij de bestrijding van internetfraude te weinig samengewerkt.



Minister wil geen aparte autoriteit voor internetfraude

Vragen van het lid Gesthuizen aan de minister van Veiligheid en Justitie over het bericht "Slachtoffers van internetfraude krijgen weinig hulp".

Mevrouw Gesthuizen (SP):

Voorzitter. Dat internet een zegening is voor heel veel zaken, bijvoorbeeld door een snelle, efficiënte en gemakkelijke manier van werken, weten we wel, maar helaas zijn er ook voorbeelden te over van bedrog en oplichting. Dat vindt door internet ook een stuk gemakkelijker plaats, en daar spinnen criminelen goed garen bij. Ik noem een valse identiteit om mensen op te lichten, het voorbeeld van de NOS van vandaag, en de nepwebsites waarop mensen niet zo moeilijk producten kunnen bestellen en ook betalen, die vervolgens uit de lucht zijn en waar je dus helemaal geen product blijkt te hebben aangeschaft. En dan is er natuurlijk ook datingfraude, een van de meest schrijnende voorbeelden van fraude via internet die ik ken, heel erg schadelijk voor mensen als ze daarmee geconfronteerd worden en ermee te maken krijgen. Het probleem is langer bekend. We hebben het hier in de Kamer al verschillende keren vanuit verschillende fracties met nadruk aangekaart. Toch is het nog niet opgelost. Hoe kan dat?

In mijn ogen zijn er drie oplossingen: beter samenwerken, meer samenwerken en sneller samenwerken. Deelt de minister deze visie en wat gaat hij doen om dat te bespoedigen? Volgens de Fraudehelpdesk, de specialist, de autoriteit mag ik wel zeggen, op het gebied van fraudebestrijding in Nederland en het helpen van mensen die slachtoffers zijn geworden van allerlei vormen van fraude, is het probleem dat overheid en bedrijfsleven nog onvoldoende samenwerken. Bedrijven geven bovendien te vaak te weinig gehoor aan de verzoeken van burgers. Volgens de Fraudehelpdesk is dan ook een waakhond nodig die toeziet op de aanpak van fraude. Ik herhaal hier mijn eerdere pleidooi: we hebben in dit land een fraudeautoriteit met doorzettingsmacht nodig. Ik hoor hierop graag de reactie van de minister. Ik wil bij deze gelegenheid ook meteen de Kamer aansporen om te zeggen dat zij graag een fraudeautoriteit wil. De ontwikkelingen gaan snel, de criminelen spinnen er goed garen bij,

maar de burgers zijn het slachtoffer.

Minister Van der Steur:

Voorzitter. Mevrouw Gesthuizen zegt het terecht: internet is een zegening voor heel veel mensen, dag in dag uit, maar het is ontegenzeggelijk zo dat internet nu en zonder enige twijfel in de toekomst ook een zegening zal blijken te zijn voor allerlei vormen van criminaliteit. Dat is nu al het geval en dat zal in de toekomst zeker ook zo zijn. Dit is iets waar politie, justitie en Openbaar Ministerie zich van bewust zijn en waar zij in hun samenwerking ook actief aan werken. Dat is onder andere het geval in de herijking van de Nationale Politie, waarbij dit een van de thema's.

Mevrouw Gesthuizen zegt terecht dat datingfraude ook een zwaarwegend probleem is. Gisteren heb ik hier uitgebreid met de hele datingbranche over gesproken, ook samen met de Fraudehelpdesk. De Fraudehelpdesk speelt overigens een cruciale rol op dit gebied, maar ook instellingen als het Landelijk Meldpunt Internetoplichting en, voor zover het identiteitsfraude betreft waar het schrijnende geval bij de NOS over ging, het Centraal Meldpunt Identiteitsfraude en -fouten van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, die overigens ook een rol vervullen bij de persoonlijke begeleiding van slachtoffers.

Internetfraude in al zijn vormen en gedaantes is iets waar actief aan gewerkt wordt. We zijn ons er zeer van bewust dat daar de komende jaren nog veel meer aan gewerkt zal moeten worden. Ik deel de analyse van mevrouw Gesthuizen dat er beter, meer en sneller moet worden samenwerkt. Op dat punt ondersteun ik ook het pleidooi van de Fraudehelpdesk. Mevrouw Gesthuizen heeft gevraagd of ik maar even kan melden wanneer het is opgelost, maar op dit punt moet ik realistisch zijn. We bevinden ons nog maar aan het begin van het probleem van fraude en criminaliteit via internet. Dat is ook de reden waarom wij het cybercrime-instituut hebben. Wij zijn ons er evenwel zeer van bewust dat wij er hard aan moeten werken.

Het kabinet heeft al meermalen gezegd dat het een fraudeautoriteit, waar mevrouw Gesthuizen tot slot naar vroeg, geen goed idee vindt. Daar

hebben wij de Ministeriële Commissie Fraudebestrijding voor waar ik de coördinerend minister van ben, en waarmee we al ontzettend veel activiteiten hebben ondernomen en nog zullen ondernemen om fraude integraal aan te pakken.

Mevrouw Gesthuizen (SP):

Als het zo mooi was dat de ministeriële commissie dit allemaal aankon, stonden wij hier niet. Het is ook echt niet zo dat ik dit vanochtend, toen ik wakker werd en mijn telefoon aanswitchte, voor het eerst op mijn netvlies kreeg. Nee, dit is een probleem dat wij al jaren kennen en waarvan wij eigenlijk allemaal vinden dat het veel meer prioriteit verdient. Daarom zijn er ook verschillende initiatieven vanuit de Kamer en daarom bevragen we de minister iedere keer op dit punt.

Als de minister samen met de sector bezig is met mooie plannen — hij zei ook dat hij in professionele zin met de datingbureaus heeft gesproken — waar ligt dan uiteindelijk de uitvoering van de plannen die de minister nu opstelt? Wie heeft er op dit terrein nu doorzettingsmacht? Gaat de minister dit persoonlijk allemaal doen? Gaat de minister tegen dit soort organisaties zeggen dat zij iedere week bij hem moeten komen rapporteren? Ik zie dat niet gebeuren, omdat deze minister hartstikke druk is met de Nationale Politie, de cao voor agenten en heel veel andere zaken. De kennis en de expertise zijn er bij de Fraudehelpdesk, bij het Openbaar Ministerie en bij de politie. Het enige wat die organisaties aangeven, is dat zij veel beter samen moeten werken. Ik zou het zo fantastisch vinden als we de kennis en expertise die wij in dit land wél hebben, zouden kunnen bundelen, de minister daarmee een beetje zouden kunnen ontlasten en zouden zeggen: er komt gewoon naar het goede voorbeeld op het terrein van cybercrime — daar hebben we het NCSC — ook een fraudeautoriteit met doorzettingsmacht, die ervoor zorgt dat dit niet onderop de stapel verdwijnt.

Minister Van der Steur:

Een groot deel van het werk dat mevrouw Gesthuizen beschrijft, is natuurlijk gedaan door het burgerinitiatief 1Overheid. Daar heb ik anderhalve week geleden samen met burgemeester Van der Laan een hele avond aan gewerkt, in combinatie met de politie, het Openbaar Ministerie en een heleboel vertegenwoordigers van departementen. 1Overheid vroeg ook of er een fraudeautoriteit kan worden ingericht. Toen hebben wij gezegd: luister eens even, de beste autoriteiten die wij in Nederland hebben, met doorzettingsmacht, zijn de ministers zelf. Ik heb als coördinerend minister dan ook de taak op mij genomen — althans, dat heeft mijn voorganger gedaan — om daarop te wijzen. Dat is en blijft een verstandig idee. Er is zeker sprake van intensivering van samenwerking tussen de banken, de politie en het Openbaar Ministerie, ook inzake de aanpak van internetoplichting. In de bijeenkomst van gisteren over datingfraude is dat aspect van de banken aan de orde gekomen, maar ook het aspect van "notice and takedown" van malafide datingsites die echt alleen maar zijn opgericht om misbruik te maken van goedgelovige mensen. Daar gaan wij samen met de branche concrete stappen in zetten, juist omdat wij heel goed beseffen dat er nog veel meer nodig is om effectief op te kunnen treden. Mevrouw Van Gesthuizen kan ervan opaan dat ik de banken zal wijzen op hun verantwoordelijkheid in dit kader, zoals overigens ook het ministerie van BZK de identiteitsfraude al actief heeft opgepakt met een aantal apps, maar ook met het Centraal Meldpunt Identiteitsfraude- en fouten.

Mevrouw Gesthuizen (SP):

Dit is jammer, want we constateren dat we de problemen al een tijd kennen en dat we er niet goed genoeg in slagen om de problemen op te lossen. Bovendien: waar je ook komt, bij welk symposium of welke vergadering met experts dan ook, vanuit het veld — vanuit politie en justitie, maar ook vanuit het bedrijfsleven — komt continu de roep dat zij beter moeten samenwerken. Ik vind het oprecht jammer dat de minister dit signaal niet oppakt, niet door de knieën gaat en niet erkent dat we in Nederland gewoon een soort commissaris, een fraudeautoriteit, moeten hebben die ervoor kan zorgen dat fraude niet meer onderop de stapel komt, maar echt prioriteit krijgt.

Minister Van der Steur:

Ik begrijp het ongeduld van mevrouw Gesthuizen heel goed. Ik denk ook dat dat goed is. De Kamer heeft dat ongeduld al heel lang. Dat ongeduld is goed geweest en blijft ook goed, omdat je daarmee ook als bewindspersoon weer een stimulans krijgt om op dit punt door te blijven pakken. Dat doen wij op allerlei terreinen. Ik kan hier hele lijsten geven van alle mogelijke manieren waarop niet alleen internetfraude maar ook fraude in de relatie tussen overheid, de verticale fraude en ook de horizontale fraude effectief worden aangepakt. Er kunnen absoluut nog betere stappen worden gezet. Mevrouw Gesthuizen heeft het niet gezegd, **maar een van de heikele punten is dat, als mensen niet uitkomen bij het Meldpunt Internetoplichting en zich melden bij een individueel politiebureau, men daar denkt dat het gaat om een civiele kwestie en dat aangifte niet nodig is. Dat zijn typisch stappen waarvan ik ook als minister vind dat wij op die punten krachtig moeten doorpakken. Ik zal de politie er nog eens op wijzen dat aangifte doen essentieel is om ook banken bijvoorbeeld te kunnen bewegen om bankrekeningen af te sluiten en dat soort zaken.**



Het recht op privacy wint steeds meer terrein maar dat gaat ten koste van het recht op bescherming, zo waarschuwt de Europese politiedienst Europol. Europol wijst als voorbeeld naar de bewaarplicht van internetcommunicatie en de recente discussies over encryptie.

Europol: privacy gaat ten koste van veiligheid

"De onthullingen over elektronische massasurveillance hebben de balans verschoven naar de maximale bescherming van het individu tegen elke inmenging van de overheid op zijn privacy", zo staat in het rapport vermeld. Dit heeft volgens Europol als gevolg dat het steeds lastiger voor opsporingsdiensten wordt om burgers tegen de schending van hun privacy door hacking, diefstal van gevoelige gegevens of andere vormen van cybercrime te beschermen.

Elk bewijsspoor van dergelijke criminele activiteiten wordt waarschijnlijk niet opgeslagen en als het al wordt bewaard is het door steeds sterkere encryptie lastig te benaderen, aldus Europol. "Het kan lijken alsof deze rechten worden verward, en daarom is het belangrijk om Artikel 12 van de Universele Verklaring van de Rechten van de Mens te citeren", zo laat de politiedienst weten. Dit Artikel stelt dat niemand zal worden onderworpen aan "willekeurige inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam."

Essentieel verschil

[Europol](#) stelt dat er een essentieel verschil is tussen hackers die de privacy van burgers schenden om misdrijven te begaan ten opzichte van de bevoegdheden van opsporingsdiensten om rechtmatige toegang tot de communicatiegegevens en inhoud van de communicatie van de hacker in relatie met het misdrijf te krijgen, wat door het woord "willekeurig" in Artikel 12 wordt omschreven.

Daarbij is het aan de wetgever om ervoor te zorgen dat er duidelijke voorwaarden zijn die omschrijven wanneer de privacy van verdachten geschonden mag worden en dat dit ook wordt gecontroleerd. "Het uitsluiten van opsporingsdiensten zodat er in geen enkel geval toegang kan worden verkregen zal niet helpen om de privacy van burgers te beschermen en zal op de lange termijn geen stand houden", zo waarschuwt Europol.



Google moet aan stichting BREIN de persoonsgegevens leveren van iemand die illegaal e-books verkocht via Google Play. Dat heeft de Haagse kortgedingrechter bepaald in een kort geding dat BREIN tegen de internetgigant had aangespannen.

Google moet persoonsgegevens afstaan aan BREIN

Volgens de rechter heeft de stichting aangetoond dat er inderdaad sprake is van inbreuk op de auteursrechten door de verkoop van e-books van onder meer Harry Mulisch, John Grisham en Tommy Wieringa tegen een prijs van 2,21 euro. Op grond van de auteurswet heeft de kortgedingrechter bevolen dat Google de persoons- en adresgegevens van de houder van het betreffende Google Play-account waarmee de e-books werden verkocht moet afstaan.

Grondrechten

Bij de beslissing zegt de rechter de grondrechten van de betrokken partijen tegen elkaar te hebben afgewogen. Aan de ene kant het recht op bescherming van eigendom van de bij [stichting BREIN](#) aangesloten auteurs en het tegengaan van inbreuken op rechten van intellectueel eigendom. Aan de andere kant keek de rechter naar het recht van Google op vrij ondernemerschap en van de accounthouder op vrije meningsuiting, waaronder het belang om anonimiteit te blijven en het recht op privacy van de persoonlijke levenssfeer.

Volgens de rechter heeft BREIN een reëel belang bij het verkrijgen van de persoonsgegevens, zodat het de geschonden auteursrechten van haar leden kan handhaven. De rechter oordeelde dat Google voor BREIN het enige aanknopingspunt is om deze houder te achterhalen. De rechten van de accounthouder spelen daarbij een minder belangrijkere rol, alsmede die van Google. "De inbreuk op de vrijheid van ondernemerschap van Google is minimaal: zij hoeft enkel de gegevens ter beschikking te stellen die zij op dit moment nog heeft", aldus de rechter.



Privacyvoorvechters zijn blij met een uitspraak van het Europees Hof van Justitie, waarin staat dat Amerika niet genoeg doet om de privacy van Europese burgers te beschermen. De zogenoemde 'Facebook-zaak' is een overwinnig voor internetgebruikers op de NSA, maar wat betekent de uitspraak nou in de praktijk?

Wat betekent de 'Safe Harbor'-uitspraak in de praktijk?

Wat is er precies uitgesproken?

Het Europees Hof van Justitie heeft gezegd dat 'internetbedrijven zoals Facebook' geen data van Europese burgers mogen opslaan op Amerikaanse servers. Dat mocht altijd wel, door het zogenaamde 'safe harbor'-verdrag ('veilige haven'). Dat is een afspraak tussen Amerika en Europa, waarin staat dat bedrijven gegevens van gebruikers mogen opslaan op servers op elkaars grondgebied. Dat mag, zolang het de Europese wetgeving respecteert.

Amerika respecteert die Europese gegevens echter niet goed genoeg. Naar aanleiding van de onthullingen over de NSA zegt de rechter dat het duidelijk is dat Amerika niet genoeg doet om de privacy van burgers te beschermen.

Dat betekent in de praktijk dat Amerikaanse bedrijven zoals Facebook en Google geen gegevens mogen opslaan in Amerika.

Wat ga ik hiervan merken?

Waarschijnlijk niets. Voor eindgebruikers maakt de nieuwe uitspraak weinig uit, het zijn vooral de bedrijven zelf die zich moeten houden aan de nieuwe uitspraken.

In de praktijk betekent het dat het een klein beetje anoniemer is geworden om op internet te gaan. In dit specifieke geval mag Facebook geen gegevens over je opslaan op Amerikaanse servers. Facebook maakt een profiel van gebruikers op basis van hun 'likes' en welke pagina's ze bezoeken.

Wat de uitspraak precies betekent voor bedrijven, is echter nog niet helemaal duidelijk. Die moeten nu een andere manier vinden om gegevens van Europese gebruikers op te slaan op Amerikaanse servers. Waarschijnlijk komt dat erop na dat zij hun gegevens moeten opslaan in Europa, en daarmee aan Europese wetgeving moeten voldoen.

Europese wetgeving zegt onder andere dat nationale Europese privacy-waakhonden (zoals het Nederlandse CBP) hun eigen onderzoek mogen instellen naar het opslaan van gegevens van Facebook of Google.



Dus ik kan weer rustig al m'n gevoelige data op Google Drive zetten?

Niet helemaal. Het is namelijk niet zo dat de NSA nu helemaal niets meer mag opzoeken van Europese burgers. Sterker nog, de meeste af luisterpraktijken blijven gewoon bestaan onder oudere modellen. Zo kan de NSA nog steeds kabels aftappen en meta-data opslaan van emailverkeer.

Bovendien kunnen bedrijven afspraken maken met nationale toezichthouders, waardoor er alsnog dataverkeer naar Amerika mag worden doorgesluisd. Hoe dat echter precies werkt en vorm krijgt, is nu nog niet bekend.

Wat betekent de uitspraak dan wel?

De uitspraak zorgt ervoor dat burgers meer rechten hebben als het om hun persoonlijke gegevens gaat. Zo kunnen ze makkelijker een klacht indienen bij bijvoorbeeld het College Bescherming Persoonsgegevens, de Nederlandse privacy-waakhond. Het CBP mag in zo'n geval zelfs verbieden dat profielinformatie mag worden opgeslagen op Amerikaanse servers.

Het CBP moet daarbij echter per bedrijf bekijken of het voldoet aan de Nederlandse privacywetgeving. Het is dus nog helemaal niet 100% zeker dat Facebook ook van Nederlanders te veel opslaat. Daar moet eerst onderzoek naar worden gedaan.

Ook kunnen burgers nu bijvoorbeeld een verzoek doen om inzage te krijgen in welke gegevens de NSA precies van hen opslaat. Dat is echter makkelijker gezegd dan gedaan, want zo'n verzoek zou waarschijnlijk jaren duren en juridisch ontzettend complex zijn.

Waar komt deze uitspraak ineens vandaan?

De uitspraak komt uit een rechtszaak die een Oostenrijker had aangespannen tegen Facebook. De privacy-activist Maximillian Schrems vond dat de onthullingen van Edward Snowden genoeg hadden aangetoond dat zijn persoonlijke gegevens niet veilig zijn bij Facebook, omdat ze daar worden doorgesluisd naar de Amerikaanse opsporingsdiensten als de NSA. Schrems klaagde Facebook aan in Ierland, maar de rechtszaak liep door tot het Europees Hof van Justitie, de hoogst mogelijke gerechtelijke macht.

Minister Kamp ziet er niets in om een systeem te laten ontwikkelen dat internetgebruikers vraagt of ze zogeheten 'supercookies' willen accepteren.

Kamp: toestemming vragen voor 'supercookies' niet zinvol

Dat liet Kamp weten op Kamervragen van PvdA-Kamerlid Oosenbrug. Ze had de minister vragen gesteld vanwege onderzoek waaruit zou blijken dat Vodafone trackingheaders in het verkeer van klanten injecteert. Deze headers worden ook wel supercookies genoemd.

Kamp stelt als eerste dat de term 'supercookie' verwarrend is, aangezien er geen informatie op het toestel van de eindgebruiker wordt geplaatst of gelezen, zoals bij cookies wel het geval is. In plaats daarvan is er sprake van ASID-headers. ASID staat voor Anonymous Subscriber Identification. Bij het gebruik van ASID-headers stuurt de internetprovider een identificerende code mee met de data die een eindgebruiker verstuurt bij het bezoeken van een website.

Als ASID-headers worden gebruikt om eindgebruikers te identificeren, is er sprake van verwerking van persoonsgegevens. Daarop is de Wet bescherming persoonsgegevens (Wbp) van toepassing, aldus Kamp. Aangezien erbij het meesturen van ASID-headers geen informatie op het toestel van de eindgebruiker wordt geplaatst of gelezen is de cookiewet, onderdeel van de Telecommunicatiewet, hierop niet van toepassing.

Toestemming

Volgens Kamp kan een ASID-header bijvoorbeeld worden gebruikt om veilig internetbankieren via een mobiel netwerk mogelijk te maken. Het is dan denkbaar dat het meesturen van een ASID-header noodzakelijk is voor de uitvoering van een overeenkomst waarbij de gebruiker deel van uitmaakt. "Als er geen noodzaak is een ASID-header mee te sturen voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, dan zal er meestal ondubbelzinnige toestemming van de betrokkene vereist zijn", zo laat de minister weten.

Oosenbrug wilde ook weten in hoeverre telecomaanhouders die supercookies gebruiken daarmee informatie kunnen verzamelen waarmee de privacy van hun klanten kan worden geschonden en wat klanten hier tegen kunnen doen. Kamp stelt dat dit meestal betekent dat er toestemming is vereist voor het verwerken van de (persoons) gegevens. Een internetgebruiker kan een eventuele schending door de aanbieder niet voorkomen, maar wel een klacht indienen bij de toezichthouders als hij misbruik vermoedt.

Kamp ziet er dan ook niets in om een systeem te ontwikkelen waarbij internetgebruikers apart toestemming voor het gebruik van supercookies moeten geven. "Het is primair de verantwoordelijkheid van de aanbieder te beoordelen of hij toestemming moet vragen of een beroep kan doen op een andere grondslag voor de verwerking van persoonsgegevens. Maakt hij daarbij een verkeerde beoordeling dan kan door de toezichthouder daartegen worden opgetreden. Het lijkt niet zinvol een systeem in te voeren waarbij de internetter ook om toestemming wordt gevraagd in situaties waarbij daar geen enkele reden toe is."



Chrome is zo goed geworden in het buiten houden van malware, dat hackers drastischere maatregelen hebben moeten treffen.

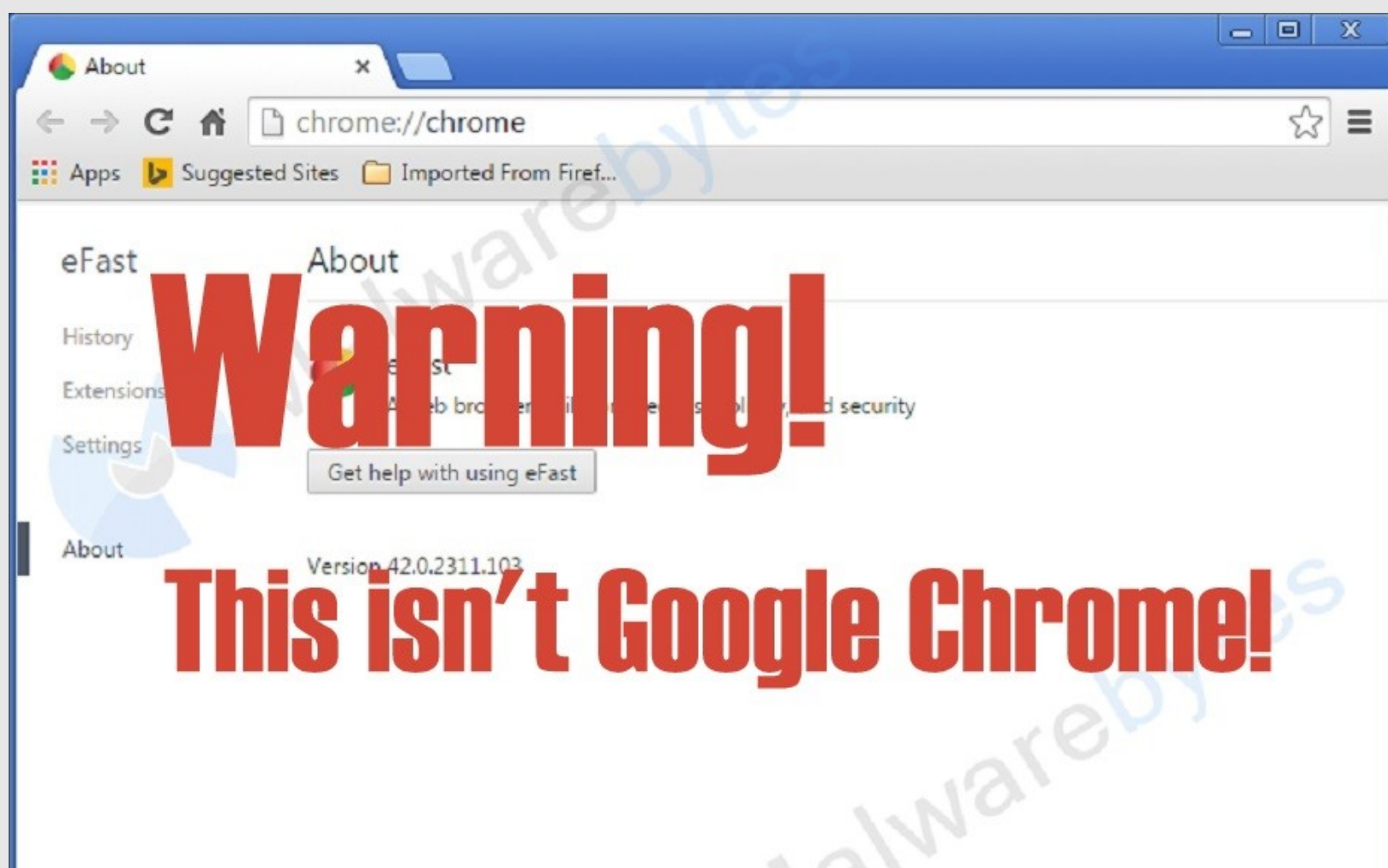


Nieuwe malware neemt heel je browser over

Sinds het ontstaan van het internet zijn er steeds mensen geweest die misbruik willen maken van goedgebouwde surfers. Met behulp van pop-ups en andere technieken proberen cybercriminelen onschuldige gebruikers naar sites vol met malware te lokken. Eenmaal je in de val bent gelopen, is het vaak erg moeilijk om je toestel terug volledig virusvrij te krijgen.

Gelukkig slagen browsers er steeds beter in dergelijke praktijken te voorkomen. Te goed zelfs, want een nieuwe vorm van malware vervangt Chrome volledig met een gehackte versie van de browser. De zogenaamde eFast Browser probeert Chrome van je toestel te verwijderen en deze volledig te vervangen. De software van de valse browser is gebaseerd op Chromium, waardoor het venster en de werking van eFast erg veel lijken op de echte Chrome. Deze browser zal echter proberen zoveel mogelijk links en standaardprogramma's over te nemen.

De eFast Browser wordt verspreid via het installatiemenu van gratis software op dubieuze websites. Het zou dus erg eenvoudig moeten zijn te voorkomen dat je de browser installeert. Om te achterhalen of de malwareversie van Chrome zijn weg tot jouw toestel heeft gevonden, dien je in het configuratiescherm naar programma's te gaan. Kies hierna voor standaardprogramma's en uw standaardprogramma's instellen en je zal een lijst met programma's zien verschijnen. Indien er in deze lijst nergens 'eFast' te vinden is, ben je nog steeds de trotste bezitter van de echte Google Chrome. Kan je het programma wel terugvinden in de lijst? Verwijder deze dan via programma's en onderdelen.



Android heeft de afgelopen jaren een aantal enge momenten gekend aangaande de beveiliging. De Stagefright bug was zonder twijfel de grootste. En hoewel er lang en breed patches zijn uitgerold voor de bug, blijkt nu dat er nog een aantal exploits zijn die niet goed worden afgedekt.

Android beveiligingslek Stagefright 2.0

Beveiligingsbedrijf Zimperium heeft een tweede ronde van Stagefright [exploits](#) publiekelijk gemaakt die volgens het bedrijf net zo veel kwetsbaarheden opleveren als de eerste. Het goede nieuws? Google heeft de patches al klaar.

Ondanks de beangstigende naam is Stagefright niet eens de daadwerkelijke naam van **de exploit**. Het refereert naar de multimedia engine library in Android die bekend staat als libstagefright. De nieuwe kwetsbaarheid in Stagefright is vergelijkbaar met de eerste, maar de benaderingshoek is anders. Stagefright 1.0 maakte gebruik van [MMS berichten](#) om een kwaadaardig mediabestand te openen. Die zouden op hun beurt in theorie in staat zijn om willekeurige code uit te voeren op het apparaat. Het nieuwe lek betreft het aanvallen van apparaten via web pagina's die ditzelfde kwaadaardige bestand hosten (een MP3 of MP4). Het effect is hetzelfde – de aanvaller kan code uitvoeren via de Stagefright library op je apparaat.

De nieuwe Stagefright bug bestaat uit twee componenten. Een daarvan is libstagefright. De relevante bug hiervoor is alleen geïntroduceerd in Android 5.0, dus de krantenkoppen die spreken van een miljard besmette apparaten vertellen maar het halve verhaal. Stagefright 2.0 omvat libstagefright die een verwijzing maakt naar een andere map, genaamd libutils, op een kwetsbare manier. Dat is de kern van de exploit. Deze

libutils map bestaat al sinds Android 1.0, dus ieder apparaat heeft deze bug. Het is mogelijk dat andere systeem componenten een vergelijkbare verwijzing kunnen maken naar libutils, dus een patch is hoog nodig. Stagefright 2.0 in zijn huidige vorm is technisch gezien alleen gevaarlijk voor Android 5.0 en hoger.

Google is op de hoogte gesteld van het lek, en heeft een patch ontwikkeld die vandaag wordt uitgerold, met de Nexus update. Dat is ook de update die Android 6.0 naar de Nexus apparaten brengt, dus alle Marshmallow gebruikers hoeven zich geen zorgen te maken. Andere Android gebruikers zullen moeten wachten op fabrikanten en providers; het klassieke Android probleem.

Ondertussen: is er reden voor paniek? Net als bij de eerste Stagefright exploit is er geen bewijs dat het lek ooit is uitgebuit in het wild. Het is belangrijk je te realiseren dat [Stagefright](#) op zichzelf niet schadelijk is, maar slechts potentieel. Een aanvaller heeft nog steeds code nodig die iets doet met het apparaat, zei het data te stelen, of root-toegang te krijgen tot het systeem. Dergelijke exploits zijn zeer moeilijk te ontdekken in Android vandaag de dag.



Apple heeft er altijd voor gezorgd dat we allemaal weten hoe veilig OS X is. In realiteit is het verre van kogelvrij, en onderzoeker Patrick Wardle heeft een nieuwe kink in de kabel weten te slaan.

Opnieuw lek gevonden in in besturingssysteem Apple

Wardle is de CTO van Synack, die er hun werk van hebben gemaakt om [exploits](#) te vinden. Hun laatste richt zich op een kern-beveiligingsfeature in OS X: Gatekeeper. Gatekeeper werd geïntroduceerd in juli 2012 toen OS X Mountain Lion arriveerde (en werd ook naar andere apparaten gepusht). Het was ontworpen om te voorkomen dat onbekende applicaties schade zouden kunnen aanrichten op Macs. Het kan installaties van apps uit de App Store limiteren en selecteert uitsluitend applicaties van vertrouwde ontwikkelaars.

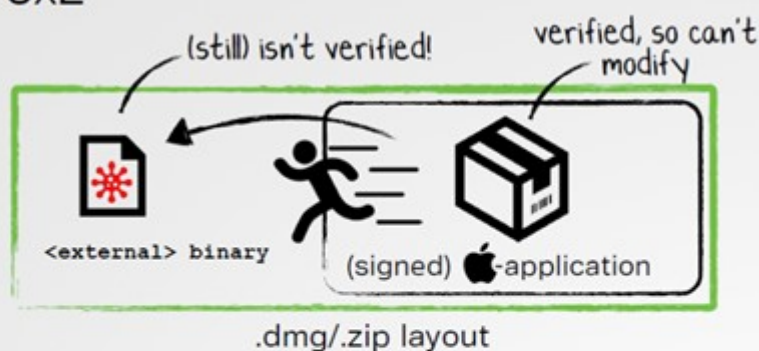
Het een redelijk effectieve manier op kwaad willende apps te weren, maar het is niet perfect. Wardle denkt zelfs dat "Gatekeeper een haperende muur is". Gatekeeper let alleen op tijdens de initiële opstart van een applicatie. Als het heeft rondgekeken en de app het groene licht heeft gegeven, is het klaar. De exploit van Wardle werkt door een externe binary in te brengen bij een getekende applicatie. Deze binary woont buiten het domein van Gatekeeper, en wordt dus ook niet gecontroleerd.

Het is de perfecte manier voor een kwaadwillende app – zoals de Chinese, gemodificeerde versie van Xcode die circuleerde – om een Mac systeem te infecteren. Wardle zegt dat de code niet eens in het pakket van de ondertekende download hoeft te zitten. Een nog geavanceerdere aanval kan deze injecteren wanneer de download via een http adres in gang wordt gezet.

Apple werkt aan een korte termijn oplossing volgens Wardle. Deze wordt zo snel mogelijk geleverd aan gebruikers, terwijl Apple werkt aan een verbeterde Gatekeeper.

GATEKEEPER BYPASS OX2 runtime shenanigans


gatekeeper only **statically**
verifies the app bundle!



- 1 find an signed app that **at runtime**, loads and executes an **external relative** binary
- 2 create a .dmg/.zip with the necessary folder structure (i.e. placing the malicious binary in the **externally** referenced location)
- 3 host online/inject

Synack

Criminelen die zich met ceo-fraude bezighouden, ook bekend als business email compromise, passen verschillende nieuwe tactieken toe om organisaties op te lichten, zoals het gebruik van de 'reply-to' optie.

Ceo-fraudeurs slaan toen via 'reply-to' optie

Criminelen die zich met ceo-fraude bezighouden, ook bekend als business email compromise, passen verschillende nieuwe tactieken toe om organisaties op te lichten, zoals het gebruik van de 'reply-to' optie. Dat claimt beveiligingsbedrijf PhishLabs. Ceo-fraude is een vorm van cybercrime waarbij financiële personen binnen een organisatie een e-mail ontvangen die van de directeur afkomstig lijkt.

In de e-mail wordt gevraagd om met spoed een groot geldbedrag over te maken. Volgens de FBI hebben criminelen op deze manier al 1,2 miljard dollar weten te stelen. Bij de eerste aanvallen gebruikten de criminelen gratis e-maildiensten of gehackte bedrijfsaccounts om de malafide verzoeken te versturen. Nu gebruiken ze gehackte e-mailaccounts van internetbedrijf GoDaddy. Deze accounts zijn namelijk eenvoudig via phishingaanvallen over te nemen, ondersteunen het gebruik van de 'reply-to' optie en de 'identiteits' feature.

Via deze feature kan er eenvoudig als afzender een willekeurig e-mailadres worden opgegeven. De fraudeurs gebruiken deze feature voor het opstellen van een e-mail met als afzender een legitiem adres van de

aangevallen organisatie, zoals het e-mailadres van de directeur.

Vervolgens vullen ze voor het reply-to-adres een e-mailadres in dat in beheer van de criminelen is. De meeste e-mailclients laten alleen de naam zien en verbergen het e-mailadres, waardoor werknemers het reply-to-adres niet meteen zien.

Een andere verandering in werkwijze is dat de eerste e-mail kort en bondig is en verder geen betaaldetails bevat. Bij eerdere aanvallen kreeg de financiële controller meteen het rekeningnummer en over te maken bedrag toegestuurd. Nu wisselen de fraudeurs meerdere e-mails uit voordat de rekeninggegevens worden doorgestuurd. En ook voor de rekening is de tactiek iets veranderd. Werden er eerst buitenlandse rekeningen in bijvoorbeeld China gebruikt, nu zijn het Amerikaanse rekeningen. PhishLabs adviseert organisaties om meer bewustzijn onder het personeel te creëren en spamfilters zo in te stellen dat de frauduleuze e-mails worden geblokkeerd.

```
Received: ... (envelope-from <compromised@somewebmail.com>) ← hidden from user
From: Barry Boss <executive@example.com> ← spoofed using "Identities" feature
To: Aaron Accountant <accounting@example.com> ← actual target
Reply-To: "Barry Boss" <ceo.email@execs.com> ← monitored by scammer
```

In het buitenland komt CEO-fraude al langer voor. De FBI becijferde dat vorig jaar in de Verenigde Staten zeker 1,2 miljard dollar is buitgemaakt met dit soort roofpogingen. In Europa is Frankrijk de koploper. "Daar zijn de afgelopen drie jaar 800 tot 900 gevallen onderzocht en is ruim 300 miljoen euro buitgemaakt."

Nederland leek lang de dans te ontspringen. "We hebben pas in mei ontdekt dat het ook hier speelt", zegt André Vermeulen van de Fraudehelpdesk. "Toen heeft KPMG ons laten weten dat er bij hen een poging is gedaan om 900.000 euro weg te sluizen. Dat schijnt overigens niet gelukt te zijn."

KPMG laat weten dat de poging tot fraude direct is herkend. Het bedrijf heeft er melding van gemaakt.

Vermeulen weet verder dat er een poging is gedaan bij Friesland Campina en een dochteronderneming van een Zweeds bedrijf. "En wij denken dat er nog veel meer bedrijven in Nederland zijn die hiermee te maken hebben."

Toch zijn hier nog niet alle alarmbellen afgegaan. Zo zit Nederland niet in de taskforce voor CEO-fraude bij Europol.

Het is een maatschappelijk probleem. In Frankrijk hebben twee medewerkers die er zijn ingestoken zelfmoord gepleegd.

Kijk ook eens [hier](#) en [hier](#).

In navolging van de aankondiging dat Facebook wel/niet werkt aan een 'niet leuk' knop volgt een golf van cyber oplichting die mikt op personen die hopen op de komst van deze knop.

Trap niet in de 'vind ik niet leuk knop' oplichterij op Facebook

Beveiligingsbedrijf Sophos vond recentelijk een nieuwe golf 'niet leuk' oplichtingen. Een list die al tenminste sinds 2011 de ronde doet. Deze keer claimen de oplichters dat de knop een "invite-only feature" is, waarvoor je iets moet downloaden.

"Als je doorklikt, ontvouwt de oplichterij zich zoals zovele 'je weet dat je dit wil' trucs" schreef Sophos' Paul Ducklin in een blog post. "Om door te gaan moet je de link waarop je hebt geklikt eerst aanraden – in feite, je moet hem actief promoten."

Er wordt nog meer druk toegevoegd doordat de oplichters zeggen dat je nog een beperkte tijd hebt om aan de "deelnamevereisten te voldoen". Dat is inclusief het delen van de link met je vrienden, en hem doorsturen naar vijf groepen waar je deel vanuit maakt.

Of je nou aan de 'voorwaarden' voldoet of niet, je wordt altijd doorgestuurd naar een website die niks te maken heeft met Facebook of een niet-leuk knop. Daar wordt je overgehaald je persoonlijk informatie achter te laten. Een van deze sites is een "wordt snel rijk" zwendel die je 1.419 dollar belooft, en een je vraagt een aantal surveys in te vullen.

"Typisch hebben de oplichters zich ingeschreven als affiliates voor de surveys of software downloads die worden aangeboden, en krijgen ze een klein bedrag wanneer iemand zich inschrijft. Zo verdienen ze hun geld", schreef Ducklin.

Een vuistregel: Als een post van je verwacht dat je hem promoot voordat je eigenlijk weet wat je promoot, doe het dan niet!

Aan het einde van de rit krijgen de mensen die in de 'vind ik niet leuk knop op uitnodiging' zijn getrapt helemaal niet zo'n knop. Omdat het allemaal nep is. Deze bestaat niet.



De hoeveelheid malware voor Linux is nog altijd zeer beperkt, zeker in vergelijking met Windows. Toch kunnen ook Linuxsystemen met malware besmet raken. Daarnaast worden Linuxsystemen vaak in Windowsomgevingen gebruikt en komen zodoende ook met Windowsmalware in aanraking.



Linuxgebruiker kan zonder virusscanner

AV-Test besloot 16 verschillende beveiligingspakketten voor Linux met zowel Linux- als Windowsmalware op een Ubuntu-systeem te testen. De resultaten zijn voor sommige producten ontluisterend, omdat ze 85% van de Windowsmalware doorlaten en tot 75% van de Linuxmalware. Acht van de zestien beveiligingspakketten weten tussen de 99,7% en 99,9% van de 12.000 gebruikte Windowsmalware te detecteren. Alleen Symantec scoort 100%. McAfee en Comodo scoren met respectievelijk 85,1% en 83% een stuk lager. Veel slechter zijn de resultaten van Dr. Web (67,8%), F-Prot (22,1%) en ClamAV (15,3%).

Voor het tweede gedeelte van de test werd er met 900 malware-exemplaren voor Linux getest. Kaspersky weet hierbij als enige alle malware te detecteren, gevolgd door ESET met 99,7%. AVG scoort 99%, gevolgd door de serverversies van Kaspersky en Avast die meer dan 98% van de malware detecteren. Symantec, dat alle Windowsmalware identificeerde, herkent 97,2% van de Linuxmalware. De overige producten scoren minder goed, waarbij ClamAV, McAfee, Comodo en F-Prot onderaan eindigen. De detectiepercentages liggen tussen de 66,1% en 23%.

Linux en malware

De vraag blijft in hoeverre het nodig is voor Linuxgebruikers om een virusscanner te installeren. Volgens AV-Test is het aantal Trojaanse paarden voor Linux de afgelopen tijd toegenomen, maar zijn ze van slechte kwaliteit. Dit komt volgens het testlab omdat aanvallers zich bewust zijn van de goede beveiligingsmaatregelen die Linux biedt. Er wordt dan ook vooral van de onkunde van gebruikers gebruik gemaakt, die bijvoorbeeld door operationele fouten besmet raken.

De meestvoorkomende manier om door Linuxmalware geïnfecteerd te raken komt door het installeren van software of updates via derde partijen, aldus AV-Test. De software vraagt tijdens de installatie om tijdelijke rootrechten. Als de gebruiker dit toestaat zal de software op het systeem worden gemanipuleerd en kunnen aanvallers een backdoor op het systeem plaatsen en kan het onderdeel van een botnet worden.

Volgens AV-Test zijn de meeste Linuxgebruikers ervan overtuigd dat ze één van de veiligste systemen beschikbaar gebruiken. "Deze verklaring klopt inderdaad als je alleen naar het systeem kijkt en de rest buiten beschouwing laat." Onveilige software van derden en gebruikersfouten kunnen er uiteindelijk voor zorgen dat ook een Linuxsysteem, net als met Windows en Mac, met malware besmet raakt.

Uit onderzoek van anti-virusbedrijven blijkt dat er tal van besmette Linuxservers zijn die onderdeel van een botnet uitmaken. Op Linux-gebaseerde botnets blijven vaak ook langer operationeel omdat de servers geen beveiligingssoftware gebruiken, in tegenstelling tot Windowservers waar dit wel het geval is. En als er al wel software is geïnstalleerd zijn dit vaak de verkeerde producten. "In veel Linuxfora worden de gratis producten van Comodo, ClamAV en F-Prot aan thuisgebruikers aanbevolen. Dit is geen goed advies", zo stelt AV-Test.

Uit de test blijkt dat thuisgebruikers beter voor de gratis versies van Sophos of Bitdefender kunnen kiezen. Voor serversystemen is er de gratis scanner van AVG. ESET komt als geheel als beste uit de bus, gevolgd door Symantec en Kaspersky. Voor servers worden Kaspersky, AVG en Avast aanbevolen.

Virusscanner noodzakelijk?

Of Linuxgebruikers een virusscanner moeten installeren ligt uiteindelijk aan hun eigen gedrag. AV-Test stelt dat beveiligingspakketten slechts een tweede verdedigingslinie zijn. De belangrijkste beveiliging is namelijk de gebruiker zelf. Iedereen die zijn systeem up-to-date houdt, geen onnodige poorten openzet, alleen software uit betrouwbare bronnen installeert, voorkomt dat de browser actieve content kan uitvoeren en niet zomaar e-mailbijlagen opent, hoeft zich als het gaat om Linuxmalware geen enkele zorgen te maken, aldus het testlab.

Manufacturer	Product	Detection Rate Windows Malware	Detection Rate Linux Malware
ESET	NOD32 Antivirus for Linux Desktop 4.0.81.0	99.8%	99.7%
Kaspersky	Anti-Virus for Linux File Server 8.0.3.265	99.8%	98.8%
AVG	Server Edition for Linux 2013.3118	99.3%	99.0%
Avast	File Server Security 1.2.1	99.7%	98.3%
Symantec	Endpoint Protection Manager 12.1.6 Build 6168	100.0%	97.2%
Kaspersky	Endpoint Security for Linux 8.0.1.50	96.3%	100.0%
Sophos	Antivirus for Linux 9.9.0	99.8%	95.0%
F-Secure	Linux Security 10.20 Build 358	99.9%	85.7%
Bitdefender	Antivirus Scanner for Unices 7.141118	99.8%	85.7%
Microworld	eScan Antivirus for Linux Desktop 7.0-18	99.8%	85.7%
G Data	Client Security Business for Linux 13.2.251	99.8%	81.2%
Dr. Web	Antivirus for Linux 10.1	67.8%	91.6%
McAfee	VirusScan Enterprise for Linux 2.0.1.29052	85.1%	41.9%
Comodo	Antivirus for Linux 1.1.268025.1	83.0%	33.1%
ClamAV	ClamAV 0.98.7	15.3%	66.1%
F-Prot	F-Prot Antivirus for Linux 6.2.39	22.1%	23.0%

Note: Test under Ubuntu Desktop 12.04 LTS 64 bit; AV-Test 09/2015

Een recente trend in IT is offensieve defensie. Niet terughacken, maar actief je verdediging versterken. Denk aan het plaatsen van honey-tokens, het gebruik van honeypots en het bewust lekken van valse inloggegevens om deze te volgen. Wat zegt de wet hierover?



Is het neerzetten van een honeypot strafbaar?

In principe is het toegestaan om jezelf te verdedigen tegen inbrekers zoals je dat wilt. Er zijn twee belangrijke aspecten om rekening mee te houden.

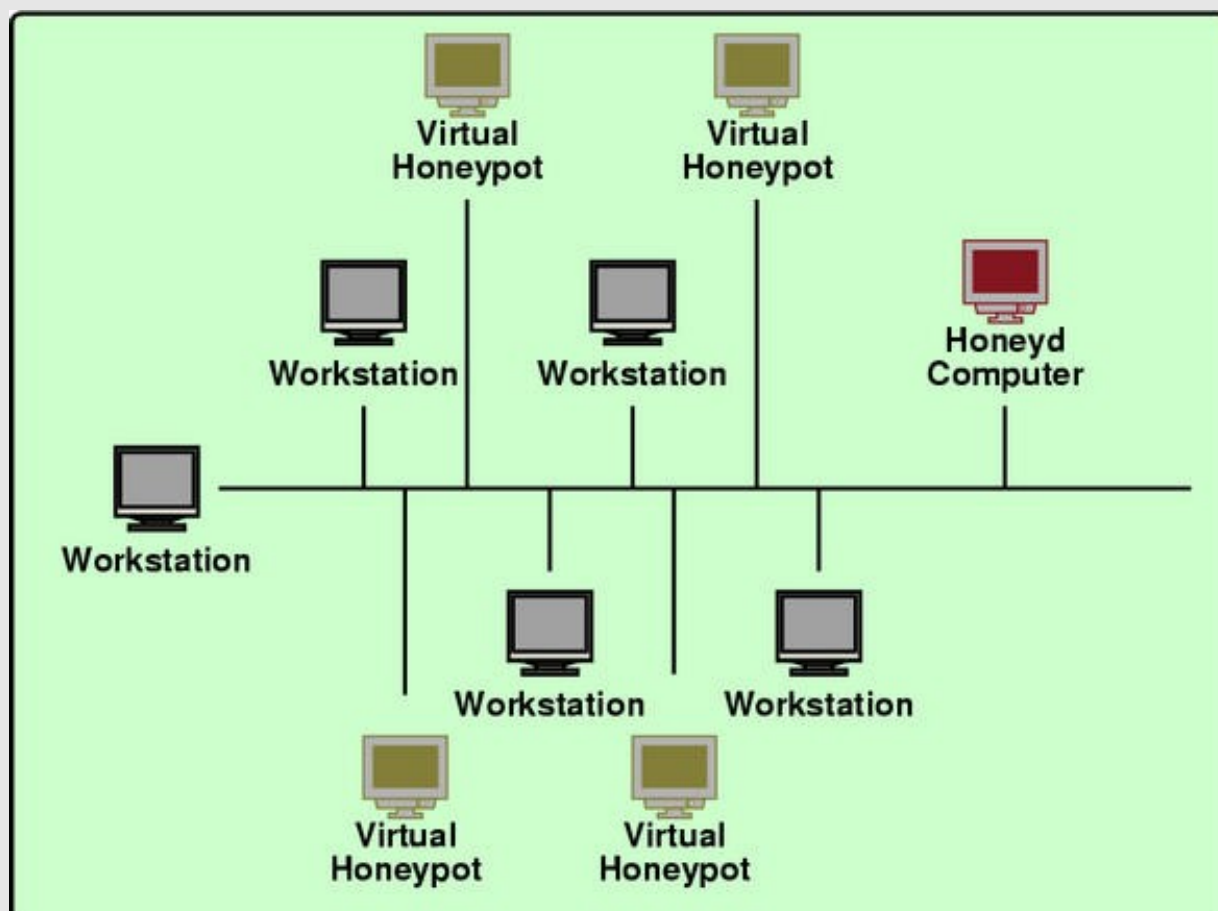
Allereerst ga je met dergelijke tools het grijs gebied in dat uitlokking heet. Uitlokken van misdrijven is strafbaar: artikel 47 lid 1 Wetboek van Strafrecht verbiedt het opzettelijk uitlokken van strafbare feiten "door giften, beloften, misbruik van gezag, geweld, bedreiging, of misleiding of door het verschaffen van gelegenheid, middelen of inlichtingen".

Kort gezegd komt het erop neer dat je mensen moet aanzetten om iets te doen dat ze niet al zelf van plan waren. In 2008 oordeelde de Hoge Raad dat het toegestaan is om een lokfiets te plaatsen op een plek waar fietsendieven actief zijn. De lokfiets stond niet op slot, maar dat was onvoldoende om van uitlokken te spreken. Had een agent de dief aangesproken en gezegd "op de hoek staat een rode fiets zonder slot, die kun je zo meenemen" dan zou het wel uitlokking zijn geweest.

Bij een honeypot of honey-token kun je niet automatisch spreken van "mensen op andere gedachten brengen", tenzij je op crackerfora gaat promoten dat die informatie of computer makkelijk te stelen is. Het posten van valse logingegevens is wél uitlokking; je wilt dan immers dat mensen die gaan gebruiken/misbruiken om bij jou in te breken.

Ten tweede loop je tegen de wet bescherming persoonsgegevens aan wanneer je tracking gaat inzetten. Je verkrijgt dan gegevens over mensen, en dat mag niet zomaar. Ook al zijn het inbrekers, je moet nog steeds kunnen rechtvaardigen welke gegevens je verzamelt en met welk (legitiem) doel. In principe is loggen van inbraakpogingen en -activiteiten legaal, maar wel moet je duidelijk kunnen maken wat je met die logs wilt gaan doen.

De inzet van honey-tokens kan vanuit dit perspectief problematisch worden als je daarmee vervolgens monitort wat men ermee doet. Vraag jezelf dus goed af wat je echt wil bereiken met dergelijke tools, leg dat vast in beleid of een privacydocument en zorg dat je geen dingen meet of doet die daarbuiten komen.



Al jaren waarschuwen anti-virusbedrijven voor Mac-malware, maar het aantal exemplaren dat Apple-gebruikers aanvalt is nog altijd zeer beperkt. Dat blijkt uit een overzicht van beveiligingsbedrijf Webroot. Jaarlijks verschijnen er zo'n twee nieuwe dreigingen voor de Mac.

Hoeveelheid Mac-malware blijft zeer beperkt

Vaak gaat het om Trojaanse paarden die zich voordoen als een applicatie maar in werkelijkheid malware zijn. De meest succesvolle Mac-malware tot nu toe was Flash-back, die voor het eerst in 2011 verscheen en in 2012 zo'n 700.000 Macs wist te infecteren. De afgelopen jaren zijn zulke grote infecties uitgebleven en in 2015 zijn er volgens Webroot nog helemaal geen grote dreiging voor de Mac verschenen. Volgens sommige experts is adware dan ook de grootste dreiging voor Mac-gebruikers.

Ondanks het kleine aantal exemplaren dat Webroot in het eigen overzicht geeft is Mac-malware volgens het beveiligingsbedrijf wel degelijk een serieuze dreiging die alleen maar groter zal worden. "Zelfs na het noemen van al deze malware zullen er mensen zijn die weigeren te geloven dat hun Mac kwetsbaar voor aanvallen is, maar vertrouw me. Het zal vanaf nu alleen maar erger worden. Apple vergroot het marktaandeel en daarmee komen er ook kansen voor malwaremakers om geld te verdienen", aldus analist Devin Byrd.

Volgens sommige experts ligt de dreiging vooral in het gedrag van gebruikers. Macs zouden vooral geïnfecteerd raken omdat gebruikers software buiten de website van de leverancier om downloaden of illegale software gebruiken. Recentelijk liet het Oostenrijkse testlab voor anti-virusprogramma's AV-Comparatives weten dat ervaren Mac-gebruikers dan ook best zonder virusscanner kunnen.



De Duitse politie heeft ouders gewaarschuwd om geen foto's van hun kinderen op Facebook en andere social media te plaatsen waar iedereen erbij kan.

Duitse politie waarschuwt voor kinderfoto's op Facebook

Volgens de politie van Hagen in de Duitse deelstaat Noordrijn-Westfalen denken veel ouders niet na bij het online zetten van kinderfoto's op social media.

In veel gevallen worden de foto's niet alleen met vrienden gedeeld, maar met iedereen. Daardoor kunnen anderen deze foto's kopiëren en opnieuw verspreiden. Wat ouders nu "schattig" vinden kan over een paar jaar erg gênant voor de kinderen zijn, bijvoorbeeld een kind dat naakt op het strand speelt, aldus het politiekorps. Ook pedofielen zouden van de foto's gebruik kunnen maken.

De politie adviseert ouders dan ook niet zomaar foto's van de eigen kinderen online te zetten en de privacyinstellingen aan te passen. De oproep die de politie op Facebook plaatste was een succes. Inmiddels is die door meer dan 7 miljoen mensen op Facebook gelezen en hebben bijna 120.000 mensen die geliket.



**Hören Sie bitte auf,
Fotos Ihrer Kinder
für jedermann sichtbar
bei Facebook und Co
zu posten. Danke!**

Auch ich habe
eine Privatsphäre!



POLIZEI
Nordrhein-Westfalen
Hagen

Fraude met geldautomaten in de Europese Unie is door lowtechcriminelen in de eerste helft van dit jaar met 15% gestegen ten opzichte van dezelfde periode in 2014. Dat laat het European ATM Security Team (EAST) weten. De organisatie baseert zich op cijfers van 20 landen, waaronder Nederland.



Toename fraude geldautomaten door lowtechcriminelen

In de 20 landen staan naar schatting zo'n 370.000 geldautomaten. In de eerste helft van dit jaar werden er 8400 fraude-aanvallen op geldautomaten waargenomen, zo'n 15% meer dan de 7300 in 2014. De schade steeg van 132 miljoen euro naar 156 miljoen euro. De stijging wordt voornamelijk veroorzaakt door 'card trapping', waarbij de kaart van de consument fysiek wordt vastgehouden en zijn pincode opgeslagen. Zodra de klant wegloopt halen de criminelen de kaart uit de geldautomaat en nemen hier geld mee op. Het aantal incidenten van card trapping steeg van bijna 2600 naar ruim 3.000.

Daarnaast was er ook een sterke stijging van 'Transaction Reversal Fraud' (TRF). In dit geval wordt er een foutsituatie binnen de geldautomaat veroorzaakt waardoor het lijkt alsof het geld niet is uitgegeven. Hierdoor wordt het opgenomen bedrag terug op de rekening van de houder gestort, terwijl de crimineel in werkelijkheid het geld toch heeft opgenomen. Dit kan bijvoorbeeld via een klauw of handmatige manipulatie van het uitgiftekanaal van de automaat. Het aantal incidenten van TRF nam met 985% toe, van 117 naar 1270.

Deze lowtechmethodes blijken populairder dan het gebruik van hightechmethodes. In de eerste helft van 2015 werden er 5 incidenten gemeld waarbij er geldautomaten-malware was ingezet. Dit is malware waarmee criminelen via een speciale toetsencombinatie de inhoud van de geldcassettes van de automaat kunnen legen. In totaal werd er bij de 5 incidenten 140.000 euro gestolen. Om de dreiging van geldautomaten-malware tegen te gaan hebben EAST en Europol in juni een speciaal document met aanbevelingen voor geldautomaten gepubliceerd.

Naast de frauduleuze aanvallen waren er ook nog fysieke aanvallen op geldautomaten. Ook hier nam het aantal aanvallen toe en verdubbelde de schade. Wisten criminelen bij zo'n 1.000 aanvallen in de eerste helft van 2014 nog 13 miljoen euro te stelen, in de eerste helft van dit jaar ging het om iets meer dan 1200 aanvallen en bedroeg de schade 26 miljoen euro.

EUROPEAN ATM CRIME STATISTICS - SUMMARY						
ATM Related Fraud Attacks	H1 2011	H1 2012	H1 2013	H1 2014	H1 2015	% +/- 14/15
Total reported Incidents	11,220	9,595	12,676	7,345	8,421	+15%
Total reported losses	€112m	€131m	€124m	€132m	€156m	+18%
ATM Related Physical Attacks	H1 2011	H1 2012	H1 2013	H1 2014	H1 2015	% +/- 14/15
Total reported Incidents	857	968	1,007	1,032	1,232	+19%
Total reported losses	€14m	€8m	€10m	€13m	€26m	+100%

Om er voor te zorgen dat Nederlandse kinderen verantwoord en veilig online kunnen is het belangrijk dat zij op school een internetdiploma halen, zo adviseert de Cyber Security Raad (CSR) in het rapport: 'advies over cybersecurity in onderwijs en bedrijfsleven' ([pdf](#)).

Verplicht internetdiploma voor Nederlandse kinderen

Volgens de [CSR](#) is het van groot belang dat Nederland in onderwijs en bedrijfsleven meer aandacht geeft aan het thema cybersecurity. "De digitale toekomst van Nederland is in het geding en dat kan gevolgen hebben voor onze positie als een van de meest concurrerende economieën in de wereld", zo laat het weten ([pdf](#)). Dat de digitale toekomst van Nederland in het geding is, heeft onder andere te maken met een tekort aan cybersecurity-professionals en een gebrek aan aandacht voor cybersecurity in het basis- en voortgezet onderwijs.

Professionals

Eerder liet onderzoek van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (WODC) van het ministerie van Veiligheid en Justitie al zien dat erop dit moment al een kwalitatief tekort is aan goede cybersecurity-professionals en dat er een kwantitatief tekort dreigt. Ook sluiten de arbeidsmarkt en de opleidingswereld onvoldoende op elkaar aan, waardoor de kwaliteit van cybersecurity-professionals onder druk blijft staan.

Volgens de CSR is daarbij cybersecurity een onderbelicht aspect in het Nederlandse onderwijs. "Er is onvoldoende aandacht voor algemene cybersecurity-kennis en -kunde bij jongeren en competenties die hen in staat stellen actief en bewust veilig deel te nemen aan de digitale samenleving. Deze nalatigheid kan Nederland zich niet veroorloven." Om ervoor te zorgen dat jongeren toch veilig online kunnen adviseert de CSR een internetdiploma dat op school gehaald kan worden.

Hiervoor zullen leraren moeten worden bijgeschoold en gecoacht door experts uit het bedrijfsleven. Onderwijs en bedrijfsleven moeten daarvoor meer dan nu het geval is de handen ineenslaan, aldus de Raad. Het advies moet er uiteindelijk voor zorgen dat Nederland over voldoende en juist gekwalificeerde cybersecurity-professionals beschikt en dat Nederlandse jongeren goed voorbereid worden op hun digitale toekomst. Daarbij moet niet alleen naar de allerjongste scholieren worden gekeken, maar de gehele keten van basis- tot beroepsonderwijs.

De aanbevelingen:

1. Bestaande en nieuwe initiatieven worden met elkaar verbonden vanuit een gedeelde visie. De Human Capital Agenda, het Platform 2032 en het Cyber Security Research and Education Platform (CSRE) bundelen de krachten op het gebied van cybersecurity in het onderwijs en de aansluiting van het onderwijs op de arbeidsmarkt.
2. Er komt meer transparantie in het aanbod van opleidingen, vacatures en loopbaanmogelijkheden voor cybersecurity specialisten. Er komt meer inzicht in de benodigde kennis en vaardigheden voor banen in het cybersecurity domein.
3. De samenwerking tussen bedrijfsleven en opleidingen wordt geïntensiveerd, zodat vraag en aanbod beter op elkaar worden afgestemd. Er worden duale trajecten ingevoerd bij bedrijven. Deze aanpak voorziet in 'learning on the job', waarbij specialisten de kans krijgen op een moderne manier hun kennis snel over te dragen aan (zij)instromers op de arbeidsmarkt. De overheid en het bedrijfsleven stellen structureel stageplaatsen/traineeships beschikbaar op het gebied van cybersecurity.
4. Er komt een geïntegreerde aanpak in het onderwijs die ervoor zorgt dat digitale geletterdheid en cybersecurity onderdeel worden van het curriculum om jongeren de vaardigheden van de toekomst aan te leren.
5. Leerlingen in het primair onderwijs halen een digitaal vaardigheidsbewijs. Dit vaardigheidsbewijs stelt kinderen in staat zich veilig in het digitale domein te begeven.¹² Ook is er aandacht voor wettelijke en morele grenzen op het internet, zodat kinderen leren hoe ver ze mogen gaan en wat de risico's zijn van het overtreden van deze regels.
6. Leraren in primair en hoger onderwijs worden geprofessionaliseerd op het gebied van digitale geletterdheid en cybersecurity. ICT'ers krijgen een rol in het geven van onderwijs en het coachen van leraren op ICT-gebied.

Zelf uw kennis eens testen?

[Klik hier](#)



Reason Core Protect is een cloudscanner die het vooral heeft gemunt op adware, spyware en PUP's en tevens een startup-, addon- en programma-manager aan boord heeft.



[download](#)

Maak je systeem veiliger

Steeds meer diensten opereren vanuit de cloud en dat is voor antivirustoestanden en aanverwanten niet anders. Ook Reason Core Security hoort in dit kamp thuis. Het is een cloudscanner die diverse bedreigingen viseert met een sterke focus op adware, spyware en PUP's (potentially unwanted programs). Let wel, de tool is niet bedoeld om je antivirus te vervangen.

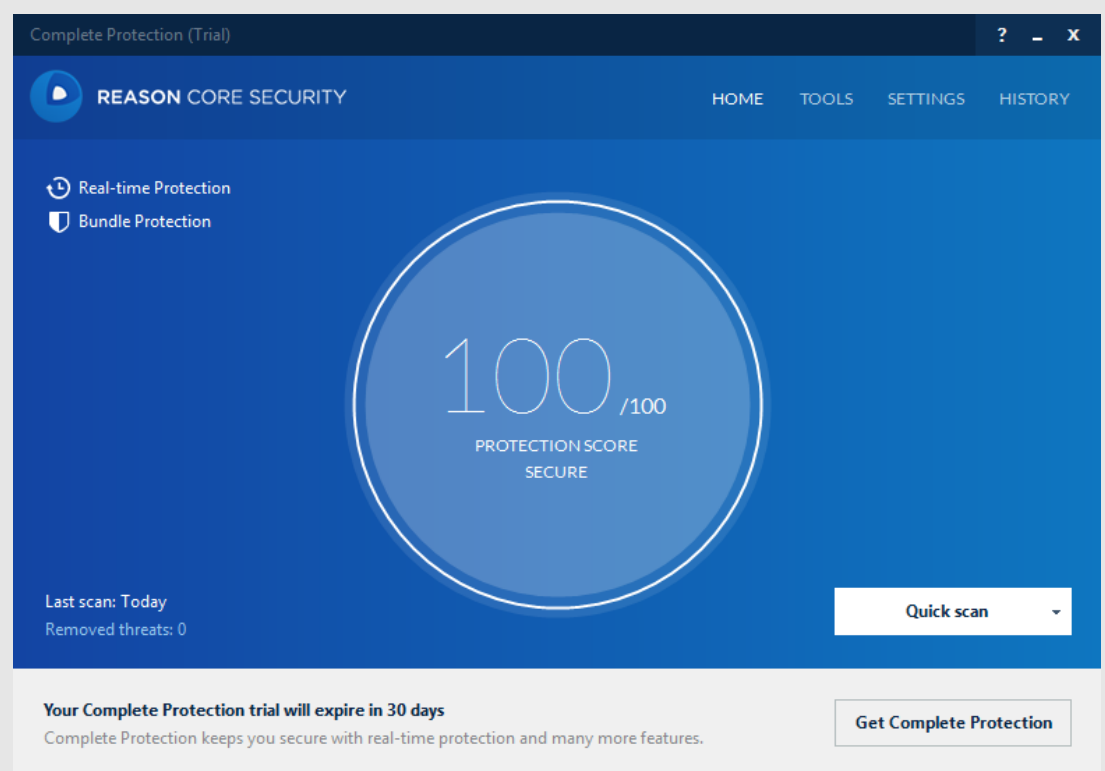
Het is eigenlijk de bedoeling dat je meteen na de installatie een initiële scan uitvoert. Dat gebeurt met de engine van HerdProtect, dat eveneens door Reason Software, de makers van [Reason Core Security](#) werd ontwikkeld. Je krijgt dan meteen een veiligheidsscore te zien en als het nodig blijkt kun je dubieuze software laten verwijderen. In de gratis versie is realtime bescherming, met automatische scans op de achtergrond, wel afgelopen na 30 dagen.

Reason Core Security bevat verder nog een aantal nuttig extra's, waaronder een 'startup manager' die nagaat hoe veilig de programma's zijn die op je systeem samen met Windows opstarten. Gezien Reason Software tevens de maker is van [ShouldIRemoveIt](#), zal het je weinig verbazen dat deze startup manager als twee druppels ware lijkt op ShouldIRemoveIt. Je krijgt meer feedback over de startups en je kunt die van hieruit ook verwijderen. Ongeveer hetzelfde geldt trouwens voor geïnstalleerde browser-addons en voor 'traditionele' programma's die op je systeem staan.

In de rubriek Remediation tref je een aantal Windows-instellingen aan die wel eens durven ontsporen en die je van hieruit makkelijk kunt

herinitialiseren. Te denken valt aan een reset van Winsock en andere netwerkinstellingen, aan een reset van de Windows Verkenner en aan het herstel van Windows systeembestanden. Ook is het mogelijk de startpagina en de standaard zoekprovider van een aantal populaire browsers opnieuw in te stellen – bijvoorbeeld nadat een browserhijacker die zonder pardon heeft gewijzigd.

Verder zit in de tool ook Unchecky geïntegreerd: een tool die bij installaties van nieuwe software nagaat of er stiekem geen additionele programma's mee worden geïnstalleerd.

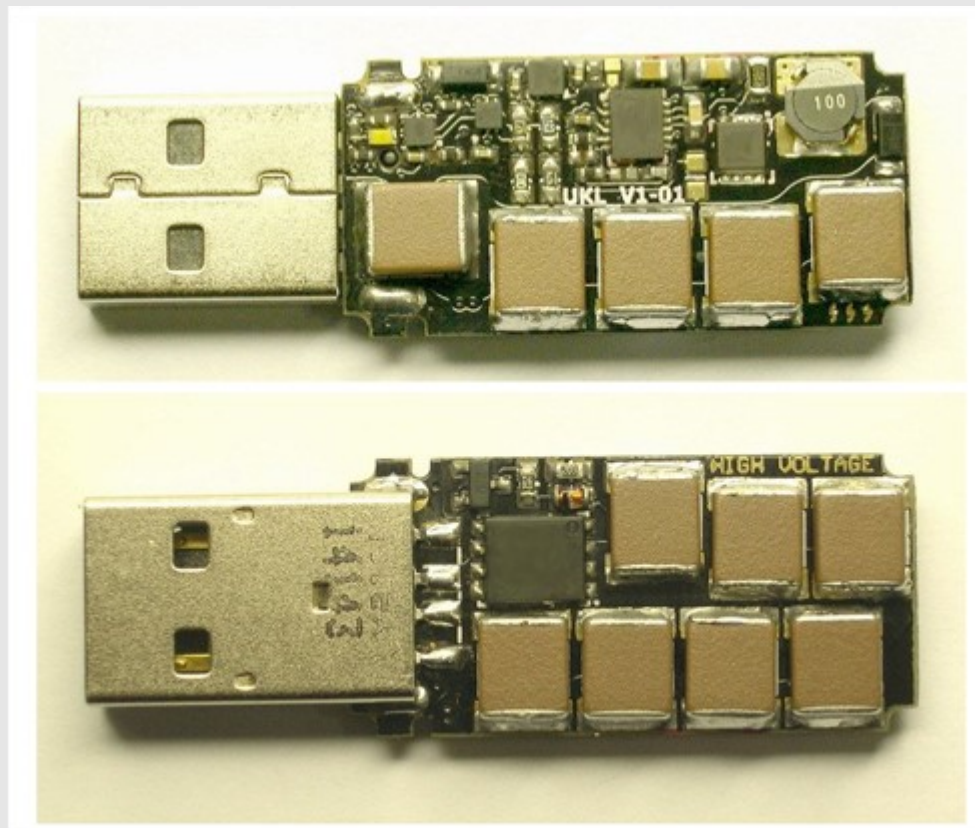


Een onderzoeker heeft een USB-stick omgebouwd tot een soort taser om een aangesloten laptop te frituren.

Gehackte USB-stick elektrocuteert je computer

Een onderzoeker, luisterend naar de naam Dark Purple, heeft een USB-apparaat ontwikkeld met maar 1 doel: het uitschakelen van het apparaat waarmee deze verbonden wordt.

Het apparaat pompt genoeg elektriciteit je computer in om deze uit te zetten of zelfs compleet te vernietigen. Het is niet zo'n heel geavanceerd apparaat, maar om die reden juist moeilijk om tegen te beschermen.



In essentie heeft Dark Purple een stungun vermomd als USB-stick die in een herhalende lus stroomstoten geeft aan je computer. En aangezien een USB-poort niet zonder stroom kan, zullen computers nog wel een tijd 'kwetsbaar' blijven.

"Wanneer [de USB-stick] wordt aangesloten op een USB-poort, laadt een omgekeerde DC/DC-converter de condensators op tot – 110V. Wanneer het voltage is bereikt, wordt de DC/DC uitgeschakeld. Op datzelfde moment opent de transistor zich. Deze wordt gebruikt om de -110V te ontladen op de contactpunten van de USB-interface. Wanneer het voltage stijgt tot -7 sluit de transistor zich en begint de DC/DC. Dit proces herhaalt zich tot alles kapot is," schrijft Purple in een blogpost.

Meneer Purple heeft het bouwschema niet openbaar gemaakt, maar een beetje hacker zou het apparaat met de huidige omschrijving kunnen namaken. Omdat de aanval direct dient plaats te vinden, en er niet echt heel veel opbrengst is, is de hack ongeveer net zo gevaarlijk voor jouw computer als, laten we zeggen, een emmer water. Wees echter wel altijd kritisch als het vreemde USB-sticks betreft.

Kijk tip!

Mr Robot

Het lezen van deze nieuwsbrief is natuurlijk een 1-dimensionale ervaring. Met veel onderwerpen zult u nooit in aanraking komen en blijven deze onderwerpen een wat ver van U bed show. Daarom deze kijk tip.



MR ROBOT

Een tv serie met het volgende verhaal:

Elliot Alderson is een protagonistische, drugs gebruikende, bipolaire, psychotische ict'r, die overdag werkt bij een internetsecuritybedrijf. 's Nachts gebruikt hij zijn kennis als hacker. Hij gebruikt zijn computerkennis om zijn medemens te hacken en te beschermen tegen bedreigingen. Op een dag wordt hij gerekruteerd door een onbekende man die 'Mr. Robot' op zijn jasje heeft staan. Mr. Robot vraagt Elliot om lid te worden van een hackerteam genaamd "fsociety". Het doel van de missie van dit hackerteam is om het bedrijf—Evil Corp.- te vernietigen. Het bedrijf van zijn werkgever beveiligd nu juist dit bedrijf.

Deze serie stijgt boven andere uit door zijn uitstekende cinematografie, de muzieklijn en gestileerd camerawerk.

De reden waarom ik deze serie voor de lezers van de nieuwsbrief aanbeveel is gelegen in het feit dat veel onderwerpen, vermeld in de nieuwsbrieven, aan bod komen. Op een manier die technisch volkomen accuraat en juist is. U kunt dus nu zien waarover u eerder gelezen heeft. Zoals social engineering, rootkit gebruik, smartphone manipulatie, DDOS aanvallen, netwerk verstoring, Raspberry Pi gebruik, Linux hacken en nog veel meer.

Mocht u in de gelegenheid zijn deze serie te bekijken, ... ik zeg DOEN!



De tijd dat You Tube alleen bestemd was voor het bekijken van
videoclips en zelfgemaakte filmpjes ligt inmiddels achter ons.

YouTube is onderdeel geworden van het nieuwe leren.

(Voor u gevonden op YouTube.....)



[Mobiele Eenheid achter de schermen](#)

[Verleiding van de misdaad](#)

[Kun jij beslissen wat de hoogste prioriteit heeft](#)

[Draadloos netwerk](#)

[Doe jij het veilig online](#)

[Malware](#)

[WiFi ontvangst verbeteren](#)

[Inbraakbeveiliging](#)

[Hoe gaat de inbreker te werk](#)

[Internetfraude via de telefoonDocumentaire:](#)

[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](#)

[Veilig politiewerk](#)

[Gezag op straat .. Als het moeilijk wordt](#)



Software schatkist

De kist is gevuld met fraaie software en naslag.

Nieuwsgierig?

Open de kist middels de sleutel en ontdek.....





Bestrijding van sexting is vooral een taak van de ouders, vindt minister Ard van der Steur (VenJ). Die moeten hun kinderen normbesef bijbrengen: verspreid geen pikante foto's van klasgenoten via internet. Van der Steur reageerde op een voorstel van de PvdA om sexting zo veel mogelijk met werk- of leerstraffen aan te pakken, al was het maar om te voorkomen dat honderden tieners een strafblad krijgen. 'Met het vervolgen van deze pestkoppen alsof ze kinderporno verspreiden is niemand geholpen', aldus kamerlid Marith Volp. Uit onderzoek bleek vorig jaar al dat één op de vijf mensen wel eens een 'seksselfie' maakt. Sexting is juridisch vergelijkbaar met het verspreiden van kinderporno, art 240b, waarop vier jaar celstraf staat. Maar een aanpak via Bureau Halt lijkt Volp een effectievere manier. 'Door deze jongeren naar Halt te sturen, zorg je ervoor dat ze straf krijgen maar ook leren van hun foute gedrag'. Over de strafmaat laat Van der Steur zich niet uit, dat is volgens hem een zaak van het OM.

In de wraakporno-zaak van Chantal vs Facebook komt een tweede kort geding. Chantal (21, uit Werkendam) sleepte Facebook juni jl voor de rechter om antwoord te krijgen op de vraag wie een seksfilmpje van haar online zette. De rechter bepaalde toen dat Facebook deze data binnen twee weken moest verstrekken, maar Facebook blijft volhouden deze data niet te hebben. Beide partijen kunnen het echter niet eens worden over de onafhankelijke expert die bij Facebook onderzoek moet gaan doen naar deze gegevens. Facebook heeft daarom een nieuw geding aangespannen: wie wordt de expert, wordt die door Facebook aangedragen dan wel door Chantal en haar advocaat? Het geding dient in november.

De overheid gaat de komende jaren bijna 40 miljoen euro investeren in ICT-onderzoek en innovatie, met name gericht op big data en cybersecurity. Volgens het Rijk is innovatie een belangrijke voorwaarde voor economische groei en wordt het gebruik van ICT daarbij steeds belangrijker.

Om ICT en innovatie op verschillende terreinen verder aan te jagen wordt er een consortium opgericht van bedrijven, kennisinstellingen en overheden dat zich richt op de toepassing van big data op het gebied van energie, zorg, veiligheid en smart industry. Tevens wil het

consortium meer ICT-specialisten opleiden op het gebied van cybersecurity en big data. Hierbij wordt samengewerkt met hogescholen en universiteiten.

"Nederland is nu één van de meest innovatieve landen ter wereld, mede dankzij een sterke ICT-infrastructuur. Om concurrerend te blijven, is ICT onmisbaar geworden. Het speelt een belangrijke rol bij de ontwikkeling van nieuwe producten en diensten. Door extra in te zetten op ICT versterken we het fundament voor verdere economische groei en zorgen we voor meer werkgelegenheid", aldus minister Kamp van Economische Zaken.

Net als je denkt dat je alles wel een keer gezien hebt, is er een nieuwe datingsite voor vrouwelijke gevangenen, Snobz.nl. De oprichter, Martin Kok van Vlinderscrime.nl, wil met de site 'lustzoekers' in contact brengen met gedetineerde vrouwen. 'In de bajes zitten vrouwen die behoefte hebben aan een seksafpraak en bovendien wat willen bijverdienen', aldus Kok in De Telegraaf. 'Dat kan ik dus regelen'. Kok, die ooit vanuit de gevangenis een escortbedrijf runde en nu dus een drukbezochte crimesite, maakt de profielen en legt het contact, 'de betaling moeten de vrouwen zelf regelen'. Hij wil met de nieuwe site ook een statement maken. 'Je mag als oud-gedetineerde geen escortbureau beginnen. De Wet Bibob houdt een vergunning tegen. Maar het runnen van een website waar escortbureaus gebruik van maken en vrouwen zich tegen betaling aanbieden, kan wel. Dat is raar toch?' Het ministerie van Justitie heeft al gereageerd: 'Daten is prima, maar seks tegen betaling kan echt niet'. Seks tijdens bezoeken zonder toezicht is weliswaar toegestaan, maar alleen voor partners; bezoekers worden daarop gescreend. Een woordvoerder zegt dat 'we prostitutie niet gaan faciliteren'.

Nederland is in 2014 'veel vaker' doelwit geweest van digitale spionage. AIVD en MIVD melden dat in het Cyber Security Beeld Nederland 2015, maar zeggen niet hoeveel aanvallen het waren, laat staan hoeveel er succesvol waren. Wel dat de aanvallen uit meer landen komen dan voorheen. Niet verrassend, aldus experts. 'Je moet echt nog wel in het stenen tijdperk zitten wil je niet aan digitale spionage doen', zegt bijvoorbeeld hoogleraar internetveiligheid Michel van Eeten. Onder de weinige gevallen die bekend

zijn, behoren de inbraak bij chipmachinefabrikant ASML, mogelijk door China, en die bij simkaartfabrikant Gemalto, door de Britse geheime dienst GCHQ. De aanvallen zijn overigens soms verbazend simpel: een mailtje met malware. Van Eeten vindt dan ook dat 'we onze bescherming nog niet op orde hebben'. Ook al liggen er nog geen staatsgeheimen op straat, 'het is te makkelijk om aan te vallen'.

Er is inmiddels meer bekend geworden over de hackersgroep Anon Nazi die afgelopen zomer de providers Ziggo en KPN platlegden met enkele DDoS-aanvallen. De vijf leden van de groep, tussen de 14 en 21 jaar oud, kenden elkaar niet in het dagelijks leven, maar werkten alleen virtueel samen. De leider zou Robin (15, uit Ruurlo) zijn, aka Blackfury, die vooral hackte 'om te laten zien hoe goed-ie is'. Ook Diederik (14, uit Lochem) had een alias: Foxelvox. Ziggo werd doelwit vanwege de slechte service, in YouTube filmpjes werden nieuwe aanslagen aangekondigd, als het bedrijf zijn service niet zou verbeteren. Internetbeveiligers Ricky Gevers van Redsocks zegt dat Blackfury de server beheerde waarmee de aanvallen werden uitgevoerd. Volgens Gevers was de groep tot de Ziggo-aanval vooral bezig met 'klein spul', zoals het platleggen van spelletjes en fora. Het zegt geen idee te hebben waarom ze besloten Ziggo te pakken. Niettemin was het opsporen van de groep relatief eenvoudig: 'er is altijd wel 'een kennis' die zijn mond voorbijpraat of die het stoer vindt te laten weten de aanvallers te kennen. 'Uiteindelijk komt het toch altijd wel uit wie achter een DDoS-aanval zit. Alleen gaat de politie er pas achteraan als een aanval veel publiciteit krijgt, zoals bij Ziggo'. Toen een andere hacker, Boefii, gegevens over het vijftal online zette, waren ze snel aangehouden. Deze Boefii spreekt geringschattend van script kiddies, 'een stelletje kinderen die niet de gevolgen zien van hun daad en die zich voor de kick misdragen op internet'.



Op basis van misdaadpatronen uit de jaren 2011-2014 vliegt de politiehelicopter in 2015 op bepaalde plaatsen en tijden. Tactical Flight Officer Martijn gaf vorige week in Nieuwsuur het voorbeeld van inbraken en roofovervallen in een bepaalde stad. Als die vaker voorkomen op vrijdagavonden in het najaar, dan vliegt de heli in volgende najaar op vrijdagavond! Volgens Martijn is het vermijden van tijdverlies door opstarten en opstijgen, het verschil 'tussen iets hebben en iets missen'. De nationale politie werkt samen met de Universiteit Twente aan een rekenmodel dat zulke patronen in kaart brengt zodat 'informatie gestuurde luchtsteun' mogelijk is. Het klinkt voor sommigen nog als Minority Report, en dat is het ook. 'In die film wordt gebruik gemaakt van algoritmes. Dat doen wij ook, dus 'predictive policing' is niet zo'n gek idee', aldus Arjen Stobbe van de Luchtvaartpolitie. Er is ook kritiek, onder meer van criminologen. Burgers die afwijken van de norm zijn verdacht en worden 'risicoburgers'. En wat als straks de helicopter een drone wordt? 'Daar zijn ethische vragen bij te stellen', aldus criminoloog Schuilenburg.

Alsof je vijftig jaar terug in de tijd gaat. In Gent vindt burgemeester Daniël Termont dat de politie niks op twitter te zoeken heeft. 'Het heeft geen zin een Twitteraccount op te starten als je dat niet 24 uur op 24 kan bemannen', stelt Termont die ook zegt dat sociale media niet het meest geschikte kanaal is om aangiftes te doen. 'Wie een dringende zaak wil melden, moet 101 bellen. Niks anders'. Volgens Termont zijn twitter en facebook 'de cafétoog van de 21ste eeuw waar iedereen makkelijk zijn gal kan spuwen'. Niet verwonderlijk is dat hij veel kritiek krijgt. Vanuit de eigen gemeenteraad waar gesteld wordt dat andere politiezones, de brandweer en zelfs de federale politiehelicopter wél actief zijn op twitter. En met succes! Kritiek is er natuurlijk ook van hoofdcommissaris Steven de Smet die als @DeFlik al jarenlang actief is op twitter en die, in 2012 al, het boek De Nieuwe Politie schreef. Volgens De Smet is niet meer mogelijk om twitter/facebook af te doen als 'informele stoorzenders vol cafépraat'. De politie staat ten dienste van de

bevolking, reageerde hij op Radio1. 'Wij dragen gemeenschapsgerichte politiezorg hoog in het vaandel. Waarom ontwijkt politie Gent dan de gigantisch publieke ruimte waar Gentenaars wachten op dialoog?' Inwoners, studenten, bezoekers en politiemensen – iedereen gebruikt volgens De Smet sociale platformen 'maar intussen wachten wij unaniem op de officiële komst van de overheid op sociale media'. Hij wijst naar vele collega's uit andere politiezones en –diensten die 'bewijzen dat het kán en dat het wérkt'.

Interpol en Europol gaan samen een taskforce starten die de internationale bestrijding van cybercrime moet verbeteren en waar opsporingsdiensten uit andere landen zich bij kunnen aansluiten. Ook zal er een samenwerkingsverband tegen misbruik van digitale valuta door criminelen worden opgezet.

Dat zijn twee van de resultaten van de Europol-Interpol Cybercrime Conferentie die vorige week in Den Haag plaatsvond. De Joint Cybercrime Cooperation & Compatibility Taskforce van Europol en Interpol zal een compatibiliteitsoverzicht maken om de verschillende juridische systemen en codes voor dataverzoeken te harmoniseren. Dit moet de samenwerking tussen verschillende opsporingsdiensten verbeteren.

Ook komt er een samenwerkingsverband tegen misbruik van digitale valuta voor criminele transacties en witwassen. Er wordt vooral gekeken naar beleid, het stimuleren van operationele samenwerking en de ontwikkeling en het geven van trainingen om het crimineel gebruik van digitale valuta te bestrijden. Zo worden opsporingsdiensten in staat gesteld om digitale valuta van criminelen te detecteren, in beslag te nemen en verbeurd te verklaren.

Het Centraal Bureau voor de Statistiek (CBS) heeft een waarschuwing voor nep-interviewers afgegeven die door middel van social engineering allerlei gegevens proberen te bemachtigen. Volgens het CBS komt het voor dat mensen zich via de telefoon voordoen als interviewer van het CBS en naar persoonlijke

gegevens vragen zoals naam, adres, woonplaats en e-mailgegevens. Het CBS laat weten dat het eerst altijd een brief stuurt voordat er telefonisch contact wordt opgenomen. Daarnaast zal een interviewer nooit om persoonsgegevens vragen en zich met voor- en achternaam bekendmaken. Mensen die door iemand zijn gebeld die zich voordeed als CBS-interviewer wordt gevraagd om contact met het CBS op te nemen.

De douane in Rotterdam verwacht, met enkele nieuwe opsporingsmethoden, sneller drugsmokkelaars te kunnen pakken. Aangiftegegevens worden gekoppeld aan informatie uit externe databases en sociale media zoals facebook, twitter en LinkedIn. Volgens douane-directeur Aly van Berckel loopt Nederland voorop met dit internetonderzoek. 'We proberen van alles te weten te komen om te achterhalen of iemand iets kwaads in de zin heeft'. Dat gebeurt anno 2015 niet meer met honden en strenge beambtes maar onder meer met kleurencans, sniffers én een stel nerds die sociale media afstruinen en informatie analyseren. 'Het gaat ons om afwijkende patronen in de informatiestroom. We weten steeds meer van steeds meer', aldus Van Berckel. 'We willen daar zijn waar de klant is. Dus op twitter, facebook en LinkedIn'. Volgens Van Berckel heeft dat resultaat. Drugsmokkelaars zouden steeds vaker de voorkeur geven aan de Antwerpse haven boven die van Rotterdam.

Vanuit Nederland zijn in de eerste helft van 2015 in totaal 397 dataverzoeken (over 593 accounts/gebruikers) gedaan aan Microsoft. Uit het nieuwste transparantierapport blijkt dat in 83% van deze verzoeken ook data is verstrekt. In 14% kon Microsoft niks vinden, 3% van de verzoeken voldeed niet aan de juridische vereisten. In 2013 deed Nederland 749 verzoeken, in 2014 734.

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

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

Computerwoordenboek

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

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. af luisterapparatuur.

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 uitspraken.
- . [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 contacten met 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



Cybercrime wetsartikelen (2)

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.

