Oktober 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+ scrolwieltje 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, Clikx, Peppermunt.net, PrivacyNieuws, HackInfo, HardwareInfo, Bright, Computerworld

De belastingdienst kan vanaf vandaag iedereen met een mobiele telefoon afluisteren via zogeheten IMSI-catchers, eigen neppe zendmasten. Zogenaamd om fraude te bestrijden kan de fiscus zonder tussenkomst van de rechter op zoek naar fraudeurs. Hoe zit dat nou precies? 5 vragen over het plan.

5 vragen over de IMSI-catchers van de FIOD

De belastingdienst kan vanaf vandaag iedereen met een mobiele telefoon afluisteren via zogeheten IMSI-catchers. Zogenaamd om fraude te bestrijden kan de fiscus zonder tussenkomst van de rechter op zoek naar fraudeurs. Hoe zit dat nou precies?

1. Wat gaat er gebeuren?

De FIOD (de opsporings-tak van de Belastingdienst) wil zonder tussenkomst van de politie IMSI-catchers gaan inzetten om vooral anonieme telefoonnummers te achterhalen. Op die manier kan de dienst onderzoek naar naar bijvoorbeeld belastingfraudeurs, zonder dat daar vooraf toestemming voor hoeft te worden gevraagd.

Op dit moment mag de FIOD al wel gebruik maken van zulke technieken, maar die bevoegdheden worden uitgebreid zodat het makkelijker voor de organisatie wordt om ze in te zetten.

2. Wat is nu de situatie?

IMSI-catchers worden nu ook al af en toe ingezet, ook door de FIOD. Daarvoor moet de fiscus echter samenwerken met de Nationale Politie. Die legt daarvoor een verzoek neer bij de Officier van Justitie, die per geval moet beoordelen of zo'n catcher mag worden ingezet.

Dat is omslachtig, en dat wil de FIOD liever niet. In de nieuwe maatregel is opgenomen dat de FIOD niet hoeft samen te werken met de politie, én dat er geen toestemming hoeft te worden gevraagd aan de Officier van Justitie.

Overigens is de FIOD niet de enige die met IMSI-catchers werkt. Ook de inlichtingendiensten AIVD en MIVD mogen zulke zendmasten plaatsen voor onderzoek. Ook zij hebben geen toestemming vooraf nodig.

3. Wat is een IMSI-catcher?

Een IMSI-catcher is een soort mobiele zendmast. Daarmee kan telefoonverkeer worden onderschept. Een IMSI-catcher voert een man-in-the-middle-aanval uit, waarbij de gebruiker een eigen zendmast maakt. Al het telefoon-verkeer in de buurt maakt automatisch verbinding met die mast, wat vervolgens weer wordt doorgestuurd naar de echte zendmast van de provider. Een gebruiker kan daardoor niet detecteren of hij afgeluisterd wordt of niet.

Met een IMSI-catcher is het mogelijk om al het data-verkeer van een toestel af te luisteren. Het gaat daarbij om telefoonverkeer, maar ook internetverkeer zoals de inhoud van emails of webpagina's.

De catcher zoekt echter, zoals de naam al verklapt, naar het IMSI-nummer van een

telefoon. Dat staat voor 'International Mobile Subscriber Identity' en wordt gebruikt om gebruikers te identificeren per abonnement of prepaid-kaartje. Het is de tegenhanger van een IMEI-nummer, dat specifiek voor telefoons bedoeld is.

4. Waarom wil de Fiod dat?

In de eerste plaats zijn de catchers bedoeld om anonieme telefoonnummers te kunnen achterhalen en te volgen. Als iemand een abonnement heeft, kan diegene makkelijk worden gevolgd via andere kanalen. Dat is echter lastiger wanneer die persoon een prepaid-telefoon en -simkaart koopt. Die zijn moeilijker te traceren.

De FIOD wil de opsporing daarvan echter makkelijker maken, omdat ze bijvoorbeeld criminelen willen volgen die aan witwassing doen. Als die daarvoor een prepaid-telefoon gebruiken, is het moeilijk die personen te traceren.

Met een IMSI-catcher kan de FIOD een soort hotspot maken op een plek waarvan ze weten dat een verdachte zich bevindt. Alle nummers in de omgeving maken dan verbinding met die hotspot, zodat de opsporingsdiensten het IMSI-nummer van een telefoon kunnen bemachtigen. Met dat nummer is het mogelijk om een nummer in de toekomst overal te traceren.

5. Wat betekent zo'n IMSI-catcher voor je privacy?

Het grote nadeel van een IMSI-catcher is dat die werkt als een sleepnet, en dat je er niet gericht mee kunt zoeken naar een specifieke telefoon. Als de opsporingsdiensten zo'n zendmast opzetten, dan maken alle telefoons in de omgeving daar verbinding mee.

Een IMSI-catcher heeft een groot nadeel: Je kunt hem alleen als sleepnet gebruiken. Het is niet mogelijk de techniek in te zetten voor een specifiek toestel, maar alleen voor alle telefoons in een omgeving. Dat betekent dat de catcher van de tientallen of zelfs honderden mensen in de buurt het verkeer opvraagt én afluistert: Niet alleen van verdachten, maar vooral van onschuldige burgers.

Bron: PCMweb

Index

"Mobiele malware neemt wereldwijd aanzienlijk toe, maar tot op heden zijn grootschalige besmettingen in Nederland nog niet vastgesteld", zo meldde het Nationaal Cyber Security Centrum (NCSC) vorig jaar in zijn Cybersecuritybeeld Nederland.

Mobiele dreiging valt niet te bagatelliseren

Een vergelijkbaar geluid dook in april van dit jaar ook op in het 2015 Data Breach Investigations Report van Verizon. Het aantal kwetsbaarheden in de beveiliging van mobiele platforms waar cybercriminelen misbruik van maken, zou verwaarloosbaar zijn. In een begeleidend persbericht werd de berichtgeving over mobiele dreigingen zelfs als 'grotendeels overdreven' afgedaan.

Feitelijk gezien hebben het NCSC en Verizon misschien gelijk; grootschalige infecties door mobiele malware zijn inderdaad nog zeldzaam. En toch vind ik het zogenaamd geruststellende signaal dat het allemaal (nog) wel meevalt met de mobiele dreiging, zoals afgegeven door bijvoorbeeld het NCSC en Verizon, ronduit gevaarlijk. Wie de mobiele dreiging nu niet serieus neemt, en geen aanvullende beveiligingsmaatregelen neemt, zal in de toekomst gericht worden aangevallen via zijn smartphone, tablet of ander mobiel apparaat. Ook dat is voor mij een feit.

Opmars mobiele malware

Mobiele platformen worden voor hackers een steeds aantrekkelijker doelwit nu het (zakelijk) gebruik van smartphones en tablets toeneemt, evenals het aantal kwetsbaarheden dat wordt aangetroffen in mobiele besturingssystemen. Met name Google's Android is geregeld de klos. Zo waarschuwde beveiligingsbedrijf Zimperium eind juli nog voor een lek dat hackers in staat stelt om een Android-smartphone geheel over te nemen. Slechts enkele dagen later maakte Trend Micro melding van een nieuw lek dat kan worden misbruikt om van een Android-smartphone of -tablet een 'kasplantje' te maken.

Het gevolg is dat mobiele malware aan een stevige opmars bezig is. Alleen al in het tweede kwartaal van dit jaar doken er volgens onderzoek van Kaspersky Lab ruim 290.000 nieuwe mobiele malwareprogramma's op. Dit is bijna drie keer zoveel als in het eerste kwartaal van dit jaar. Ondertussen constateer ik nog dagelijks dat bijna al het securitybudget wordt besteed aan het versterken van de randen van het netwerk, en dat smartphones en tablets vrijwel onbeveiligd over de organisatie worden 'uitgestrooid' en op die manier de zwakke schakel in de beveiliging vormen.

Mobiel veiliger in vier stappen

Om te voorkomen dat je als organisatie wordt aangevallen via de mobiele platformen die in gebruik zijn, is het naar mijn mening absoluut noodzakelijk om ook mobiele apparaten integraal mee te nemen in de beveiliging. Maar hoe beveiligen we al die mobiele apparaten? Vanuit het oogpunt van performance wordt niemand gelukkig van een antiviruspakket op zijn smartphone of tablet. Met een Mobile Device Management-oplossing het apparaat van de gebruiker volledig onder controle nemen, is volgens mij ook niet de oplossing om diezelfde gebruiker mee te krijgen. Een oplossing die wel kan rekenen op de instemming van de gebruikers, kan naar mijn mening worden gecreëerd door in ieder geval onderstaande vier stappen op te volgen:

Stap 1. Zorg voor een 'container' op de mobiele apparaten waarin zakelijke data volledig versleuteld en gescheiden van de persoonlijke data worden opgeslagen.

Stap 2. Zorg ervoor dat mobiele apparaten altijd via een beveiligde (VPN)-verbinding het internet op gaan, waar het verkeer inline wordt gescand op malafide inhoud.

Stap 3. Zorg voor slimme technologie om mobiele apparaten vrij te houden van apps met malware.

Stap 4. Zorg ervoor dat documenten al bij de creatie een 'automatische beveiliging' meekrijgen waardoor alleen geautoriseerde gebruikers toegang hebben tot beveiligde documenten op al hun apparaten en waarmee bijvoorbeeld printen, kopiëren of delen met andere personen is te blokkeren.

Deze vier stappen zorgen ervoor dat de data zo veilig mogelijk zijn. Het 'managen' van het apparaat zelf is dan minder belangrijk, zelfs als het om een Android-apparaat gaat.

Bron: Bart Verhaar >werkzaam als Pre-Sales Consultant Netwerkwerkbeveiliging en Gebruikersbeveiliging bij Motiv.

Index

Incassobureaus hebben ook last van phishing. Niet dat ze zelf slachtoffer worden van mails met viagra-pillen of gestolen creditcards, maar door het wantrouwen van burgers tegen de instanties.

Incassobureaus niet meer geloofwaardig door spammails

Door het grote aantal spam-berichten dat zogenaamd uit naam van incassobureaus wordt gestuurd, gooien mensen vaker echte brieven van echte bureaus weg.

Dat zegt de Fraudehelpdesk naar aanleiding van klachten van Intrum Justitia, één van de grootste incassobureaus van Nederland.

Spam

Omdat Intrum Justitia zo groot is, worden er erg veel spam-mails verstuurd uit naam van het bureau. Daarin worden ontvangers gewaarschuwd dat zij nog een openstaande boete hebben, en wordt er vaak gedreigd met een deurwaarder als er niet meteen geld wordt overgemaakt.
Verwarring Veel ontvangers zien inmiddels wel door die spam heen en weten zulke berichten meteen naar de digitale prullenbak te verwijzen. Maar de naam Intrum Justitia is door die brieven inmiddels zo notoir dat ook échte brieven niet meer worden herkend. De Fraudehelpdesk heeft al diverse mensen moeten helpen die een brief van het incassobureau op de mat hadden liggen, maar die niet wisten of dat echt was of niet.

Controle

De Helpdesk adviseert iedereen die een brief krijgt van een incassobureau het bankrekeningnummer in de brief te vergelijken met dat op de website van het incassobureau. Ook een belletje naar het incassobureau kan helpen.

Maar in de meeste gevallen betekent dat helaas maar één ding: Betalen...

Eind vorig jaar werden er via e-mail documenten met een kwaadaardige macro verstuurd die van het incassobureau afkomstig leken. Ook werd de naam van het bedrijf voor de verspreiding van ransomware gebruikt. De laatste aanval dateert van juni, waarbij de CTB-locker-ransomware via frauduleuze e-mails die van Intrum Justitia afkomstig leken werd verspreid. Vanwege de aanvallen hebben consumenten nu ook hun twijfels over de legitieme post van het bedrijf.

"Het is voor het eerst dat authentieke post als vals wordt aangezien. Wat vaak voorkomt is dat mensen in nepmails trappen die ogenschijnlijk door bestaande en betrouwbare bedrijven zijn verstuurd", aldus de Fraudehelpdesk.

Bron: CiD

Index

Welke maatregelen er ook worden genomen, phishing blijft een populaire methode van oplichting. Wat doen phishers precies met de gegevens en het geld dat ze stelen?

Phishing: dit doen criminelen met gestolen geld

Bij phishing wordt geprobeerd een ontvanger van een e-mail over te halen naar een frauduleuze website te gaan en daar persoonlijke gegevens achter te laten. Soms gebeurt dat met websites die nauwelijks te onderscheiden zijn van de echte websites. Beveiligingsbedrijf DearBytes zocht uit wat de phishers ermee doen.

DearBytes gebruikte prepaid-creditcards zonder saldo, om te kijken wat de criminelen dan verder met de gestolen gegevens doen. De gegevens van de creditcard werden ingevuld op verschillende frauduleuze websites. Binnen enkele uren werden de gegevens al misbruikt om uitgaven te doen.

Computerspel en hotel
In het rekeningoverzicht van de creditcard kon worden bijgehouden welke transacties werden gedaan, en wanneer die werden gedaan. Ook werd duidelijk waar de cybercriminelen transacties doen.

In het onderzoek van DearBytes kochten phishers iets bij Wehkamp, een computerspel van 59,99 euro, twee keer tickets van ruim 270 euro, en probeerden ze 2117,14 euro te betalen voor een luxe hotel in Dubai.

Uiteindelijk draait het natuurlijk om geld. Vaak zijn phishers uit op de inloggegevens van internetbankieren, om zo simpelweg geld te stelen. Ze proberen geld over te maken van je rekening, of ze gebruiken je bankgegevens om betalingen te doen.

Toegang tot de e-mail
Eén van de doelen van phishing is ook om toegang te krijgen tot je mailbox. Zodra dat is gelukt, kan je mailaccount zelf misbruikt worden om phishing-e-mails te versturen naar je contacten. Die vertrouwen het mailtje omdat ze je kennen en klikken eerder op een link dan wanneer het mailtje van een vreemde komt.

Daarnaast kan via je e-mailaccount geprobeerd worden andere accounts te kapen, zoals die van Spotify of clouddiensten. Dat gebeurt dan meestal door een nieuw wachtwoord aan te vragen via je mailadres.

Bron: RTLnieuws

Index

Dat politie en Justitie tegenwoordig in één moeite telefoon én internet laten aftappen gaat de perken te buiten, vindt een verbolgen SP. De partij eist tekst en uitleg.

Nieuw tapbeleid Justitie 'aanval op onze grondrechten'

Sinds begin 2014 is er geen sprake meer van aparte taps op telefonie of internet, maar wordt al dit verkeer met één tapbevel onderschept. Dat bleek recent uit een summiere rapportage van Justitie.

"Sinds de invoering van de nieuwe interceptiestandaard wordt, zowel technisch als procedureel, geen onderscheid meer gemaakt tussen een telefoontap en een internettap. Het onderscheid in de tellingen komt hiermee te vervallen."

Minachting grondrechten

Dit beleid kan op twee fronten niet door de beugel, reageert de SP op de kwestie. "Het is niet proportioneel en legitiem om altijd ook internetverkeer af te tappen. In Nederland wordt al heel veel getapt, nu wordt het ook nog met de Franse slag gedaan. Dit is een aanval op onze grondrechten," aldus SP-Kamerlid Sharon Gesthuizen.

Dat een verdachte wordt getapt is één ding, maar vaak wordt dit uitgebreid tot een brede kring van familie, vrienden en relaties. Met het automatisch onderscheppen van IP-verkeer wordt deze ongewenste bijvangst exponentieel groter. Gesthuizen: "De rillingen lopen over mijn rug als ik besef hoeveel extreem privacygevoelige data van onschuldige mensen dan wordt verzameld."

Rookgordijn

Ten tweede leidt de nieuwe 'interceptiestandaard' er toe dat de Kamer, die jarenlang aandrong op transparantie, ineens minder inzicht krijgt in tappraktijken in plaats van meer. De SP roept dan ook minister Van de Steur van Veiligheid & Justitie op het matje, middels Kamervragen, meldt Gesthuizen.

De bewindsman moet uitleggen waarom tot deze meer ingrijpende opsporingsmethoden is overgegaan en of privacywaakhond CBP hier naar gekeken heeft. "Ik ben hier verbolgen over. Dit ondermijnt het vertrouwen in de overheid. Het is typisch een geval van 1 stap vooruit, 2 achteruit," aldus het Kamerlid.

Het Ministerie van Veiligheid & Justitie laat weten dat er 'juridisch en wettelijk' niets is veranderd. Dat nu automatisch naast telefonie ook IP-verkeer wordt afgetapt is een uitvloeisel van de opkomst van de smartphone, verklaart de woordvoerster de nieuwe 'interceptiestandaard'.

Bron: Computerworld

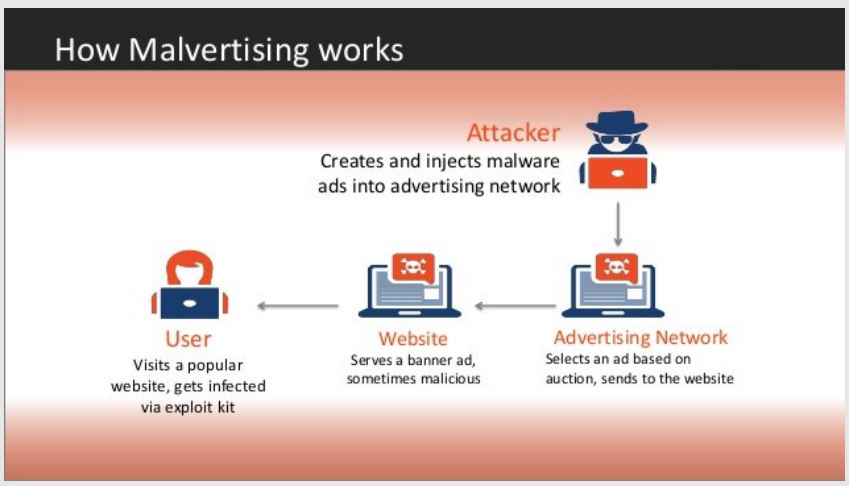
Index

Vraag op straat wat malvertising precies is en er zullen maar weinig mensen zijn die je een correct antwoord kunnen geven. Phishing, malware en virussen spreken meer tot de verbeelding, maar het zal niet lang meer duren voordat malvertising bij iedere internetgebruiker op de radar komt te staan.

Hoe moet malvertising worden aangepakt?

Op het internet van enkele jaren terug kwam het fenomeen malvertising nog niet voor en dat verklaart direct waarom het nog een relatief onbekend begrip is. Maar de bedreiging, waarbij advertenties op websites worden gekaapt door cybercriminelen, maakt een stormachtige ontwikkeling door en is inmiddels de meest voorkomende vorm van malware.

Dat is vooral dit jaar te merken. In de eerste helft van 2015 werden bijna drie keer zoveel advertenties met malware geplaatst in vergelijking met de eerste zes maanden van 2014, zo blijkt uit onderzoek van securitybedrijf RiskIQ.



Cybercriminelen hebben in malvertising blijkbaar een nieuw favoriet wapen gevonden om de niets vermoedende internetgebruiker, zonder dat daar een muisklik voor nodig is, te infecteren met kwaadaardige code. Maar ook gebruikers die wel bekend zijn met online dreigingen lopen risico. Malvertising is namelijk lastig op te merken of af te wenden, want de getoonde advertentie ziet er legitiem uit - op het oog is het niet te zien dat op de achtergrond verbinding wordt gelegd met een malware-server.

Lastige problematiek voor grote en kleine sites

Bega niet de vergissing dat alleen kleine websites met onoplettende beheerders slachtoffer worden van malvertising. Hoewel deze sites een eenvoudiger doelwit zijn van de kwaadwillende hacker, zijn het juist de grote populaire websites die ten prooi vallen aan malvertising. Deze zomer werd het advertentienetwerk van Yahoo, een site met een bereik van 6,9 miljard bezoeken per maand, slachtoffer van een grootschalige aanval. En ook YouTube kon cybercriminelen niet buiten de deur houden; slimme hackers wisten videoadvertenties te voorzien van hun malware.

Maar ook in ons land vindt malvertising op grote schaal plaats. Zo werden afgelopen zomer de sites van populaire krantensites en het videoplatform Dumpert besmet met een trojan, terwijl ook Nu.nl en Voetbalzone.nl problemen kenden omdat hun advertentienetwerken waren gekaapt.

Site-eigenaren zijn om twee redenen niet blij met deze relatief jonge vorm van malware. Niet alleen brengt malvertising de gebruiker (klant) van een computer of mobiel device in gevaar, wat een site bepaald geen goede reclame oplevert, ook leidt de opkomst van malware tot een sterke opkomst van adblockers omdat in de ogen van gebruikers apparaten alleen op deze manier tegen malvertising beschermd kunnen worden. Bekijkt niemand meer advertenties, dan betalen de adverteerders ook de site-eigenaren niet uit. Het gevolg: sites die het vooral moeten hebben van advertentie-inkomsten gaan op zwart.

Ontoereikend

Voor het bestrijden van het probleem worden wel degelijk oplossingen aangedragen. Zo wordt advertentienetwerken opgeroepen hun systemen beter te beveiligen, zouden site-eigenaren alleen met reputabele netwerken zaken moeten doen en zien anderen in eerder genoemde adblockers een panacee. Adblockers zijn namelijk prima als site-eigenaren in plaats van advertenties namelijk advertorials in de vorm van enkel tekst en hyperlinks gaan tonen in plaats van foto en video, zo luidt de redenering.

Geen van deze oplossingen snijdt hout. Advertentienetwerken kunnen, ook al gaat de beveiliging omhoog, altijd gekraakt worden. Dat zal hoe dan ook blijven gebeuren omdat malvertising voor hackers vanwege het gigantische bereik van sites enorm interessant is. Daarnaast is het niet meer van deze tijd te denken dat gebruikers alleen op sites die geverifieerd oké zijn komen, terwijl juist veel marketingpower huist in foto en video en adverteerders precies daarmee de meeste eyeballs krijgen en niet met een simpel linkje of artikel.

Lacune in de securitywereld

De echte oplossing lijkt te moeten komen vanuit de securityindustrie. Daarbij valt te denken aan slimme software die de advertentienetwerken scant door de links in afbeeldingen en filmpjes te volgen en alarm te slaan bij verdachte activiteit of servers. Pas op dat moment zou een adblocking-mechanisme ingeschakeld kunnen worden. Deze vorm van bescherming kan worden geïntegreerd in bestaande end-point antivirus software, maar ook in browser plug-ins en clouddiensten die verkeer via beveiligde servers laten lopen.

Toegegeven, ook indien de securityindustrie dit probleem serieus gaat nemen, is het daarmee niet opgelost. Zoals ook bij antivirus/antimalware jarenlang het geval was, zal niet iedere gebruiker (gratis) software installeren. En ook de kwaliteit van verschillende producten en diensten zal uiteen blijven lopen. Zeker binnen bedrijfsomgevingen zal daarom trainingbelangrijk blijven: een gewaarschuwd mens telt immers voor twee.

Bron: Webwereld

Index

Nederland is uniek door de talloze publiek-private samenwerkingsverbanden op het gebied van cybersecurity. Maar hoe schaalbaar is dit model buiten ons kikkerlandje?

Kan Nederland 'de cyber' veilig polderen?

Nederland is wereldkampioen samenwerken en andere landen kijken met verbazing wat we allemaal voor elkaar krijgen qua publiek-private cybersecurityprojecten. Zoveel werd onlangs duidelijk op het 'Holland Strikes Back' evenement in Amersfoort . Wat weer onderdeel is van Alert Online, de brede publiek-private campagne over security die deze weken Nederland overspoelt.

Wildgroei aan 'nationale netwerken'

De overheid, hosters, isp's en experts bezongen op 'Holland Strikes Back' talloze recente successen van dit unieke poldermodel. Zo is AbuseHub, een centrale clearinghouse voor providers over botnetinfecties, geheel functioneel, vertelde voorzitter Gert Wabeke, tevens abuse-chef van KPN. Er worden maandelijks inmiddels 4,7 miljoen meldingen verwerkt door het systeem.

Op Europees niveau is een soortgelijk project gaande, ACDC genaamd, vertelde hoogleraarMichel van Eeten, gespecialiseerd in "Governance for Cybersecurity". Maar ook de Belastingdienst, SURFnet, Defensie CERT (DefCERT), de Informatiebeveiligingsdienst voor gemeenten (IBD) en het NCSC werken sinds dit jaar samen in het Nationaal Respons Netwerk. Uitvloeisel daarvan is het Nationaal Detectie Netwerk, waarin dreigingsinformatie wordt verzameld en onderling gedeeld.

De NBIP, die oorspronkelijk aftapfaciliteiten biedt voor kleine isp's, heeft twee nieuwe projecten: De Nationale anti-DDoS Wasstraat (NaWas) en Trusted Flagger, een centraal meldpunt voor Notice en Takedown-verzoeken. Die vorderingen worden door juristen van NBIP beoordeeld voordat ze, indien geldig en juist, worden doorgestuurd naar de hoster in wiens netwerk de illegale of strafbare content staat. Het NBIP wil met deze nieuwe diensten uitgroeien tot een compleet shared service center voor kleine isp's.

Ophaalbrug

En als gigantische DDoS-aanvallen toch de cyberdijken dreigen te doorbreken is er een interessant nieuw initiatief: Het Trusted Networks Initiative, een soort stormvloedkering voor isp's. Het voordeel van dit initiatief is dat het niet is beperkt tot de landsgrenzen, elke isp die aan de vereisten voldoet kan lid worden van de exclusieve club van netwerken.

Aan de eisen wordt nog geschaafd, maar te denken valt aan bijvoorbeeld bescherming tegen BGP-kaping en een snelle responstijd bij incidenten.

Krijgt een netwerk of site een enorme DDoS voor de kiezen, dan kan al verkeer van het niet vertrouwde deel van het internet helemaal worden geblokkeerd. Het clubje vertrouwde netwerken koppelt zich feitelijk af, haalt de 'ophaalbrug' op, maar kan onderling nog wel verkeer delen via een aparte VLAN op één of meer internet exchanges.

Straatje schoonvegen

Constatering na 'Holland Strikes Back': de neuzen staan zeker niet altijd dezelfde kant op, en regelmatig trekken isp's aan de bel dat ze onder druk staan van autoriteiten om pro-actief op te treden, bijvoorbeeld tegen vermeende Jihad-propaganda. Maar uiteindelijk zit iedereen om de tafel, en met veel koffie en een biertje achteraf komen de partijen weer met mooie nieuwe plannen en initiatieven.

Eendrachtig pompen we zo onze eigen cyberpolder veilig. En dat is mooi geregeld. Helaas kent cybersecurity geen grenzen. Bovendien zijn cyberaanvallen en -criminaliteit veelal extreem schaalbaar. "De Nederlandse samenwerkingsinitiatieven zijn stuk voor stuk mooi, maar cybersecurity is vooral een probleem van [internationale] schaal", aldus professor Van Eeten. Met andere woorden: heeft het wel zin om samen steeds ons eigen straatje schoon te vegen als de rotzooi van alle kanten binnenwaait?

Red Queen

Overigens diskwalificeert Van Eeten de talloze doemscenario's en intimiderende exponentiele curves over cyberdreigingen, aanvallen en malware. Dat zijn de beruchte damned lies & statistics. "Geef me een berg data en ik tover een exponentiële curve tevoorschijn. Maar als je daar doorheen prikt zie je een dynamisch evenwicht, eigenlijk net als het weer." Dat betekent niet dat de ontwikkelingen niet snel gaan, het is een kat & muisspel op volle snelheid. Van Eeten: "Net als in Alice in Wonderland: we moeten hard hollen om op dezelfde plek te blijven."

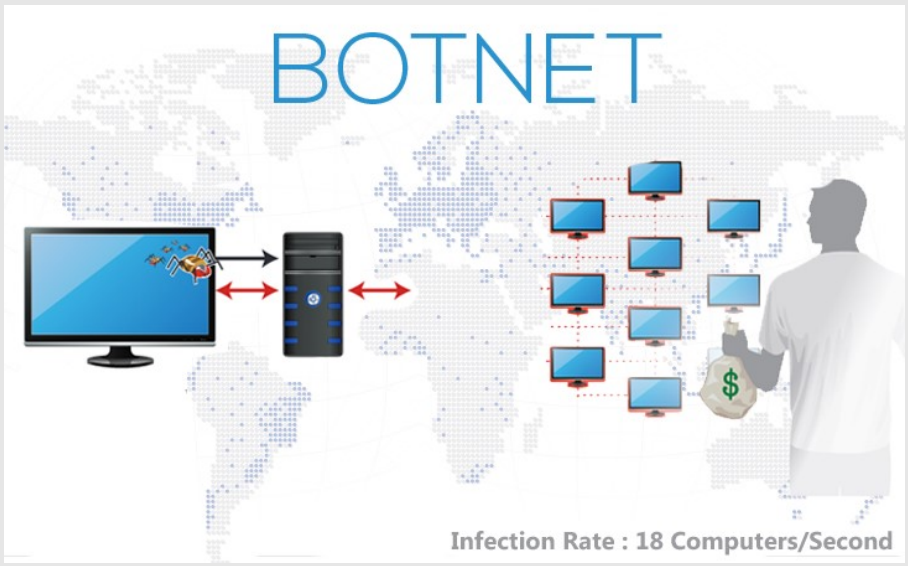
Bron:

Index

Botnets worden vaak met veel bombarie 'neergehaald', maar initiatieven van overheden en isp's om de miljoenen zombie-pc's te desinfecteren zijn kansloos. Het zijn veelal oude, illegale Windows-machines die nooit meer een update krijgen.

Waarom zombie-pc's jarenlang ondood blijven

Het beruchte Conficker, een van de grootste botnets ooit, is inmiddels al zes jaar ter ziele. Het netwerk is onthoofd, de botherders hebben hun heil elders gezocht of zijn opgepakt (al is die kans miniem). Toch zijn nog steeds één miljoen pc's besmet, zombie's die nog steeds op de automatische piloot op bevelen wachten van een bepaald IP-adres, waar eens de command & control (C&C) server was.



De afgelopen jaren zijn er talloze initiatieven ontplooid om dergelijke botnets op te ruimen, en de geïnfecteerde pc's te redden van hun noodlottige zombiebestaan. Want eens een zombie, worden ze daarna vaak opnieuw gerekruteerd in een nieuw botnet.

Zombie's weigeren updates

Deze pogingen zijn echter hopeloos, een druppel op een gloeiende plaat, blijkt uit onderzoek van de TU Delft. Ze volgden jarenlang het Conficker-zombieleger met een zogenaamde sinkhole, een soort 'afluisterstation' om verkeer tussen zombie's en C&C servers te onderscheppen.

Uit de data blijkt dat het aantal infecties slechts heel langzaam afneemt, en de opruimcampagnes hebben 'geen zichtbaar effect' hierop, is de pijnlijke conclusie. Zombie's zijn namelijk bijna altijd ook echt zombie's: het zijn systemen waarop veelal verouderde en illegale software draait, en om die reden worden er nooit enige patches of updates binnengehaald.

Er is dan ook een sterke relatie tussen het 'institutionele ICT-klimaat' en de voortdurende zombieplaag. Op plekken waar veel illegale software wordt gebruikt en (dus) laks wordt omgesprongen met updates telen de zombie's welig, en daar zal geen opruimcampagne iets aan veranderen, constateren de Delftse onderzoekers Hadi Asghari, Michael Ciere en Michel van Eeten. Ze presenteerden hun bevindingen op de Usenix-conferentie in Washington D.C..

ICT-ontwikkelingshulp

Zo bleek de afname van het aantal Conficker-infecties trager te gaan dan de afname van het marktaandeel van Windows XP. Het advies: botnetbestrijding is een zaak van de lange adem. Het heeft meer zin om de algemene ICT-ontwikkeling in een land naar een hoger plan te (helpen) tillen dan om op de korte termijn te koketteren met kansloze opruimcampagnes.

Wel zouden isp's agressiever kunnen optreden tegen infecties (klanten blokkeren of zelfs op afstand desinfecteren?), nu heeft dit vaak geen prioriteit, zeker als het botnet in kwestie onthoofd is. Dat is slechts schijnveiligheid: de zombie's blijven dus bestaan en zijn de eerste rekruten in het volgende botnet of andere malware-campagnes.

Bron: Webwereld

Index

Onderzoekers van DearBytes lokten phishers uit de tent met aas in de vorm van een creditcard en e-mailaccounts. Wat doen cybercriminelen zoal met deze informatie?

Nederlands securitybedrijf phisht de phishers

Ook phishers trappen in phishingmails, toont Wesley Neelen van het Beverwijkse DearBytes aan. Hij voerde expres creditcard- en e-mailaccountgegevens in op een phishingsite, met als doel de handelingen van de phishers te traceren.

Prozaïsch shoppen

Het is niet meer dan een kijkje in de keuken, maar die bevestigt én ontkracht een aantal vooroordelen over cybercriminelen. De phishers die Neelen aan de haak sloeg waren in elk geval geen doorgewinterde cyberboeven, eerder scriptkiddies. Met de gestolen creditcard werden geen wapens en drugs gekocht, maar een VPN-abonnement, wat spulletjes bij Wehkamp, tickets, een Steam-abo en nog zo wat prozaïsche zaken.

Al springt een transactie van ruim 2000 euro bij het luxueuze Chelsea Tower 1 in Dubai er wel uit. De conclusie van deze steekproef: "Het amateurgehalte is hoog, de phishers besteedden weinig aandacht aan het verhullen van hun identiteit", schrijft Neelen.

Reconstructie surfgedrag

Met het expres laten kapen van je e-mailaccount wordt het spannender en persoonlijker. Met een slimme truc zijn de gangen van de phisher te achterhalen: omdat het gaat om Microsoft en Google-accounts kan ook het surfgedrag worden gereconstrueerd op basis van IP-adres, locatie, zoek- en browserhistorie.

Over de gebruikte IP-adressen valt weinig te zeggen, die komen overal vandaan, mede door het gebruik van VPN- en proxydiensten. Zijn de phishers eenmaal binnen op een mail-account, dan is hun gedrag redelijk voorspelbaar. Is het account niet echt interessant wordt het bijvoorbeeld vooral gebruikt om spam te versturen.

Geld naar een vage 'neef'

Maar toegewijde phishers gaan op zoek naar gevoelige informatie in eerdere mails. Zij sturen phishingmails naar de contactenlijst of mengen zich zelfs in e-mailconversaties in de hoop een transactie uit te lokken. Neelen had op een gegeven moment een phisher in zijn net uit, jawel, Nigeria, berucht om zijn gewiekste cybercriminelen en oplichters. Middels Google Translate probeerde die in gebrekkig Nederlands een geplande transactie weg te sluizen naar 'een neef in Turkije', via Western Union.

Ook hier dus geen hogere cyberkunde. Maar goed, als een account eenmaal is gekaapt, kunnen ook enigszins vreemde mailtjes geloofwaardiger worden vanwege de aangenomen identiteit van het slachtoffer. Kortom, phishing is en blijft een fascinerend fenomeen.

Bron: CXQ

Index

De politie heeft geen zicht op de omvang van identiteitsfraude in Nederland, aangezien maar weinig slachtoffers aangifte doen. Dat blijkt uit onderzoek van de Universiteit van Leiden. Hoewel id-fraude veel aandacht in de media krijgt is er weinig bekend over de huidige situatie in Nederland.

Politie heeft geen zicht op omvang identiteitsfraude

Op basis van een representatieve slachtofferenquête is vastgesteld dat tussen 2008 en 2012 4,6% van de bevolking (van 16 jaar en ouder) hiervan het slachtoffer is geworden. Gemiddeld bedroeg de schade 400 euro per persoon, in ruim 80% van de gevallen werd dit bedrag in die periode volledig vergoed. De maatschappelijke schade, voor banken en hun klanten, bedroeg in deze periode naar schatting 300 miljoen euro.

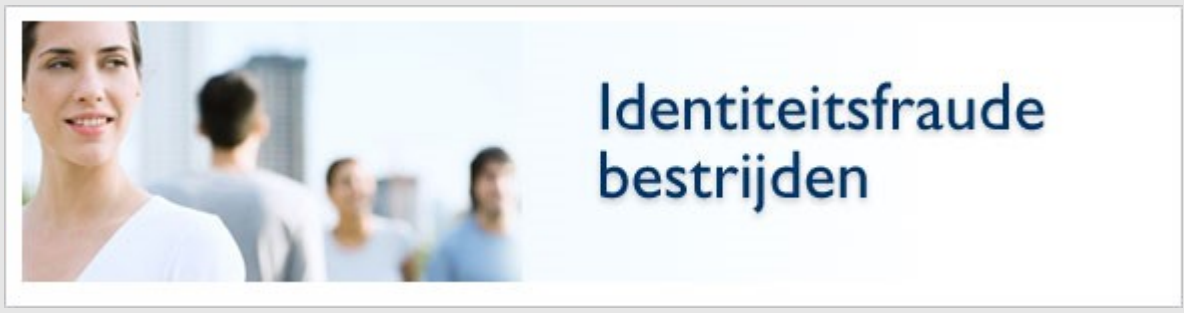
Ondanks het grote aantal slachtoffers blijkt dat slechts 10% aangifte bij de politie doet. Het gaat in dit geval vaak om slachtoffers die ernstige financiële schade hebben geleden. Door het beperkte aantal aangiftes heeft de politie geen goed beeld van identiteitsfraude. "Omdat relatief veel slachtoffers van identiteitsfraude geen aangifte doen van het delict dat hun is overkomen, zoals overigens voor meer vormen van cybercrime geldt, is het werkaanbod dat bij de politie terechtkomt relatief klein", aldus de onderzoekers.

Niet alleen de omvang en de geleden schade zorgen voor een probleem, ook de opsporing en aanpak van identiteitsfraude blijken lastig. Ten eerste vergroot internet de anonimiteit van daders, wat het opsporingsproces kan bemoeilijken. Daarnaast bestaat, ondanks de grote inhaalslag van de afgelopen jaren, nog steeds het probleem dat politiemensen relatief weinig kennis hebben over cybercrime en ook specifiek over identiteitsfraude, zo stellen de onderzoekers.

Schade

In hun conclusie stellen ze dat als naar de omvang en de geleden schade wordt gekeken, identiteitsfraude (4,6% in 2012) niet veel afwijkt van andere vormen van criminaliteit, zoals fietsendiefstal (3,7% van de bevolking werd slachtoffer). Ten tweede is gebleken dat de meerderheid van de slachtoffers uiteindelijk geen schade lijdt, omdat in meer dan 80 procent van de gevallen de schade meestal door de bank wordt vergoed.

Daarnaast lieten de resultaten zien dat wanneer er wel een netto schadebedrag overblijft, meer dan 90 procent van de slachtoffers niet meer dan 50 euro kwijt is. "De uiteindelijke individuele financiële schade lijkt dus, uitzonderingen daargelaten, mee te vallen. Niettemin draaien banken en verzekeringsmaatschappijen wel op voor deze kosten - en uiteindelijk hun klanten", zo laten de onderzoekers weten.



Bron: Universiteit van Leiden

Index

Onderzoekers hebben in zeven populaire babycamera's verschillende lekken ontdekt, waardoor in het ergste geval vreemden op afstand met de beelden kunnen meekijken of in het geval van lokale netwerktoegang de camera volledig kunnen overnemen. Dat meldt beveiligingsbedrijf Rapid7 .

Lek in populaire babycamera's laat vreemden meekijken

De problemen zijn aanwezig in de iBaby M6, iBaby M3S, Philips In.Sight B120/37, Summer Baby Zoom Wifi Monitor & Internet Viewing System, Lens Peek-a-View, Gynoii en TRENDnet WiFi Baby Cam TV-IP743SIC. Vijf van de tien gevonden kwetsbaarheden betreffen "backdoor credentials". Het gaat in dit geval om vaste inloggegevens waardoor een aanvaller bijvoorbeeld via Telnet verbinding met de camera kan maken.

In het geval van de Philips blijkt dat de vaste inloggegevens het ook mogelijk maken om de ingebouwde webserver en het besturingssysteem te benaderen. Andere problemen die de onderzoekers in de babycamera's aantroffen maakten het mogelijk om eerder opgeslagen video's te bekijken, het meekijken met live videostreams, het inloggen op willekeurige camera-accounts zonder wachtwoord en het verkrijgen van beheerdersrechten door een normale gebruiker.

Update

Alle fabrikanten werden begin juli ingelicht, maar updates zijn in een aantal gevallen nog niet beschikbaar. Rapid7 verwijst consumenten meerdere keren naar de fabrikant om informatie over een eventuele firmware-update op te vragen, aangezien de onderzoekers hier niet over beschikken. In het geval van de Philips blijkt dat een andere fabrikant het model heeft overgenomen en vrijdag met een update komt.

Eigenaren van de iBaby M6 wordt aangeraden om de fabrikant over een update te benaderen of anders het apparaat niet te gebruiken. Voor andere camera's wordt geadviseerd die alleen vanaf het lokale netwerk toegankelijk te maken. Volgens de onderzoekers speelt het probleem niet alleen bij babycamera's, maar gaat het hier om een systematisch probleem van het Internet of Things waarbij onveilige producten aan het web worden gehangen.

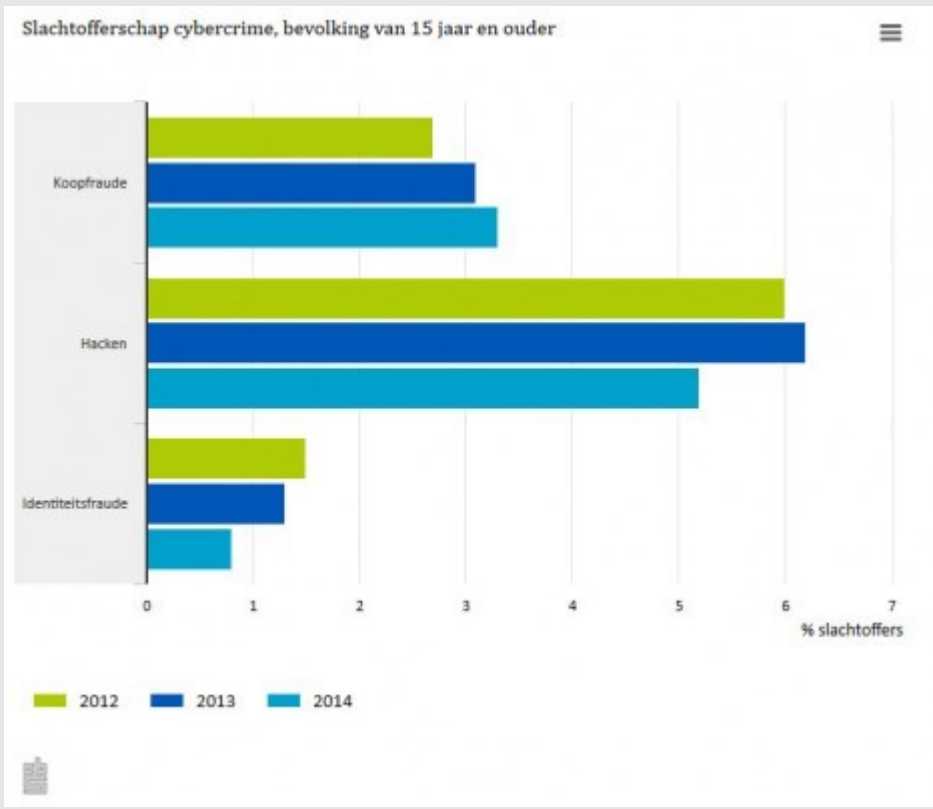
Bron: Rapid 7

Index

Het aantal slachtoffers van online koopfraude is in de periode tussen 2012 en 2014 gestegen. Dat is opvallend, aangezien andere vormen van cybercriminaliteit juist zijn afgenomen. Dat meldt het Centraal Bureau voor de Statistiek (CBS).

CBS: online shoppers vaker slachtoffer cybercrime

In de periode 2012-2014 is het slachtofferschap van identiteitsfraude vrijwel gehalveerd. In 2012 gaf 1,5 procent van de bevolking van 15 jaar en ouder aan slachtoffer te zijn geweest van identiteitsfraude via elektronische betaalsystemen of via het internet. In 2014 was dit 0,8 procent, wat neerkomt op ruim 100 duizend personen. Dit is een relatieve daling van ongeveer 51 procent. Wanneer er wordt gekeken naar de bevolking van 15 jaar en ouder die dagelijks het internet gebruikt, dan is het beeld vrij vergelijkbaar (zie tabel 1 en technische toelichting). De afname komt doordat het aantal skim-incidenten is teruggedrongen. Het aandeel mensen van 15 jaar en ouder waarvan de



bankpas of creditcard is gekopieerd bij een betaal- of pinautomaat daalde van 1,1 procent in 2012 naar 0,4 procent in 2014. Banken hebben de laatste jaren skimmen bemoeilijkt door de magneetstrip op een betaalpas te vervangen door een chip, en door betaalpassen standaard uit te schakelen buiten Europa. Het aandeel dat naar eigen zeggen te maken kreeg met phishing of pharming, bleef gelijk op 0,4 procent, ondanks dat steeds meer mensen hun betalingen en andere bankzaken regelen via internet. Skimming komt nu ongeveer even vaak voor als phishing of pharming.

Hoewel het slachtofferschap van identiteitsfraude is afgenomen, bestaan er nog wel verschillen tussen bevolkingsgroepen (zie tabel 2). Zo blijken de middenleeftijden (25- tot 45-jarigen en 45- tot 65-jarigen) bijna twee keer zo vaak slachtoffer van deze digitale fraude als jongeren (15- tot 25-jarigen) en ouderen (65-plussers). Dat ouderen hier relatief weinig 3.1.1 Slachtofferschap identeitsfraude – naar delictsoort, bevolking van 15 jaar en ouder slachtoffer van worden komt doordat zij minder vaak dagelijks gebruik maken van internet. Als hier rekening mee wordt gehouden door te kijken naar de populatie van dagelijkse internetgebruikers, blijkt het risico op identiteitsfraude vooral laag onder jongeren. Tussen de andere leeftijdsgroepen bestaat dan nog maar weinig verschil. Jongeren zijn het minst vaak slachtoffer van phishing/pharming, ondanks dat de overgrote meerderheid van hen een e-mailaccount heeft (96 procent) en online bankiert (81 procent). Ruim 90 procent van de jongeren geeft ook aan dat ze goed in staat zijn om hun persoonlijke gegevens op computer of internet te beschermen.

Hoogopgeleiden zijn vaker slachtoffer van beide vormen van identiteitsfraude dan laagopgeleiden (zie tabel 2). Ondanks dat meer dan driekwart van de hoogopgeleiden van mening is dat ze hun persoonsgegevens op computer of internet kunnen beschermen, krijgen ze toch vaker met phishing/pharming te maken (0,5 procent). Hoewel laagopgeleiden minder vaak bankieren via internet, verandert het patroon nauwelijks als gekeken wordt naar de betreffende internetpopulatie. Een vergelijkbaar beeld tekent zich af bij mannen en vrouwen. Mannen zijn iets vaker slachtoffer van phishing/pharming dan vrouwen, terwijl ze vaker dan vrouwen aangeven persoonsgegevens te kunnen beschermen. Dat vrouwen minder vaak gebruik maken van internet en internetbanieren lijkt ook hier niet de volledige verklaring; het verschil in slachtofferschap van phishing/pharming blijft bestaan als gekeken wordt naar degenen die dagelijks gebruik maken van internet.

(lees HIER het volledige CBS rapport)

Bron: CBS

Index

Een doorsnee Mac heeft een heleboel achterpoortjes die wagenwijd open staan, aldus onderzoekers, en malware om die lekken uit te buiten bestaat al.

Apple verwaarloost beveiliging: lek tot gevolg

De tijden waarin een Mac-virusbestendig was liggen helaas al ver achter ons. Hoewel het besturingssysteem onbetwistbaar erg veilig is, heeft Apple toch enkele steken laten vallen als het op low-level-beveiliging aan komt. Vorig jaar werd al duidelijk dat ook een Mac onderhevig was aan bootkits, nu wordt duidelijk dat hackers die kwetsbaarheid ook buiten het laboratorium kunnen uitbuiten.

Een bootkit is malware die geactiveerd wordt nog voor een computer het besturingssysteem laadt. Bijgevolg is dergelijke schadelijke software amper te detecteren, en heeft het virus de hele pc aan z'n vingertippen. De bootkit die vorig jaar ontworpen werd kreeg de naam Thunderstrike, maar een aanvaller moest zich fysiek aan de Mac schuiven om het toestel te infecteren.

Thunderbolt

Trammel Hudson, een werknemer van Two Sigma Investments, werkte nu samen met twee andere onderzoekers om dat probleem om te lossen. Dat weet Forbes. De onderzoekers maakten een bootkit die van Mac naar Mac kan springen via Thunderbolt-apparaten.

Volgens Forbes werkt de bootkit enkel wanneer een hacker al administratorbevoegdheden heeft op het toestel. Dat is zeker niet onmogelijk: er zijn genoeg lekken in onder andere Flash of Java die een naarstige computercrimineel de nodige tools kunnen geven om root-toegang te bemachtigen. Vervolgens moet een hacker gebruik maken van de Darth Venamis-kwetsbaarheid. Die kwetsbaarheid, genoemd naar een slechterik star Wars, is al sinds vorig jaar gekend maar Apple repareerde ze nog niet helemaal. Een aanvaller geraakt er mee in de Bios van de Mac.

Firmware-virus

Vanuit de Bios kan de Thunderstrike-bootkit de firmware op Thunderbolt-toestellen aanvallen. Ieder apparaat heeft immers zelf een minimum aan firmware die er voor zorgt dat je geen dood stuk elektronica vast hebt. Door die firmware aan te passen kan Thunderstrike zich via een fireworm verspreiden. Iedere Mac-eigenaar die een geïnfecteerd toestel in z'n computer steekt zou het Thunderstrikevirus oplopen.

In juni bracht Apple een patch voor de Darth Venamis-kwetsbaarheid uit maar die blijkt ontoereikend om Thunderstrike en de fireworm te stoppen. De bootkit kan zich voorlopig nog niet zomaar via het net verplaatsen, maar wie in aanraking komt met geïnfecteerde toestellen krijgt het virus wel binnen. Gelukkig gaat het hier om een proof-of-concept: de hackers hebben het virus niet losgelaten op de wereld. Andere talentvolle computerwetenschappers met een duister kantje zouden de kwetsbaarheid al wel uitgebuit hebben. Detectie van dergelijke firmware-virussen is immers bijna onmogelijk, toch zeker voor een eindgebruiker.

Onvoldoende bescherming

Een Mac beschermen tegen een dergelijke aanval is niet onmogelijk, maar de bal ligt in het kamp van Apple. Intel gaf fabrikanten al de raad specifieke beveiliging in te bouwen, iets waar onder andere Dell en HP, in tegenstelling tot Apple, wel oren naar hadden. Heb je een Mac en ben je bezorgd? Steek dan geen wildvreemde Thunderbolt-toestellen in je computergleuf, je weet nooit wat voor vieze ziektes dat met zich mee brengt.

Bron: TabletGuide.nl

Index

Oude, oudere en zelfs recente IE-versies zijn over een half jaar niet meer veilig. Microsoft trekt een streep in het zand voor security: alleen de allernieuwste versie krijgt support.

Vorige IE-versies gaan in de ban

Het gaat hier om de allernieuwste versie van Internet Explorer (IE) die beschikbaar is voor een bepaalde Windows-versie. Laatstgenoemde moet dan natuurlijk ook nog officieel support genieten. De oudste Windows-versie die Microsoft nu ondersteunt, is Vista dat nog tot april 2017 securitypatches krijgt. Dit geldt voor alle varianten van Vista, dat begin 2012 stilletjes - en op de valreep verlengde support kreeg voor de consumentenuitvoeringen.

IE-wirwar

Van origine draait Internet Explorer 7 op Vista, maar opvolgers IE8 en 9 zijn ook uitgekomen voor dat oudere besturingssysteem. De supportdeadline van Microsoft betekent dat na 12 januari 2016 op Vista alleen IE9 nog updates krijgt. Op Windows 7 is IE11 het hoogst haalbare, terwijl opvolger Windows 8 het met een versie minder moet doen: IE10.

Windows 8 is namelijk op zijn beurt opgevolgd door de gratis update naar 8.1. Die nieuwere versie geldt als de basis voor support, wat dus ook de ingebakken browser betreft. Windows 8.1 draait dan ook wél het nieuwere IE11. Wie na 12 januari 2016 nog Windows 8 gebruikt, met daarop dus IE10, is voortaan permanent kwetsbaar voor dan ontdekte beveiligingsgaten. Hetzelfde geldt voor 'IE-plakkers' op Vista en 7, die zijn begonnen bij respectievelijk IE7 en IE8. Patches voor IE9 komen dan nog wel uit voor Vista, maar niet voor 7.

Legacy en vooruitgang

De ondersteuning voor het nog altijd veelgebruikte Windows 7 loopt tot 14 januari 2020. Met ingang van Windows 10 is Microsoft overgeschakeld op automatische updates.

Tegelijkertijd debuteert in die huidige versie de geheel nieuwe browser Edge. IE wordt nog wel aangehouden, maar dat lijkt vooral voor zakelijk gebruik waarbij interne (web)applicaties of intranetten nog gebonden zijn aan IE-specifieke technieken, zoals ActiveX.

"De meeste klanten gebruiken al de nieuwste versie van Internet Explorer voor hun Windows-besturingssysteem, maar we hebben ontdekt dat er nog altijd fragmentatie is in de install base", schrijft Microsoft in de FAQ over de Internet Explorer Support Lifecycle Policy. Deze fragmentatie "stelt webdevelopers en supportmedewerkers voor problemen". Dit betreft ook Microsoft zelf dat vorige week nog een noodpatch uitbracht voor een groot gat in alle IE-versies op alle Windows-versies. Het officiële advies is dus IE te upgraden, "voor een hoger prestatieniveau, verbeterde beveiliging, betere backwards compatibiliteit en support voor moderne webtechnologieën".

Bron: TabletGuide.nl

Index

Ziggo kampte recentelijk met DDoS-aanvallen, waardoor een groot deel van de gebruikers al twee avonden zonder internet zit. Wat was er aan de hand, en wat kun je er zelf aan doen?

Zo overleef je een nieuwe Ziggo-storing

Bij een DDoS-aanval wordt een groot aantal computers - vaak een botnet, een groot netwerk van computers - ingezet om de servers, in dit geval van Ziggo, te bestoken met verzoeken. De servers kunnen het grote aantal niet aan, wat leidt tot internetproblemen bij gebruikers. Dinsdag en woensdag was Ziggo het slachtoffer van zo'n aanval.

Door de aanval raakten de zogenaamde DNS-servers van Ziggo buiten gebruik. DNS-servers zorgen er simpel gezegd voor dat je op deze website terechtkomt als je www.computertotaal.nl of www.macworld.nl intikt. Omdat het daar spaak liep, kon je niet via Ziggo's DNS-servers op internet komen.

Gelukkig bestaan er veel meer DNS-servers dan alleen die van Ziggo. Door de DNS-server aan te passen in de instellingen van je pc, Mac, smartphone of tablet kun je via bijvoorbeeld de servers van Google toch gewoon internetten. Hieronder lees je hoe je dat doet.

Windows

In Windows ga je naar het Configuratiescherm en klik je op Netwerkverbindingen. Klik met de rechtermuisknop op de verbinding die eigenlijk zou moeten werken en klik op Eigenschappen. In het tabblad Netwerk ga je naar de IPv4-verbinding (of in sommige gevallen IPv6) en klik je opnieuw op Eigenschappen. Typ in het vakje Voorkeurs-DNS-server de getallen 8.8.8.8. Dit is de DNS-server van Google. Als je ook nog een alternatieve DNS-server kunt instellen, kies dan 8.8.4.4.

Mac OS X

Op je Mac ga je via Systeemvoorkeuren naar Netwerk. Selecteer de te repareren verbinding en klik op Geavanceerd. Zoek het tabje DNS en voeg een nieuwe server toe door op het plusje te klikken. Vul hier de server in, bijvoorbeeld 8.8.8.8 voor Google's server, en 8.8.4.4als alternatief.

Mobiel

Ook op Android en iOS kun je de DNS-instellingen makkelijk wijzigen. Op iOS ga je via Instellingen naar Wi-Fi, druk je op het i-teken achter het betreffende netwerk en druk je op de getallen achter DNS. Verwijder de getallen en typ 8.8.8.8 om met de Google-server te verbinden.

Op Android werkt het nagenoeg hetzelfde: Ga naar Instellingen > Wifi, houd je vinger even op het betreffende netwerk en kies Geavanceerde opties weergeven. Hier kun je de bestaande DNS-server veranderen in 8.8.8.8 voor Google's server.

Bron: ComputerTotaal

Index

De Windows 10-paniek du jour gaat momenteel over de feature Windows Hello. Deze zet logischerwijs de webcam aan en dat heeft geleid tot een schrikreactie.

Paniek! Windows 10 zet uitgeschakelde webcam aan

Het nieuwste privacypaniekvoetbal draait om Windows Hello wat een handige beveiligingsfeature moet zijn. Je vindt deze feature (als je een webcam hebt) onder Instellingen > Accounts > Aanmeldingsopties. Hello zorgt ervoor dat je de pc ontgrendeld via je webcam die herkent wie er voor de pc zit. Voor een gezins-pc kan Hello ervoor zorgen dat het familielid dat voor de pc kruipt automatisch wordt ingelogd in zijn of haar profiel.

Camerafeature gebruikt camera

Je zou denken dat mensen die deze feature inschakelen wel begrijpen dat de webcam daarvoor nodig is. Ondanks dat is er ophef ontstaan dat Windows Hello de webcam aanspreekt voor biometrische herkenning, ook als deze is uitgeschakeld.

Mensen die niet beseffen dat apps de camera weer in kunnen schakelen, moeten even naar de FAQ kijken van Windows 10 over de webcam en privacy. Daarin staat expliciet: "Als u Windows Hello inschakelt, zal dit programma uw camera gebruiken om u aan te melden, zelfs wanneer uw camera-instelling is uitgeschakeld. Als Windows Hello is uitgeschakeld, heeft het geen toegang tot uw camera."

Klassieke Windows-toepassingen onvermeld

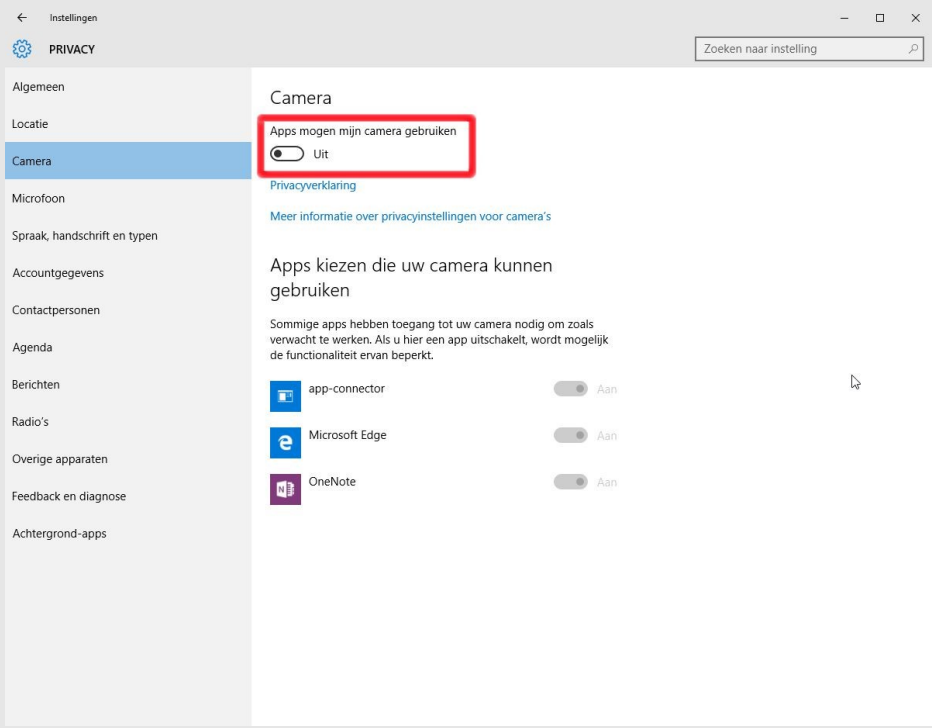
Hoe weet je of je webcam wordt gebruikt? De FAQ: "Als uw systeem van een cameralichtje is voorzien, zal het lichtje gaan branden wanneer de camera in gebruik is. Als uw systeem geen cameralichtje heeft, wordt een melding weergegeven wanneer de camera wordt in- of uitgeschakeld." Let wel, als je geïnfecteerd bent met een RAT - wat vaak voorkomt - gaat het lampje helemaal niet aan.

Je ziet onder de privacyinstellingen een lijst van apps die je webcam afzonderlijk kunnen inschakelen waar je deze apps individueel kunt uitzetten. Maar, zoals een gebruiker op Redditopmerkt, hierbij ontbreken 'klassieke Windows-toepassingen'. Dat zijn volgens Microsoft toepassingen die "Windows-platformonderdelen zoals .NET, COM, Win32 en andere gebruiken." Dit zijn volgens de omschrijving typische bureaubladtoepassingen en geen web-apps.

Apps toegang ontzeggen

Microsoft zegt er niet bij dat deze klassieke toepassingen bij de camera kunnen als die is uitgeschakeld in de privacyinstellingen. Sterker nog, de Windows 10-maker stelt: "Als u de camera-instelling uitschakelt, hebben apps die de camera gebruiken, geen toegang tot de camera."

Maar let op: als bij de privacyinstellingen "Apps mogen mijn camera gebruiken" is ingeschakeld, kunnen apps de camera wel degelijk aanspreken.



Je kunt individuele apps verbieden de camera te gebruiken, maar niet alle applicaties en features worden hierin weergegeven, zoals Windows Hello. Microsoft legt uit in de FAQ: "De Windows Camera-app wordt niet weergegeven in de lijst Apps kiezen die uw camera kunnen gebruiken omdat de app al over een ingebouwd besturingselement beschikt."

Schakel automatisering uit

"De Camera-app staat apps en services alleen toe om de camera te gebruiken wanneer u daarom vraagt; bijvoorbeeld een berichten-app zou de Camera-app gebruiken om een foto te nemen die u kunt delen in een chatbericht."

Kortom, als je niet wilt dat apps de camera inschakelen, ga naar Instellingen > Privacy > Camera en pak zelf de controle over wanneer de camera mag worden ingeschakeld. En ja, dan kun je Windows Hello dus niet gebruiken.

Bron:

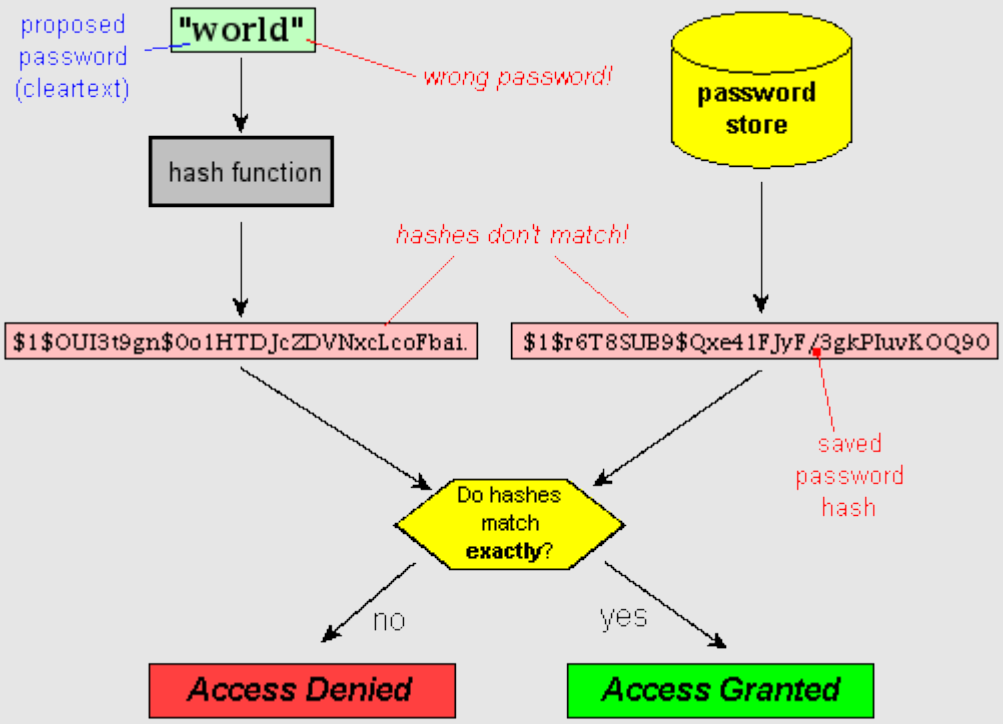
Index

Er gaat bijna geen week voorbij of er is wel weer nieuws over een datalek waarbij miljoenen of zelfs miljardenwachtwoorden worden buitgemaakt.

Maak je wachtwoorden lang en sterk

Wat meestal wordt gestolen is niet het wachtwoord zelf, maar een versie die door een algoritme is gehaald om de inhoud te verhullen. Het nieuwste rapport van Trustwave laat zien dat deze techniek, hashing genoemd, niet helpt wanneer gebruikers domme wachtwoorden maken en dat de lengte van een wachtwoord belangrijker is dan de complexiteit.

Hackers zullen een ingewikkeld wachtwoord als @u8vRj&R3*4h sneller kraken dan een langer wachtwoord als DeKatKrabtDeKrullenVanDeTrap.



Hashen

Het idee achter het 'hashen' van wachtwoorden is dat de beveiligde website nooit het wachtwoord van een gebruiker opslaat. Het bewaart alleen het resultaat van het hashingproces dat overblijft na het draaien van het algoritme. Hashing is een soort van eenrichtingsencryptie. Dezelfde input zorgt altijd voor hetzelfde resultaat, maar vanaf het resultaat kom je nooit terug bij de originele invoer. Wanneer je inlogt vergelijkt de server de gehashte versie van jouw invoer met de opgeslagen hash en als die overeen komen kan je naar binnen.

Het probleem van deze aanpak is dat hackers ook toegang hebben tot de algoritmen om wachtwoorden te hashen. Ze kunnen elke mogelijke combinatie van letters en cijfers voor een bepaalde wachtwoordlengte door het algoritme halen en de resultaten vergelijken met de gestolen gehashte wachtwoorden. Voor elke passende hash hebben ze een nieuw wachtwoord gedecodeerd.

Gedurende duizenden netwerktesten in 2013 en begin 2014 heeft Trustwave meer dan 600.000 gehashte wachtwoorden weten te verzamelen. Hierop draaiden ze speciale software om hashes te kraken en kraakte in enkele minuten meer dan de helft van de wachtwoorden. Over een maand tijd wisten ze maar liefst 90 procent van de wachtwoorden te kraken.

Wachtwoorden - you're doing it wrong

De meeste mensen zullen je kunnen vertellen dat een wachtwoord dat zowel hoofd- als kleine letter bevat, naast cijfers en tekens, het lastigst te kraken is. Dat blijkt niet helemaal te kloppen. Ja, het is lastig voor een kwaadwillende om een wachtwoord als N^a&$1nG te raden, maar volgens Trustwave is zo'n wachtwoord in een dag of vier te kraken. In tegenstelling tot een lang wachtwoord als ZieMaarHoeJeDitRaadtScriptkiddie, waar een hacker al snel een jaar of 18 zoet mee is.

Veel IT-afdelingen bij bedrijven eisen dat je een wachtwoord kiest van tenminste acht karakters, met hoofd- en kleine letters en cijfers. Dit rapport wijst ons erop dat, jammer genoeg, ook 'Wachtwoord1' aan deze eisen voldoet. Niet geheel ontoevallig was dit ook het meest gevonden wachtwoord in het onderzoek van Trustwave.

De onderzoekers constateerden ook dat gebruikers precies doen wat ze wordt gevraagd, maar ook geen stap meer. Toen ze door de collectie wachtwoorden ging spitten bleek dat bijna de helft precies uit de genoemde acht tekens bestaat.

Maak ze dus langer

We hebben dit al vaker gezegd, maar het is het waard om te herinneren. Hoe langer het wachtwoord (of liever zelfs: de wachtwoordzin) hoe lastiger het is voor hackers om dit te kraken. Gebruik een favoriete quote of zinsnede, haal de spaties eruit en je hebt een behoorlijke wachtwoordzin.

Ja, uiteraard zijn er ook andere manieren om wachtwoorden te kraken. In plaats van elke mogelijke combinatie van letters en cijfers te

Bron: PCmag

Index

Mozilla heeft de mobiele Firefox-app een update gegeven, waardoor de browser nog meer op de privacy en veiligheid van gebruiker is afgestemd. Zo wordt de privémodus nog anoniemer, en wordt het veiliger om add-ons te installeren.

Firefox maakt Do Not Track standaard in app

De meest prominente verandering zit in de privémodus. Daarin wordt niet alleen je surfgeschiedenis niet opgeslagen, maar worden ook standaard alle trackers uitgeschakeld.

Do Not Track

Firefox biedt al een paar jaar een Do Not Track-functie aan, waarbij de browser cookies en andere (advertentie)trackers blokkeert. Die functie zat echter verborgen in het menu en moest handmatig worden ingeschakeld.

Trackers handmatig aanzetten

In de nieuwe privé-modus worden die trackers automatisch uitgezet, maar het is wel mogelijk om de trackers op te roepen via een knop in de adresbalk. Daarmee is het mogelijk bepaalde trackers alsnog aan te zetten. Dat is ook wel nodig, want sommige websites werken niet als je trackers uitschakelt.

Add-on-verificatie

Daarnaast worden add-ons in Firefox voortaan ook geverifieerd. De toevoegingen krijgen een eigen cryptografische handtekening, waardoor de browser ziet welke plugins authentiek zijn en welke niet. Als daarbij bijvoorbeeld een add-on wordt gevonden met malware, wordt de handtekening daarvan direct geblokkeerd zodat andere gebruikers er ook geen last van hebben.

De veranderingen zitten in v42, die op dit moment nog in bèta-fase zit.

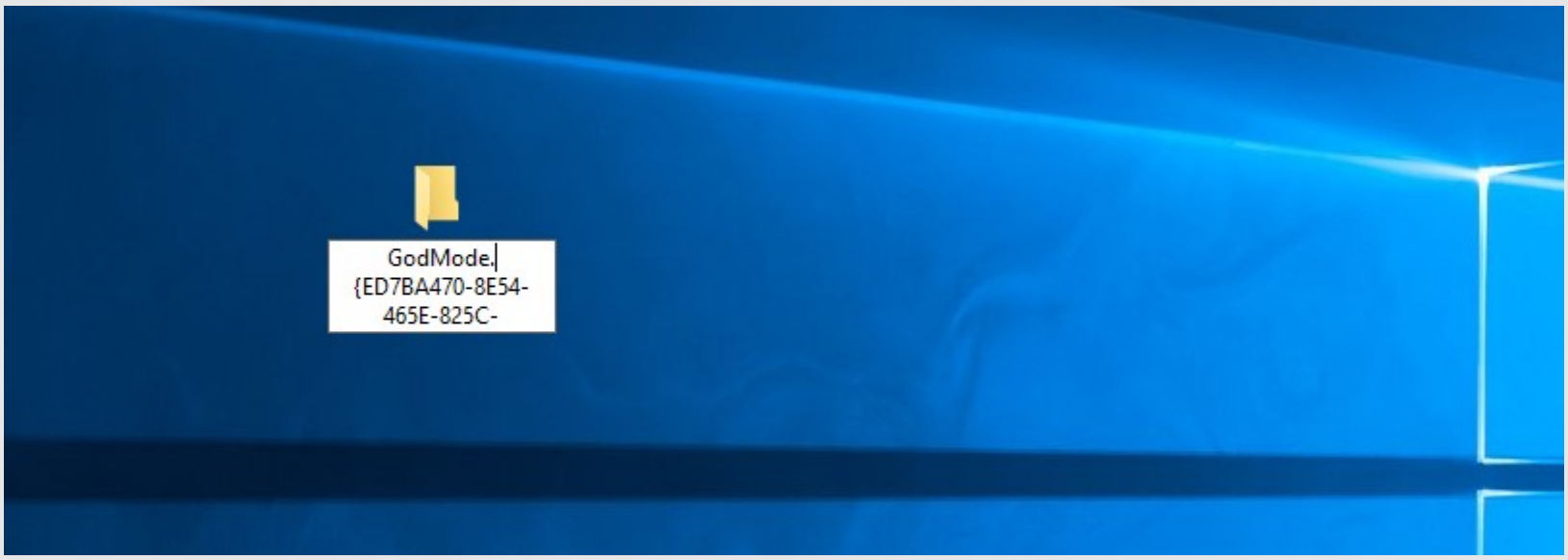
Bron: TabletGuide.nl

Index

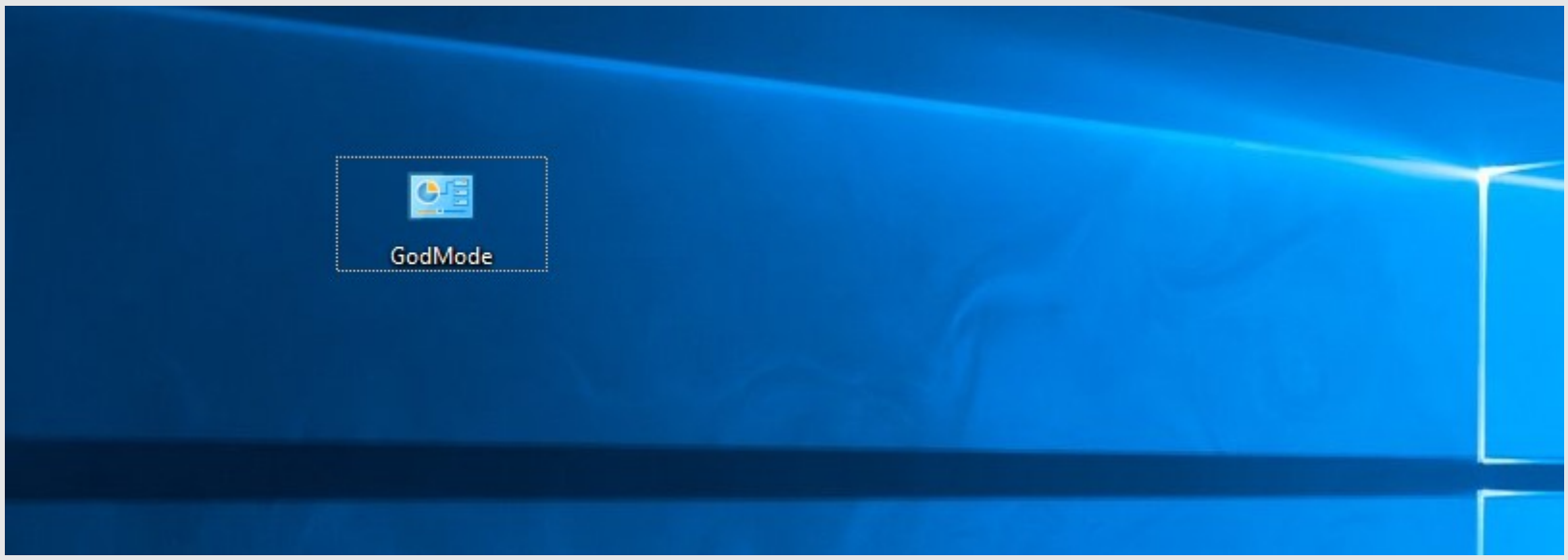
Windows 10 kent veel opties en deze kunnen goed verstopt zitten, zelfs nu het instellingenmenu een welkome opfrisbeurt heeft gekregen. Een geheime feature biedt uitkomst: God Mode. Zo zet je het aan.

Windows 10 overzichtelijk beheren met God Mode

God Mode bestaat al langer in Windows, en deze is in Windows 10 op dezelfde manier te activeren als altijd. Heel simpel: maak een nieuwe map aan en geef deze de naam 'GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}' - minus de aanhalingstekens.



Nadat je op Enter drukt, verandert het icoontje. Als je wilt, kun je God Mode nu gewoon hernoemen (F2).

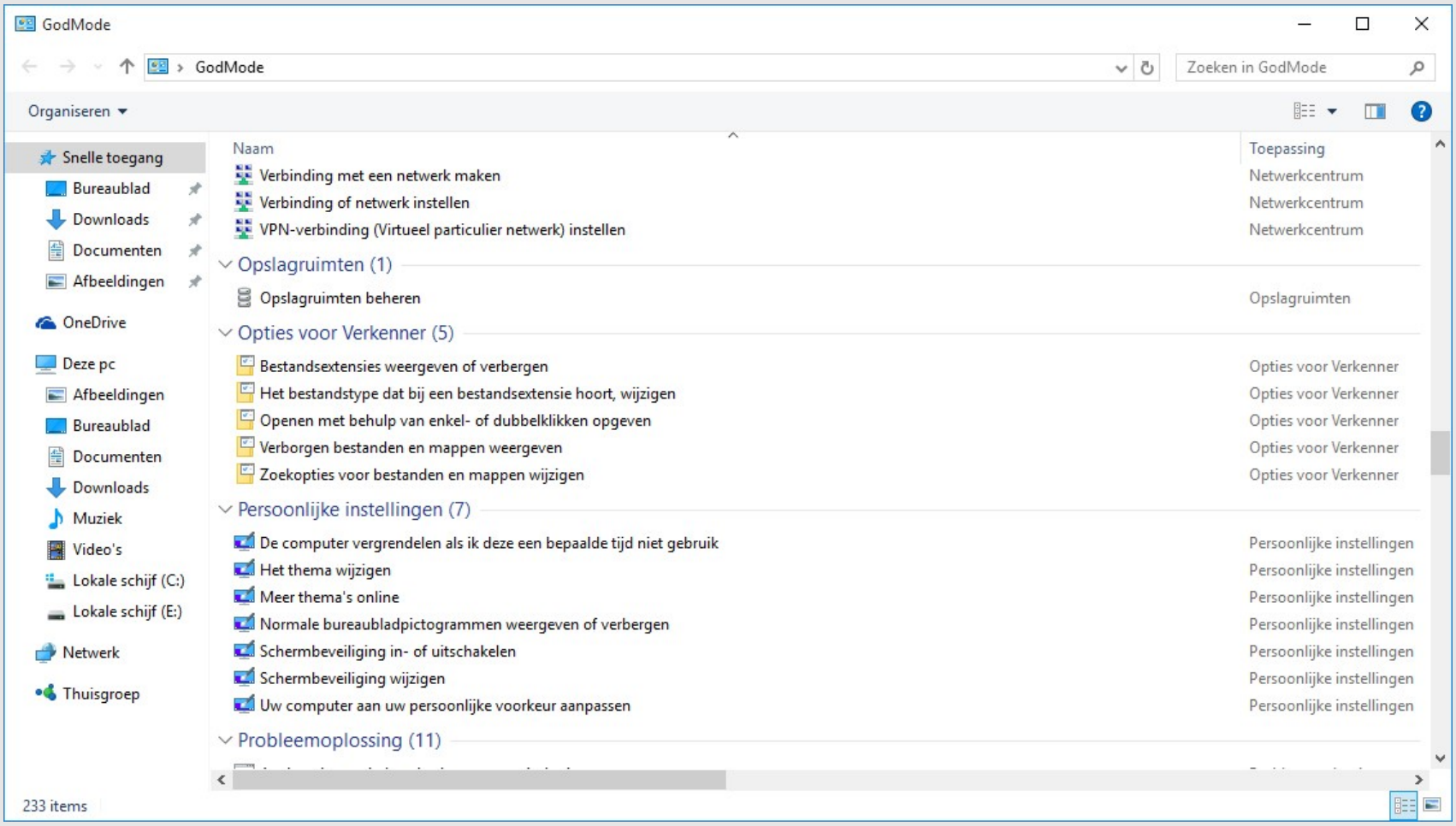


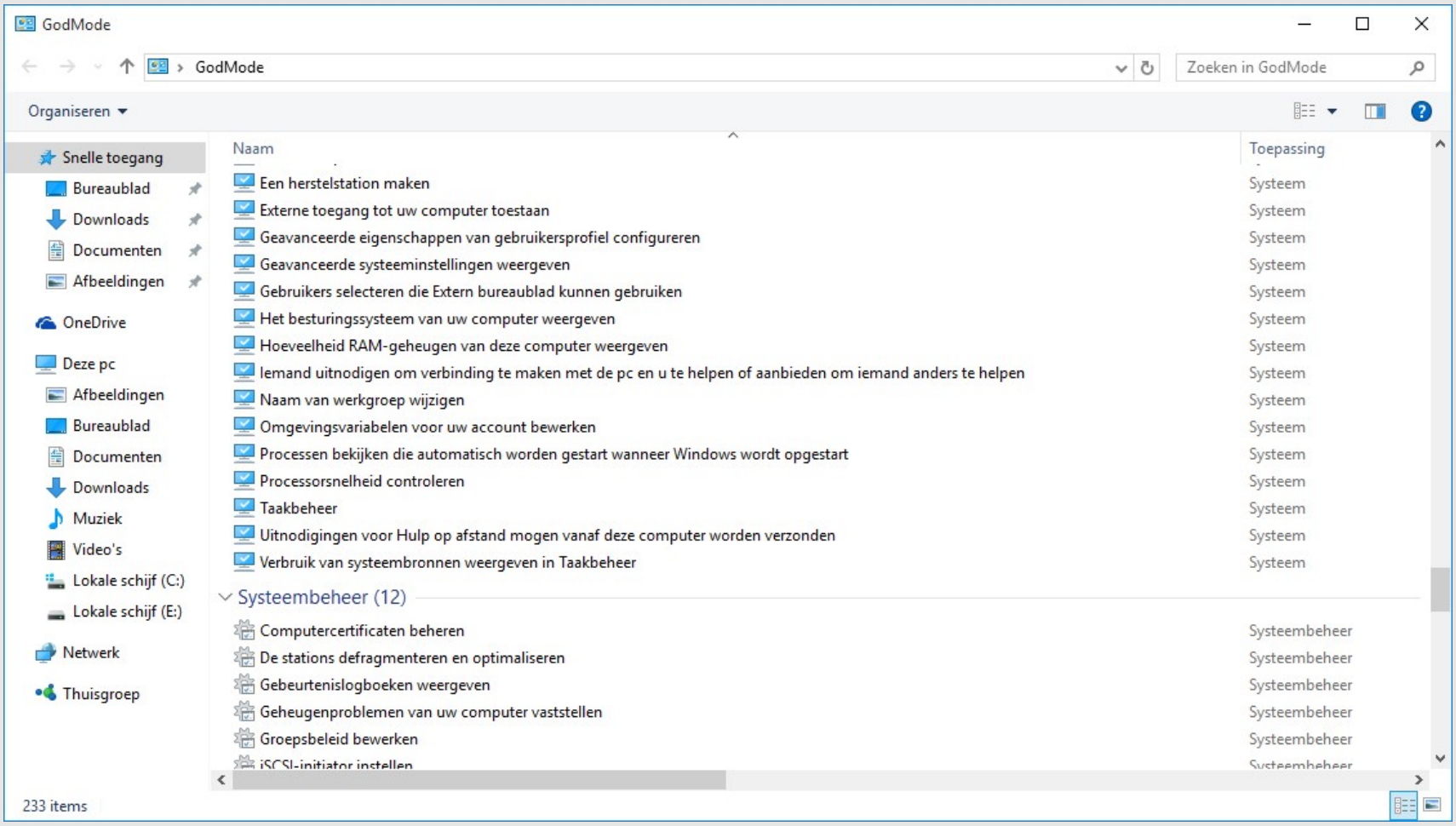
Dubbelklik om de map te openen en je ziet alle geavanceerde opties en tools van Windows 10 op een rijtje. Handig gerangschikt in thema's, op alfabetische volgorde. Zo hoef je niet langer eindeloos tabbladen in afzonderlijke menu's af te struinen.

Bron: PCM web

Index

GodMode





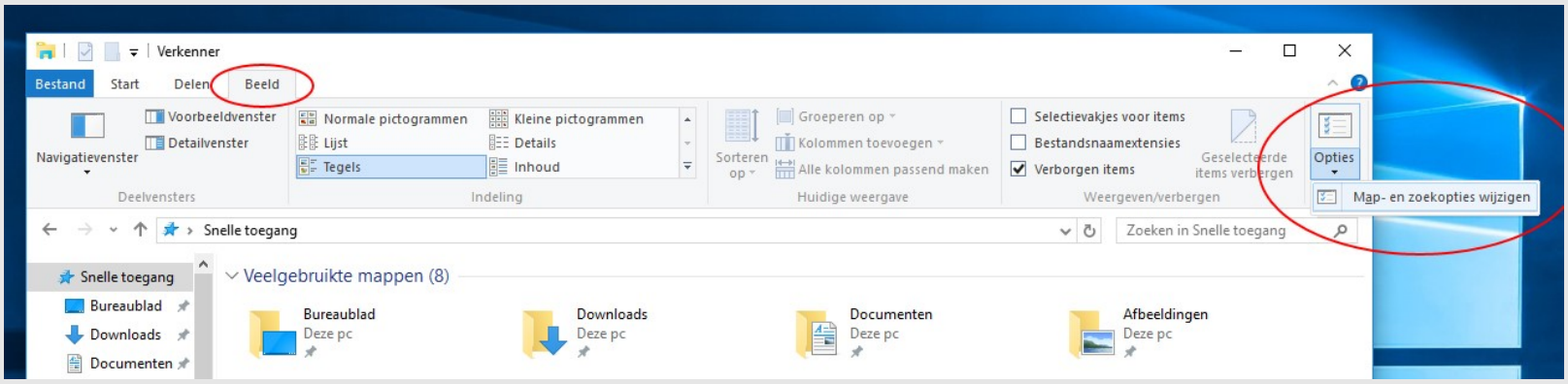
Bron: PCMweb

Index

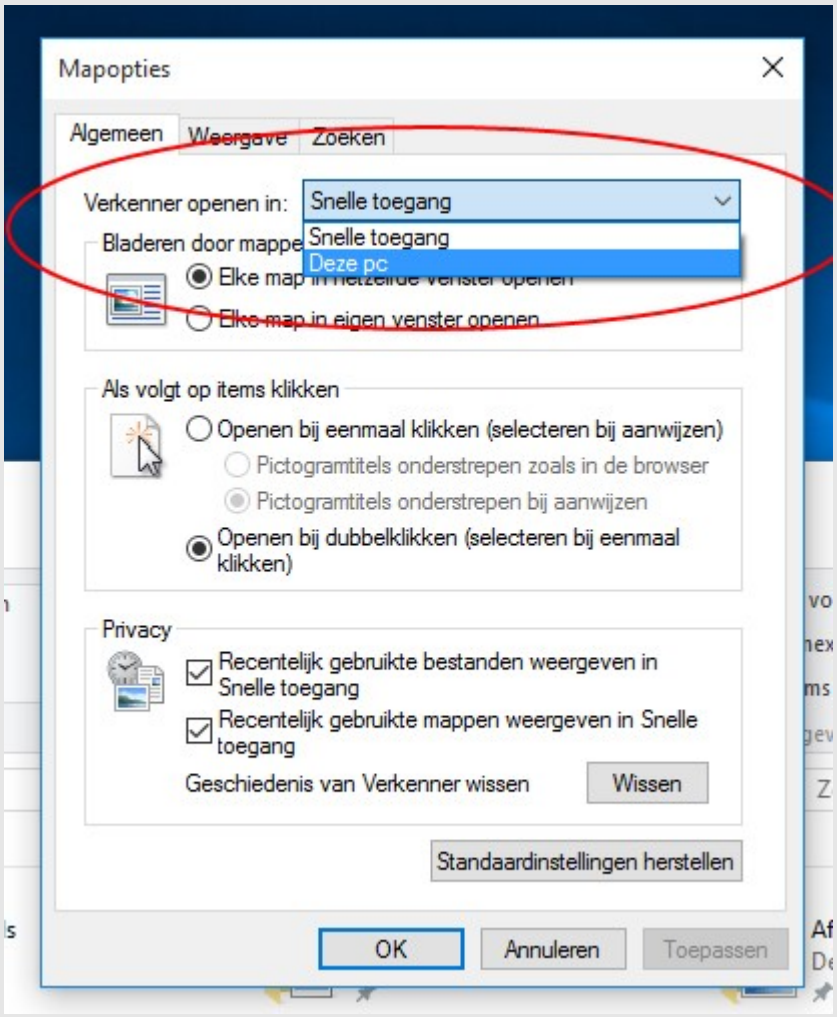
De Verkenner is in Windows 10 uitgerust met een nieuwe functie: Snelle toegang. De mappen die je het meest gebruikt, zie je hier in één oogopslag. Wil je liever dat de Verkenner gewoon weer direct 'Deze pc/Deze computer' toont? Het is in een paar muisklikken geregeld.

Windows 10: Snelle toegang vervangen voor Deze pc

Open de Verkenner onder in de taakbalk of druk **Windows-toets + E**. Kies bovenin voor **Beeld** en klik helemaal rechts op **Map- en zoekopties wijzigen**.



Onder het tabblad **Algemeen** vind je meteen wat je zoekt. De bovenste optie is **Verkenner openen in**. Klik op Snelle toegang om een dropdown menu te openen. Kies daar 'Deze pc'.



Druk tot slot op **OK** om de aanpassingen door te voeren.

Index

Bron: Computer Idee

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……..)

Bron: YouTube

Index

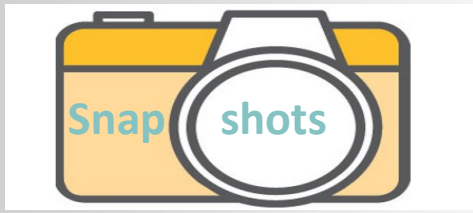
Software schatkist

De kist is gevuld met fraaie software en naslag.

Nieuwsgierig?

Open de kist middels de sleutel en ontdek…….

Index



Uber is slordig in het aannemen van chauffeurs voor zijn vervoersdienst. Daardoor kon zelfs een veroordeelde moordenaar binnenlopen, en kregen ook nog eens een aantal zedendeliquenten een plaatsje achter het stuur. Volgens openbaar aanklager George Gascon is de claim van Uber dat het nauwgezet de achtergronden van zijn nieuwe chauffeurs onderzoekt, niet waar. Hij zegt dat in een rechtszaak in San Francisco, waarin Uber zich moet verantwoorden voor zijn aannamebeleid. In totaal zouden zeker 25 veroordeelde misdadigers zich in het bedrijf hebben weten te solliciteren. "Maar dat is slechts het topje van de ijsberg", onderstreept Gascon.

———————————————————

Een officier van Justitie zou het Facebook- en Hotmail-account van een politieman waarmee ze een conflict heeft gekaapt hebben. De officier is geschorst. Dat zie je niet elk dag: een officier van Justitie die een politieagent hackt. Ten minste, dat is de verdenking, al zijn de omstandigheden mysterieus te noemen. Het onderzoek loopt al sinds 2013. Het Nederlands Forensisch Instituut zou hebben vastgesteld dat via het draadloos netwerk in de woning van de officier de accounts van de politieman zijn gekraakt. Maar ook zou zijn vastgesteld dat dit niet vanaf een van haar computers kan zijn gebeurd. Momenteel zou worden onderzocht of er dan iemand anders zou hebben ingebroken op het netwerk van de officier. Zij is sinds eind vorig jaar geschorst, het OM houdt het op een 'integriteitskwestie'. De officier zou een conflict hebben met de agent, en dat hebben verzwegen.

———————————————————

Dat Whatsapp goed werkt bij allerlei buurtinitiatieven, preventieprojecten, winkeliersverenigingen en wijkbewoners is inmiddels meer dan bekend. Veel winkeliers in centrum, straat of wijk hebben zulke groepen, waarmee ze elkaar waarschuwen als ze een winkeldief betrappen of wanneer ze ontdekken dat er iets gestolen is. ‘Dan zoeken we beelden van de beveiligingscamera’s terug en plaatsen we een foto van de dader in de Whatsapp-groep’, zegt ook een supermarktondernemer in Lelystad. Dat werkt. ‘De doorgewinterde boefjes weten dat ze in de gaten worden gehouden’. Omdat de politie vaak aan dit soort groepen is toegevoegd, gaat die actief mee in de meldingen. Ondernemers doen weer (of vaker) aangifte, de politie kan simpel terugkoppelen wat er na die aangifte gedaan is. Ook gemeenten hebben Whatsapp ontdekt. Maar gemeentelijke dienstverlening blijkt dan toch iets anders. Zo kunnen inwoners van Lelystad sinds kort via Whatsapp vragen stellen over de vele wegwerkzaamheden in de stad. De gemeente behandelt die vragen dan ‘tijdens kantooruren, van maandag tot en met vrijdag van 8.30 uur tot 17.00 uur’.

———————————————————-

Nieuw onderzoek van VDMMP in opdracht van het Rode Kruis toont (weer eens) aan hoe belangrijk sociale media zijn als informatiebron bij noodsituaties. Anno 2015 verwachten mensen dat de betrokken instanties snel reageren en antwoorden via kanalen als Whatsapp, twitter, facebook en zelfs YouTube. Sterker nog, meer dan de helft van de respondenten geeft aan dat ze hulpdiensten via sociale media benaderen indien het telefoonnetwerk overbelast is. Bij noodsituaties halen mensen steeds vaker informatie van sociale media, of ze daar nu bij aanwezig zijn of niet. Volgens onderzoeker Niek van As van VDMMP is sociale media één van de informatiebronnen, naast familie, buurtbewoners, hulpdiensten en andere media. Maar op die sociale media komt alles tezamen. Het onderzoek ‘Sociale media bij noodsituaties’ (voor het eerst in 2012 uitgevoerd, nu herhaald) laat, net als veel andere onderzoeken, zien dat sociale media vooral worden gebruikt om informatie te ontvangen bij noodsituaties en minder om zélf informatie te delen. Van As: ‘Je zag bijvoorbeeld na de ramp met de MH17 dat 45% van de respondenten sociale media gebruikte, maar 90% daarvan alleen om informatie te verzamelen’. Het Rode Kruis heeft sinds enige tijd de website Ikbenveilig.nl, maar nog weinig mensen kennen die site. De website is bedoeld om het grotere sociale netwerk buiten directe familie en vrienden te bereiken in geval van nood.

———————————————————-

Er gaat iets niet goed bij de Nederlandse informatieverzoeken aan Yahoo – net als in 2014 heeft Yahoo ook in 2015 alle Nederlandse verzoeken om gebruikersgegevens geweigerd, blijkt uit het nieuwste Transparantierapport. Politie en justitie vroegen in de eerste helft van 2015 tien keer om gegevens, over dertien accounts, maar er is nul keer data verstrekt. Onduidelijk is de reden van de weigering. Volgens de eigen voorwaarden weigert Yahoo als er problemen met het verzoek zijn. Het kan zijn dat een land informatie vraagt buiten de jurisdictie om, of dat er gegevens worden gevraagd die niet rechtmatig zijn te verkrijgen. Nederland is overigens niet het enige land in deze positie: Griekenland zag alle negen verzoeken geweigerd, Frankrijk zag 645 van de duizend verzoeken niet gehonoreerd worden en Denemarken, ach de Denen, kregen zelfs hun ene verzoek niet gehonoreerd. In totaal kreeg Yahoo overigens ruim 15 duizend verzoeken om informatie. Ongeveer eenderde werd geweigerd.

———————————————————

De Nederlandse Vereniging van
Banken meldt een stijging van de fraude met internetbankieren en skimming. Werd in de eerste helft van 2014 nog voor 2,1 miljoen euro gefraudeerd, in de eerste helft 2015 was dit 3,1 miljoen euro. De reden is dat internetcriminelen hun phishingmethoden ‘perfectioneren’ – vooral phishing zorgt voor veel fraude. Via malware is drie ton gestolen (vorig jaar 380 duizend euro), via skimming acht ton (vorig jaar 640 duizend euro).

———————————————————

Het aanbod gestolen persoonsgegevens is tegenwoordig zo groot dat je voor minder dan een euro adressen, telefoonnummers, burgerservicenummers, bank- en creditcardgegevens kunt kopen. Albert Kramer van beveiliger Trend Micro zei op BNR dat ook de tools die cybercriminelen van oudsher gebruiken, steeds meer in het bereik van ‘gewone’ mensen komen. Volgens hem doen bedrijven nog veel te weinig om zich te wapenen tegen onlinerisico’s. Er kan volgens hem nog veel meer aan preventie gedaan worden. En de overheid zou strengere regels moeten hebben om bedrijven op die verantwoordelijkheden te wijzen.

———————————————————

Tussen 26 oktober en 6 november as loopt (voor de vierde keer) de campagne Alert Online. De overheid wil hiermee burgers ‘securitybewuster’ maken op internet. De campagne is een gezamenlijk initiatief van overheid, bedrijfsleven en wetenschap en moet kennis over online
veiligheid vergroten, ‘bij jong en oud en van werkvloer tot boardroom’. De nadruk ligt dit jaar op het toepassen van kennis en op cyberveilig gedrag: het stimuleren van werknemers en andere gebruikers om te handelen naar wat ze weten.

Index

Geheel ter goede trouw en indachtig alle twitterrichtlijnen plaatste wijkagent Benjamin de Vries uit Nunspeet een foto op twitter. Daarop lag een 15-jarig meisje laveloos op een bankje. De Vries zette er een tip voor ouders bij: ‘Weet wat je kinderen doen zo laat nog op straat…’ Vervolgens stak een twitterstorm op. Hoewel het meisje onherkenbaar was gefotografeerd – geen gezicht in beeld, wel braaksel – zou ze herkend kunnen worden. En toen BNN-presentator Tim Hofman de tweet oppikte, waren de rapen helemaal gaar. Hofman richtte zich persoonlijk tegen De Vries, die de foto uiteindelijk verwijderde. Volgens een woordvoerder is De Vries ‘geschrokken van alle ophef’ maar heeft hij niks fout gedaan. De tweet zal ook geen gevolgen voor hem hebben. ‘Zijn boodschap blijft overeind: hij wilde zijn zorg uitspreken over het feit dat een 15-jarige laveloos op straat lag, ook richting de ouders’. En al doende leert men, nietwaar?

———————————————————-

Onderzoekers van de Universiteit Tilburg melden dat een ‘spectaculaire daling’ in het aantal woninginbraken in Tilburg toe te schrijven is aan het ‘afschrikeffect’ van de vele Whatsapp-groepen. Ze onderzochten het effect van Whatsapp-buurtwachten nu zo’n beetje in vrijwel elke Nederlandse gemeente zo’n groep actief is. Inbrekers blijken volgens de onderzoekers massaal de buurten te mijden waar bewoners elkaar online waarschuwen. ‘Inbraken worden vaak gepleegd door lokale inbrekers. Als ze weten dat er een whatsapp-groep actief is, haken ze af’, aldus onderzoeker Martijn Akkermans. Buurtbewoners zijn daarnaast mogelijk alerter geworden en eerder geneigd de politie te bellen als ze iets verdachts zien. Het aantal inbraken in de 35 onderzochte buurten daalde van gemiddeld zestig naar dertig per maand. Volgens Akkermans is de Tilburgse aanpak een ‘schoolvoorbeeld voor de rest van Nederland’. Voorwaarde is wel dat er per wijk voldoende mensen meedoen én dat de gemeente de Whatsapp-groepen ‘strak coördineert’. Deelnemers zijn geselecteerd en uitgenodigd door de gemeente, in het protocol staat dat eerst 112 gebeld moet worden en dat een lid van de groep het bericht online zet. Pas dan kunnen andere deelnemers reageren. Alle berichten worden doorgezet naar de politie die op deze manier al tien inbrekers op heterdaad wist te betrappen of aan te houden. Bij de nationale politie zegt Sybren van der Velden, landelijk coördinator woninginbraken, dat Whatsapp-groepen ‘extra ogen en oren in de wijk’ zijn. ‘Op deze manier kan snel veel informatie worden verzameld die de politie kan helpen bij het sneller opsporen van verdachten’.

———————————————————

Er is vertraging bij het indienen van het wetsvoorstel dat (opnieuw) een bewaarplicht voor telecomgegevens moet regelen. Het kabinet werkt daaraan sinds rechtbank Den Haag begin 2015 vonniste dat de Nederlandse regeling ongeldig was – het Europees Hof bepaalde in 2014 al dat de Europese bewaarrichtlijn ongeldig was. Minister Ard van der Steur (VenJ) schrijft de Kamer dat er meer tijd nodig is om te onderzoeken wat de precieze gevolgen zijn van deze Europese uitspraak. Het kabinet blijft stellen dat de bewaarplicht nodig is voor de bestrijding van ‘ernstige misdaad’. Niet bekend of duidelijk is echter in hoeverre opsporingsdiensten er de afgelopen maanden last van hebben gehad. In ieder geval gaat ook het komende voorstel uit van een bewaarplicht van twaalf maanden voor telefoongegevens en zes maanden voor internetgegevens.

———————————————————

De rechtbank in Hannover, Duitsland heeft een man (22, uit Hamelen) veroordeeld tot vier jaar en elf maanden cel voor het verkrachten van een 11-jarige jongen in Mechelen, België. De vader (45) van het jongetje had zijn zoon via internet aangeboden. Hij kwam in contact met de Duitser die enkele weken later naar België reisde om de jongen te misbruiken. De vader filmde de zaak en deelde de beelden op internet. De beelden doken op in een Australisch onderzoek naar internetpedofielen. Rechercheurs van de politie in Australië ontdekten dat de beelden in België gemaakt waren. Daarna werd de vader opgepakt, de Duitse politie ingelicht en de Duitse verdachte gearresteerd. De Belgische vader zit (uiteraard) nog vast en wordt later berecht.

———————————————————-

Cybercrime verdwijnt. Beter gezegd: de aparte benaming cybercrime wordt overbodig nu steeds meer misdrijven een digitale component hebben. Volgens Aalbergsberg is kinderporno het snelst groeiende misdaadsegment van dit moment, gevolgd door huiselijk geweld en it-gerelateerde fraude. De politie moet daarop inspelen. ‘De aloude gedachte – die nog stamt uit de tijd van Napoleon – dat het simpel vergaren van informatie genoeg is, heeft zijn langste tijd gehad’. Daarnaast kent internet ‘geen territorium meer’, wordt de politie ‘elk jaar een jaartje ouder, terwijl de criminelen vooral in de groep van 18 tot 25 jaar blijven zitten’. Ook andere sprekers zagen hoe de wereld verandert. ‘Misdaad kan gepleegd worden vanaf iedere pc, dat maakt het zo gevaarlijk’, zei NCSC-directeur Hans de Vries, die maar weer eens wees op het belang van (internationale) samenwerking. De Vries wees ook op het gebrek aan fall-back situaties: ‘bij hoeveel banken kun je nog aan het loket terecht’.

———————————————————-

De rechtbank in Haarlem heeft een oud-agent die via internet zijn politiekleding aanbood, veroordeeld tot dertig uur voorwaardelijke taakstraf met een proeftijd van twee jaar. De oud-agent, sinds 2013 op non-actief en in 2015 ontslagen, dacht dat zijn oude uniformen wel interessant konden zijn voor toneelverenigingen of verzamelaars. Hij wist naar eigen zeggen niet dat hij zijn uniform moest indienen bij vertrek uit het korps. Een waarschuwing tegen die online verkoop werd door de korpsleiding gedaan op het moment dat de man wegens ziekte thuis zat. Pas toen zijn oud-chef hem belde, snapte hij dat hij fout zat. Opvallend is dat vele andere agenten ook kleding aanbieding op internet. De rechtbank stelt dan ook dat de politie ‘actiever had kunnen zijn’ in het terugkrijgen van de dienstkleding. Precies die nalatigheid had de advocaat van de verdachte aangevoerd. Waarom deze oud-agent wel vervolgen en al die andere niet? Hoe dan ook, de uitspraak van de rechter kan betekenen dat andere agenten die online politiekleding aanbieden, ook vervolgd zullen worden.

Index

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

POLITIE Meldpunt internetoplichting

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

Index

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.

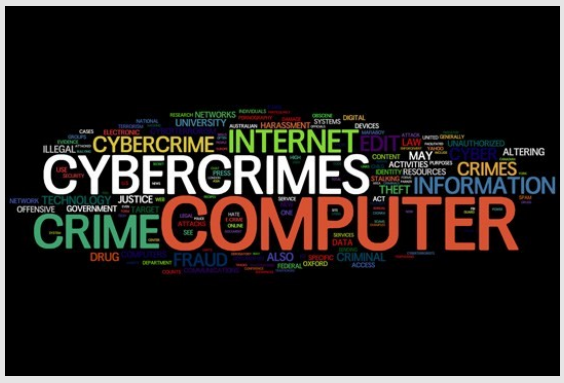
Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



Index

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.

————————————————————————

Index