Jaargang 5 December 2016

Secure Computing Magazine

Rubrieken:

Met de CTRL toets + het scrolwieltje van uw muis , kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen.

INDEX

AKTUEEL

Zelfs wijkagent moet strijden tegen internetcriminelen

Da's logisch he? Volgens bijzonder hoogleraar politiestudies en cybersafety Wouter Stol (NHL) moet elke agent zaken op internetkunnen oplossen. 'Iedereen kan te maken krijgen met online pesten of identiteitsfraude'.

Stol ziet echter ook dat de politie in verschillende lagen in de organisatie kennis en kunde tekort komt. En waar in 2015 ongeveer een op de negen Nederlanders slachtoffer werd van cybercrime, werden er in dat jaar slechts 130 daders opgepakt, minder dan 1% van het aantal aangiftes.

Stol wijt dat vooral aan kennisgebrek en wil daarom dat 'iedereen binnen de politie' basiskennis heeft van cybercrime en ict, 'van wijkagent tot chef'. Het gaat dan niet om pure cybercrime maar vooral om zaken als hacken en ransomware, om kleinere conflicten die online uitgevochten worden.'Waar buren vroeger bij een ruzie nog elkaars ruiten ingooiden, maken ze elkaar nu belachelijk op internet'.

Als wijkagenten ook kennis hierover hebben, kunnen ze dit soort conflicten makkelijker herkennen en voorkomen, denkt Stol. Advocaat Aldo Verbruggen, voormalig officier van justitie, gaat nog een stap verder. Volgens hem heeft ook het OM te weinig kennis en kunde in huis. 'En als je kijkt naar degenen die digitaal rechercheren, dan is dat gewoon C-materiaal vergeleken met de echte specialisten.

De overheid is kwantitatief en kwalitatief onderbezet'. Stol ziet de uitdaging vooral in het verkleinen van de afstand tussen 'de normale agent en het team vol specialisten' – 'die komen niet heel makkelijk in contact met elkaar'.

Bezoek de website voor meer actuele onderwerpen !

Politie mag kwetsbaarheden in software gebruiken om te hacken

Het kabinet vindt dat opsporingsdiensten gebruik moeten kunnen maken van kwetsbaarheden in software om verdachten te kunnen hacken. Een slechte zaak, zegt burgerrechtenorganisatie Bits of Freedom: "De overheid vindt hacken belangrijker dan onze digitale veiligheid."

Het kabinet reageert hiermee op de vragen van D66-Kamerlid Verhoeven over het gebruik van zogeheten zerodays: kwetsbaarheden in software die niet door de fabrikant zijn gedicht. Zerodays zijn een veelgebruikte manier om in te breken op onder andere smartphones en computers.

Kwetsbaarheden heb je nooit alleen

Zerodays mogen door de Nederlandse opsporingsdiensten worden ingezet om verdachten te hacken, vindt het kabinet. Tegelijkertijd benadrukt het kabinet dat digitale veiligheid in de samenleving belangrijk is. Een opvallende tegenstrijdigheid, vindt Ton Siedsma van Bits of Freedom: "Dat spreekt elkaar tegen."

"Als de politie kennis over kwetsbaarheden in software achter gaat houden, kan het lek door iedereen worden misbruikt", zegt Siedsma. "Het is een illusie dat alleen Nederland deze kennis over een kwetsbaarheid heeft. Ook buitenlandse overheden en criminelen kunnen deze kwetsbaarheden misbruiken."

Hoe komen opsporingsdiensten aan zerodays?

De vraag blijft vooral: hoe komt de overheid aan zerodays. In de reactie schrijft staatssecretaris Dijkhoff van Veiligheid en Justitie dat opsporingsdiensten zelf naar dit soort kwetsbaarheden zoeken. "Maar de praktijk leert dat dit soort kwetsbaarheden met name worden ingekocht", zegt Siedsma, die het bedrijf Hacking Team als voorbeeld noemt.

Hacking Team biedt software aan die kwetsbaarheden misbruikt om doelwitten te hacken. Er is veel kritiek op Hacking Team: nadat het Italiaanse bedrijf zelf is gehackt werd duidelijk dat Hacking Team zijn software ook levert aan totalitaire regimes als Bahrein en Saoedi-Arabië.

Ook de Nederlandse overheid is klant bij dit soort bedrijven. Zo gebruikt de Nederlandse politie apparaten van Cellebrite waarmee in beslag genomen telefoons kunnen worden uitgelezen. Binnenkort wil de politie ook op afstandverdachten kunnen hacken.

Ransomware

Volgens Siedsma zijn zerodays niet de enige manier om digitaal in te breken bij een verdachte: "Als de verdachte zijn beveiliging niet op orde heeft, bijvoorbeeld als hij een verouderd besturingssysteem gebruikt, kan er nog steeds worden ingebroken."

"Als de overheid de digitale infrastructuur verbetert, zou criminaliteit op het internet ook worden aangepakt, denkt Siedsma: "Ransomware wordt bijvoorbeeld verspreid via kwetsbaarheden in software, en daarom moeten die kwetsbaarheden moeten dus worden gedicht."

CDA en VVD willen wet computercriminaliteit snel behandelen

CDA en VVD willen twee wetsvoorstellen die de politie en inlichtingendiensten meer bevoegdheden geven snel behandelen, zo blijkt uit een motie die door beide partijen is ingediend. Het gaat om de Wet computercriminaliteit III en de modernisering van de Wet op de inlichtingen- en veiligheidsdiensten 2002.

De wet computercriminaliteit III werd vorig jaar december al bij de Tweede Kamer ingediend, maar is nog altijd niet behandeld. Het voorstel geeft politie de bevoegdheid om op afstand op de systemen van verdachten in te breken. De modernisering van de Wet op de inlichtingen- en veiligheidsdiensten werd in april gepresenteerd. De ministerraad stemde er toen mee in dit wetsvoorstel voor advies aan de Raad van State te zenden. Het streven was het wetsvoorstel en het advies van de Raad van State nog voor de zomer van dit jaar aan de Tweede Kamer voor te leggen, maar dat is niet gelukt.

CDA-Kamerlid Van Toorenburg en VVD-Kamerlid Tellegen willen dat er met beide wetsvoorstellen haast wordt gemaakt. "Overwegende dat twee belangrijke wetsvoorstellen die dienstig kunnen zijn in de strijd tegen zware criminaliteit en terreurbestrijding nog niet plenair (Wet computercriminaliteit III) en schriftelijk (Wet op de inlichtingen- en veiligheidsdiensten 2002) zijn behandeld in de Kamer en al langere tijd bij de regering liggen; verzoekt de regering, deze wetten zo spoedig mogelijk na het herfstreces en in elk geval ruim voor het kerstreces aan de Kamer te zenden, zodat de Kamer deze als prioritair kan behandelen", aldus de motie die tijdens het debat over mogelijke plannen voor een aanslag op Schiphol werd ingediend.

Europol start campagne voor beveiligen smartphones

Europol is een campagne gestart om ervoor te zorgen dat particulieren hun smartphone tegen malware beschermen, hoewel dit volgens experts op dit moment helemaal geen dreiging voor Europese smartphonegebruikers is. De opsporingsdienst stelt dat mobiele malware is doorgebroken, maar geeft geen exacte cijfers over de omvang, behalve dat bij verschillende politieonderzoeken in 14 landen mobiele malware is aangetroffen.

Om ervoor te zorgen dat gebruikers maatregelen nemen vindt er in 22 EU-landen deze week een campagne plaats. Daarnaast heeft Europol een pagina met verschillende beveiligingstips gegeven. Zo wordt aangeraden om alleen apps van betrouwbare bronnen te downloaden en voor het downloaden eerst de app en ontwikkelaar te verifiëren, alsmede de gevraagde permissies te controleren.

Verder moeten gebruikers hun besturingssysteem en apps up-to-date houden, iets dat in het geval van Android nog altijd lastig blijkt te zijn, aangezien fabrikanten niet alle toestellen van updates blijven voorzien. Ook wordt het uitschakelen van wifi en bluetooth aangeraden als de functies niet in gebruik zijn. Tevens waarschuwt Europol voor het jailbreaken van toestellen, omdat dit de beveiliging kan verzwakken.

Wet op de inlichtingen- en veiligheidsdiensten

Het kabinet wil de inlichtingendiensten de bevoegdheid geven om meer soorten gegevens grootschalig te onderscheppen. Maar hoe zit het precies met dat controversiële voorstel?

De huidige Wet op de inlichtingen- en veiligheidsdiensten (Wiv) stamt uit 1987 en werd in 2002 voor het laatst vernieuwd. In de wet is geregeld wat de Nederlandse geheime diensten, de Algemene Inlichtingen - en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD), wel en niet mogen en wie daar toezicht op houdt.

De aanzet voor een nieuwe Wiv werd in 2013 gegeven. De door het kabinet aangestelde commissie-Dessens besloot toen dat de tijd rijp was voor de AIVD en de MIVD om nieuwe bevoegdheden te krijgen, om in te spelen op nieuwe dreigingen van terroristen en andere staatsvijanden.

Uiteindelijk werd de wet in april van dit jaar door ministers Hennis (Defensie) en Plasterk (Binnenlandse Zaken) gepresenteerd en eind oktober naar de Tweede Kamer gestuurd.

Wat is er nieuw?

De belangrijkste nieuwigheid is dat de AIVD en de MIVD voortaan niet alleen ongericht satellietverkeer mogen aftappen, maar ook verkeer dat via kabels verstuurd wordt. Daar valt bijna al het internetverkeer onder, zelfs verkeer van en naar mobiele apparaten. Die gelden als kabelgebonden omdat het verkeer vanaf de zendmast via glasvezelkabels loopt.

Het zou onder het nieuwe voorstel bijvoorbeeld mogelijk worden om alle communicatie tussen Nederland en een ander land af te tappen, of om lokaal al het verkeer via een bepaalde app op te vangen. Ook moet communicatie in bijvoorbeeld bepaalde games of de privéberichtenfuncties van diverse sociale media afgetapt kunnen worden.

Die verandering wil het kabinet doorvoeren op aandringen van de inlichtingendiensten, omdat tegenwoordig bijna al het internetverkeer via kabels verloopt. Door het aftappen van kabelgebonden verkeer, hopen zij meer grip te krijgen op de communicatie tussen onder meer terroristen.

Ook zijn er passages in de wet opgenomen die regelen hoe de informatieuitwisseling met buitenlandse inlichtingendiensten eruit moet gaan zien. Zo wordt het mogelijk dat bijvoorbeeld de AIVD een dataset deelt met een buitenlandse dienst zonder dat die dataset eerst door de AIVD zelf is geanalyseerd.

Commissie

Om te voorkomen dat de inlichtingendiensten op grote schaal onschuldige burgers gaan aftappen, moet een speciale commissie in het leven geroepen worden. Die Toetsingscommissie Inzet Bevoegdheden (TIB) bestaat uit minimaal drie personen, waaronder twee rechters en bijvoorbeeld een cybersecurityspecialist.

Voordat een inlichtingendienst een sleepnet uitzet, moet de TIB bepalen of dat door de beugel kan. Ook voor individuele telefoontaps en het hacken van computers moet de commissie toestemming geven. Beperkingen van het sleepnet moeten vooral van de TIB komen.

Ook wordt de rol van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), die nu al achteraf toezicht houdt op de inlichtingendiensten, versterkt. De organisatie zal onder meer bindende oordelen kunnen uitspreken over de handelswijze van de diensten. Nu heeft de CTIVD nog een adviserende rol.

Kritiek

Het voorstel is controversieel, omdat uit onthullingen van klokkenluider Edward Snowden is gebleken hoe inlichtingendiensten in het buitenland omspringen met de bevoegdheid om grootschalig communicatie op te vangen. Onder meer de Amerikaanse NSA bleek enorme hoeveelheden internetverkeer van onschuldige burgers te verwerken.

De Raad van State (RvS) is van mening dat de wet in deze vorm niet naar de Kamer had gemogen. In een advies aan het kabinet schrijft het hoogste rechtsorgaan van Nederland dat het toezichtsstelsel van de wet tekortschiet.

De RvS vindt dat de toetsingscommissie uit het voorstel geschrapt had moeten worden, en dat in plaats daarvan een sterkere CTIVD had moeten ontstaan.

Te lang

Ook vindt de Raad dat gegevens te lang bewaard worden. Het kabinet wil verzamelde gegevens drie jaar kunnen bewaren, maar dat is volgens de adviseurs niet proportioneel.

Wel vindt de Raad dat de noodzaak van nieuwe bevoegdheden voor de inlichtingendiensten is voorzien van afdoende argumentatie. Het ongericht aftappen van communicatie is in principe niet in strijd met de mensenrechten, schrijft de Raad, als de waarborgen en het toezicht maar goed zijn geregeld.

Ook privacyvoorvechters vinden de nieuwe Wiv te ver gaan. Privacyorganisatie Bits of Freedom vindt dat de privacy van onschuldige Nederlanders niet de dupe mag worden. Privacy First, een andere belangenorganisatie, noemt de wet een inbreuk op de privacy van elke Nederlander.

Hoe nu verder?

De wet ligt nu bij de Tweede Kamer voor verdere behandeling. Het is nog onduidelijk of er een Kamermeerderheid voor het voorstel te vinden is.

De VVD sprak zich eerder enthousiast uit over de wetsvernieuwing en mogelijk is ook bij de PVV steun te vinden. Andere partijen, waaronder de PvdA en D66, steunen in principe een herziening van de Wiv maar hebben wel zorgen over de bescherming van de privacy in het voorstel. D66-Kamerlid Kees Verhoeven wil daarom experts horen in de Tweede Kamer.

Vanwege de complexe materie en de controversiële inhoud van het voorstel lijkt het onwaarschijnlijk dat de behandeling nog voor de verkiezingen kan worden afgerond.

EU Hof: websites mogen jouw ip-adres verzamelen

Een ip-adres is een persoonsgegeven, net zoals je woonadres. Maar ondanks dat jij de baas bent over jouw ip-adres, mogen websites deze gegevens wel verzamelen om zich te wapenen tegen internetaanvallen.

Dat heeft het Europees Hof recentelijk bepaald.

De uitspraak is gedaan in een zaak tussen de Duitser P. Breyer en de Bondsrepubliek Duitsland. Breyer sleepte de Duitse overheid voor de rechter omdat websites van de overheid ip-adressen van bezoekers verzamelen. Hij vindt dit niet noodzakelijk, terwijl de Duitse overheid zegt dat het deze data verzamelt om internetaanvallen te weren.

DDoS afslaan

Het Europees Hof oordeelt nu dat het verzamelen van ip-adressen zonder expliciete toestemming van bezoekers is toegestaan, maar alleen als websites de informatie gebruiken om internetaanvallen af te slaan. Als een website last heeft van een DDoS-aanval, kan het bijvoorbeeld de ip-adressen van de aanvallers blokkeren.

Het verzamelen van ip-adressen is toegestaan, ondanks dat het ip-adres door het Europees Hof wordt gezien als een persoonsgegeven. Volgens het Hof kan een ip-adres de identiteit van een internetgebruiker onthullen, bijvoorbeeld via een kort geding bij de internetprovider. De internetprovider weet namelijk wie de facturen betaalt en wie verantwoordelijk is voor de internetverbinding.

Eerder zei de Duitse overheid dat burgers niet via hun ip-adres konden worden geïdentificeerd. Daar is het Europees Hof het dus niet mee eens.

Gerechtvaardigd belang

"De exploitant van een website kan een gerechtvaardigd belang erbij hebben bepaalde persoonsgegevens van de bezoekers te bewaren om zich te beschermen tegen cyberaanvallen", zo luidt het oordeel van het Hof.

De Duitse overheid heeft er volgens het Hof 'een gerechtvaardigd belang bij' dat hun websites bereikbaar zijn en goed werken, en daarom mogen zij ip-adressen van bezoekers opslaan.

Dynamisch ip-adres

Het Hof spreekt zich specifiek uit over dynamische ip-adressen. Dit zijn ip-adressen die kunnen veranderen. Volgens het Hof zijn deze ip-adressen, ondanks dat ze per burger kunnen veranderen, ook persoonsgegevens.

Het gros van de Nederlanders heeft een dynamisch ip-adres, maar dat verandert pas als zij een geruime tijd offline zijn. In de meeste gevallen blijft een ip-adres hetzelfde als de persoon actief zijn internetverbinding gebruikt.

Alle politiegebouwen krijgen wifi-netwerk in 2017

Om de politie toekomstbestendig te maken zullen alle politiegebouwen volgend jaar een wifi-netwerk krijgen, zo heeft korpschef Erik Akerboom tijdens het Innovatiecongres Tomorrow is Today laten weten. Het gaat om een intern, beveiligd en gemonitord netwerk voor agenten en een open netwerk voor gasten.

Verder zal de politie volgend jaar zowel smartphones als tablets versneld beschikbaar stellen. Volgens Akerboom zijn deze stappen nodig voor een toekomstbestendige politie. Daarnaast gaan meerdere politieteams uitvoerig experimenteren met bodycams. Dit moet antwoord verschaffen op diverse vragen, zoals hoe burgers en agenten hierop reageren, hoe bodycams bijdragen aan waarheidsvinding en wat politiemensen er zelf van kunnen leren. Ook het voldoen aan de eisen van bijvoorbeeld de Wet politiegegevens vormt hierbij een aspect.

Internet of Things

Ook het Internet of Things heeft de aandacht van de politie. Naar verwachting groeit het aantal sensoren - van auto en computer tot thermostaat en sportkleding - de komende vijf jaar wereldwijd van vijf naar vijftig miljard. De politie stelt dat deze apparaten wezenlijke informatie bevatten voor de taken die het uitvoert. Om te kijken hoe hiermee moet worden omgegaan heeft de politie een "virtuele broedplaats" voor data en technologie ingericht. Het gaat om een initiatief dat bestaande, interne expertise bundelt en moet bijdragen aan de besluitvorming over het onderwerp.

Politie verstuurt 126.000 e-mails naar slachtoffers misdrijven

De politie heeft in juli en augustus 126.000 e-mails verstuurd naar slachtoffers van internetoplichting, diefstal of vernieling die aangifte deden. In het bericht wordt een update over de stand van zaken gegeven. Bij een inbraak of geweldsmisdrijf neemt de politie al een paar jaar persoonlijk contact op.

Voor heel ernstige geweldsmisdrijven zet de politie familierechercheurs in, die de nabestaanden ondersteunen tijdens het politieonderzoek. Via Mijn Politie kunnen nu ook aangevers van diefstallen, vernielingen en internetoplichting op de hoogte worden gehouden. Het gaat om ongeveer 700.000 aangiftes per jaar. Dit is zo'n 85% van alle aangiftes. In deze gevallen gaat het niet om persoonlijk contact, maar om een e-mail dat er iets veranderd is in de status van de aangifte. Slachtoffers kunnen dan op Mijn Politie kijken wat dit precies is.

Mijn Politie bestaat al sinds eind april 2016. Eerst konden hier alleen slachtoffers van internetoplichting terecht. Sinds 1 juli 2016 is de persoonlijk pagina ook toegankelijk voor slachtoffers van diefstal en vernieling. In de maanden juli en augustus is er ruim 91.000 keer aangifte gedaan van diefstal of vernieling. Over deze aangiftes zijn zo'n 126.000 e-mails verstuurd naar de slachtoffers.

Inloggen op Mijn Politie gebeurt via DigiD, net als het doen van online aangifte. "Zo weet de politie zeker dat vertrouwelijke informatie alleen gelezen wordt door het slachtoffer. En weet het slachtoffer zeker dat het de politie is die de aanvullende vragen stelt", aldus de politie.

Killer clown rage zegt ons dat er veel mis is met internetcultuur

Mooie analyse in The Independent, over het fenomeen killer clown. Of beter: het fenomeen pranking. Waarbij geldt: je kunt het zo gek niet bedenken, illegaal of immoreel, maar je denkt er mee weg te komen als je zegt dat het voor de grap is. 'Just a prank'. En dat in tijden waarin iedereen z'n 'fifteen seconds of fame' kan claimen op sociale media.

Tja. Dan moet je niet verbaasd zijn als iedereen er aan mee doet. Filmpjes worden dan binnen een uur honderdduizenden keren bekeken, copycats zijn overal en iedereen probeert elkaar te overtreffen. Zie de ontgroeningen, zie de clowns, zie alle voorgaande 'challenges'.

De krant schrijft over een 'cluttered and democratised world of cyberspace' waar aandachttrekkerij de hoofdrol speelt. En zo zijn de bananenschil en het scheetkussen van vroeger vervangen door poepgooien en mensen-laten-schrikken. 'Hoe gewelddadiger de prank, hoe meer views en shares' – de raison d'etre van elke vlogger.

Daardoor is er nauwelijks nog reflectie op eigen handelen, het is toch een grap, en al helemaal geen aandacht meer voor mogelijke slachtoffers. 'The contemporary prankster – both violent and offensive – fails to grasp this most basic idea of individual liberty and, indeed, human decency'. En dat mensen er dus (psychologisch) gewond raken – ach, het levert wel tig nieuwe volgers op.

Oplichters ook actief op WhatsApp

Technologiesites melden dat Whatsapp steeds meer gebruikt wordt door criminelen om persoonlijke gegevens van gebruikers te stelen. De oplichters doen zich voor als een bestaand contact, sturen een link naar bijvoorbeeld een website met kortingen. Vervolgens wordt malware geïnstalleerd en kunnen de oplichters hun slag slaan.

In Nederland verloor een vrouw 1700 euro toen haar 'dochter' appte dat haar zakgeld op was. De vrouw maakte geld over en besefte pas later dat ze was opgelicht. Dochterlief had helemaal geen geldproblemen; de oplichters hadden met een foto van de dochter een nep-account gemaakt. In België benadrukken beveiligingsexperts dat het nog niet zo'n vaart loopt, schrijft Het Nieuwsblad.

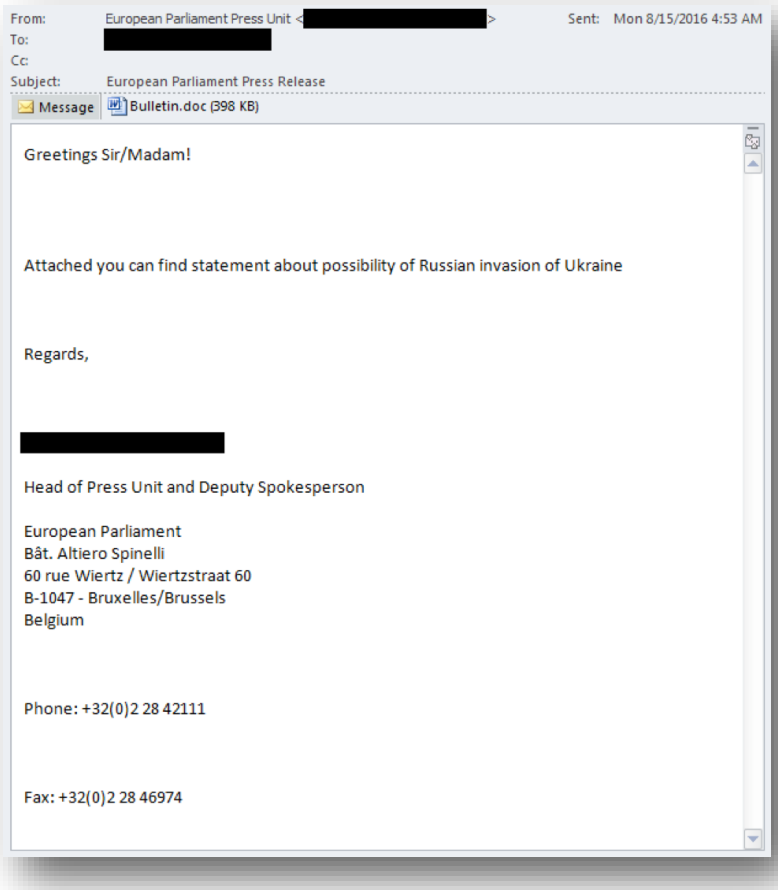
Wel moeten mensen beseffen dat ze niet alleen hun computer moeten beschermen maar ook hun smartphone. En ja, ook criminelen zitten op Whatsapp. 'Niet alleen om zelf met elkaar te communiceren maar ook omdat veel mensen hun smartphone niet beveiligen'.

Cyberspionnen vallen Flash-lekken aan via Word-document

Een groep cyberspionnen die de afgelopen jaren een groot aantal organisaties aanviel maakt tegenwoordig ook gebruik van Word-documenten om gebruikers via beveiligingslekken in Flash Player te infecteren. De aanval begint met een Word-document dat als e-mailbijlage wordt verstuurd.

Het Word-document bevat een kwaadaardig Flash-bestand dat de aanvallers op twee manieren kunnen gebruiken. In het eerste scenario controleert dit Flash-bestand de aanwezige versie van Adobe Flash Player en probeert vervolgens één van drie kwetsbaarheden in Flash Player aan te vallen. Het gaat om een lek uit 2015 en twee lekken van dit jaar. In het tweede scenario wordt er informatie over het systeem naar een remote server gestuurd. Wat er vervolgens gebeurt kon niet worden vastgesteld, maar onderzoekers denken dat de server een exploit voor Flash Player terugstuurt.

Om slachtoffers niets te laten vermoeden krijgen die een "lokdocument" te zien. Uit details van de malware lijkt het erop dat zowel Windows- als Mac OS X-computers het doelwit van de aanvallen zijn. Dezelfde spionagegroep kwam onlangs ook in het nieuws vanwege de ontdekking van Mac-malware. Voor zover bekend zijn een Oekraïens defensiebedrijf en een ministerie van Buitenlandse Zaken in dezelfde regio via de documenten aangevallen, zo meldt beveiligingsbedrijf Palo Alto Networks.


From: European Parliament Press Unit <[redacted]> Sent: Mon 8/15/2016 4:53 AM
To: [redacted]
Cc:
Subject: European Parliament Press Release
Message Bulletin.doc (398 KB)

Greetings Sir/Madam!

Attached you can find statement about possibility of Russian invasion of Ukraine

Regards,

[redacted]

Head of Press Unit and Deputy Spokesperson

European Parliament
Bât. Altiero Spinelli
60 rue Wiertz / Wiertzstraat 60
B-1047 - Bruxelles/Brussels
Belgium

Phone: +32(0)2 28 42111

Fax: +32(0)2 28 46974

Het gebruik van Flash-bestanden in Word-documenten om malware te verspreiden komt al jaren voor. Al in 2009 werd deze tactiek toegepast. Drie jaar later in 2012 waarschuwde Microsoft Office-gebruikers nog om maatregelen tegen Flash -aanvallen in documenten te nemen. Ook dit en vorig jaar werden Flash-lekken via Word-documenten aangevallen.

De groep cyberspionnen achter de nu ontdekte Word-documenten wordt Pawn Storm genoemd, maar staat ook bekend als 'Fancy Bear', 'Sofacy', 'Sednit', 'APT28', Threat Group-4127 en 'Strontium'. Eerder werden de onderzoekraad van MH17, verschillende ministeries van Buitenlandse Zaken, een Amerikaanse defensieorganisatie, de Turkse overheid, een NAVO-lid, Linuxgebruikers, het CDU, Sanoma, de presidentscampagne van Hillary Clinton, het Wereld Anti-Doping Agentschap (WADA) en MH17-onderzoekers van het onderzoekcollectief Bellingcat door de groep aangevallen.

Politie VS wil vingerafdruk voor ontgrendelen telefoons vorderen

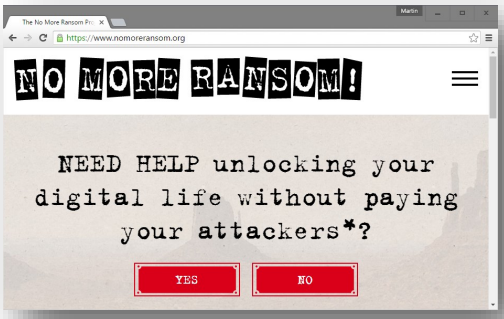
De Amerikaanse politie heeft de rechter om toestemming gevraagd om tijdens een huiszoeking in een wooncomplex van alle aanwezige personen de vingerafdrukken te mogen vorderen, om zo vergrendelde smartphones te kunnen ontgrendelen.

Niet alleen had de politie toestemming voor de huiszoeking gevraagd, ook wilde justitie personen op het terrein dwingen om hun toestel via hun vingerafdruk te ontgrendelen. Volgens het verzoek kon de politie niet van tevoren de identiteit van elk apparaat of vingerafdruk vaststellen die agenten tijdens de doorzoeking zouden tegenkomen, maar had het aangetoond dat er een sterke verdenking was dat er bewijs op de zoeklocatie zou worden aangetroffen, en het de mogelijkheid moest hebben om deze apparaten te kunnen doorzoeken. Het verzoek spreekt dan ook over het in beslag nemen van wachtwoorden, encryptiesleutels en andere toegangsapparaten die nodig zijn om de telefoons te ontgrendelen.

Juridische experts maken zich zorgen over het verzoek van de overheid. "Ze willen de mogelijkheid om een bevel te krijgen op basis van de aanname dat ze meer zullen ontdekken nadat ze het bevel hebben gekregen", zegt juridisch expert Marina Medvin. Ze stelt dat het bevel gebruikt kan worden om mensen mee te laten werken waarvan de politie pas mogelijk later zal bepalen dat ze verdachte zijn. Medvin spreekt dan ook van machtsmisbruik als het verzoek zou worden goedgekeurd.

Politieportaal helpt 2500 ransomware-slachtoffers

Een portaal die eind juli door de politie, Europol en beveiligingsbedrijven Intel Security en Kaspersky Lab werd gelanceerd heeft inmiddels meer dan 2500 ransomware-slachtoffers geholpen met het kosteloos terugkrijgen van hun versleutelde bestanden.

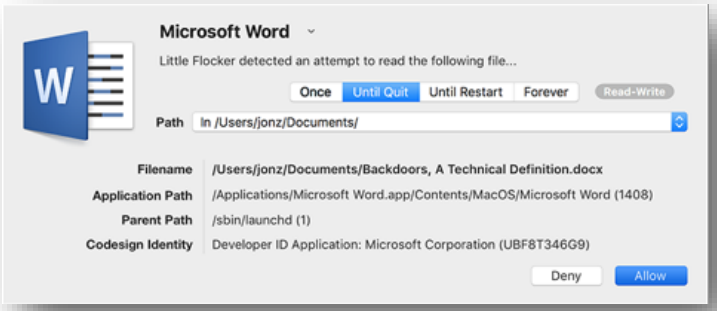


Via de portal NoMoreRansom biedt de politie verschillende decryptietools aan. Drie maanden na de lancering hebben zich nu 13 nieuwe landen bij het initiatief aangesloten. Het gaat om Bosnië en Herzegovina, Bulgarije, Columbia, Frankrijk, Hongarije, Ierland, Italië, Letland, Litouwen, Portugal, Spanje, Zwitserland en Groot-Brittannië. Daarnaast verwacht Europol dat meer opsporingsdiensten en particuliere bedrijven zich de komende maanden zullen aansluiten.

"Hun samenwerking zal ervoor zorgen dat er meer gratis decryptietools beschikbaar zullen komen, zodat nog meer slachtoffers worden geholpen met het ontsleutelen van hun bestanden en informatie, en waarbij criminelen worden gepakt waar ze het meest voelen, in hun portemonnee", zo stellen de opsporingsdienst en politie. Om meer ransomware-slachtoffers te bereiken zal de portal in verschillende talen worden vertaald.

Mac-tool beschermt bestanden tegen spyware en ransomware

Beveiligingsonderzoeker Jonathan Zdziarski heeft een tool voor Mac OS X ontwikkeld die bestanden tegen spyware, ransomware en andere kwaadwillende applicaties moet beschermen. De tool heet Little Flocker en voorkomt dat applicaties zonder toestemming van gebruikers toegang tot bestanden krijgen.



Volgens Zdziarski is het programma een soort firewall voor het bestandssysteem. Het geeft gebruikers controle over hun bestanden en voorkomt ongeautoriseerde toegang door kwaadaardige of nieuwsgierige applicaties. Om dit te realiseren nestelt Little Flocker zich binnen het besturingssysteem. Het heeft daardoor hogere rechten dan root, waardoor het effectief tegen rootkits en andere malware kan optreden, aldus de onderzoeker.

Naast het blokkeren van toegang tot bestanden kan Little Flocker ook toegang tot de webcam regelen, voorkomen dat de Spotlight - en Suggesties-functie metadata verzamelen, iOS-pairinggegevens worden gestolen en dat applicaties zonder toestemming zich als opstartproces kunnen installeren. Er is zowel een interface voor beginners als meer geavanceerde gebruikers. Daarnaast kunnen gebruikers zelf regels voor het programma opstellen.

WordPress-sites gehackt via zero day-lek in Marketplace-plug-in

Een beveiligingslek in een plug-in voor WordPress waarvoor nog geen beveiligingsupdate beschikbaar is wordt actief gebruikt om websites te hacken en van een backdoor te voorzien. Daarvoor waarschuwt beveiligingsbedrijf Sucuri. De kwetsbaarheid bevindt zich in de Marketplace-plug-in.

Deze plug-in fungeert naar eigen zeggen als "volwaardige ecommerce-oplossing" voor WordPress-sites en maakt het mogelijk om een website zonder al teveel kennis in een webwinkel te veranderen. Het beveiligingslek in de plug-in maakt het mogelijk voor een aanvaller om willekeurige bestanden te uploaden. In de nu waargenomen aanvallen gaat het om een backdoor die aanvallers volledige controle over het systeem geeft.

Aangezien er geen beveiligingsupdate beschikbaar is hebben de ontwikkelaars van WordPress de plug-in van de WordPress.org Plugin Directory verwijderd. Volgens cijfers zou de plug-in op minder dan 500 WordPress-sites zijn geïnstalleerd. Het geeft echter ook aan dat zelfs obscure plug-ins de aandacht van aanvallers hebben.

Amnesty adviseert Signal en WhatsApp voor chatgesprekken

Wie een chat-app zoekt die gesprekken tegen luistervinken beschermt kan volgens Amnesty International het beste voor Signal kiezen, maar WhatsApp is ook een prima alternatief. De mensenrechtenorganisatievergeleek 11 aanbieders van populaire chat-apps en bekeek hoe ze encryptie toepassen.

Verschillende van de bekende chat-apps maken gebruik van end-to-end-encryptie, zodat alleen de ontvanger en afzender de inhoud van een bericht kunnen lezen. WhatsApp is van de populaire chat-apps de enige app die gebruikers uitdrukkelijk waarschuwt als een chatgesprek niet end-to-end versleuteld is. Van de verschillende aanbieders van chat-apps komt Facebook dan ook al beste uit de bus, met een score van 73 van de 100 haalbare punten.

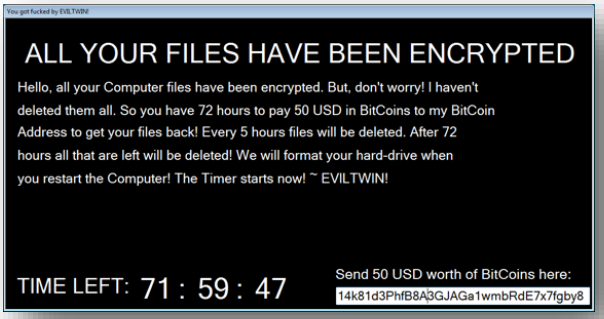
Apple en Telegram volgen met beide 67 punten, terwijl Google met 53 punten een onvoldoende scoort. Dat geldt ook voor Microsoft (40), Snapchat (26) en Blackberry (20). Tencent, de Chinese aanbieder van WeChat en QQ, scoort geen enkel punt omdat het op geen enkele manier de privacy van gebruikers beschermt. Daarnaast heeft het zich niet uitgesproken tegen het toevoegen van backdoors voor de overheid.

Een belangrijke app die in het overzicht van de 11 aanbieders mist is Signal. Amnesty heeft echter ook een advies met zes privacy-tips online gezet, en daarin wordt Signal wel genoemd. Signal is een chat-app die door allerlei experts wordt aangeraden. De code is open source en de ontwikkeling wordt door een non-profitorganisatie gedaan. Het Signal Protocol dat voor de end-to-end-encryptie zorgt wordt ook door WhatsApp, Facebook Messenger en Google Duo gebruikt. "Natuurlijk maken mensen gebruik van het platform waar hun vrienden en familie op zitten. Voor de meeste mensen is Whatsapp een alternatief dat goed genoeg is aangezien het standaard over sterke end-to-end-encryptie beschikt."

Bron: Amnesty International

Ransomware maakt pc onbruikbaar door encryptieproces

Onderzoekers hebben een nieuwe ransomware-variant ontdekt die continu blijft zoeken naar bestanden om te versleutelen, waardoor de computer zo goed als onbruikbaar wordt. De meeste ransomware versleutelt aanwezige bestanden op een computer en zal zich daarna verwijderen.



Alleen de op dat moment versleutelde bestanden blijven achter. De nu ontdekte Exotic -ransomware blijft echter continu naar nieuwe bestanden zoeken om te versleutelen. Het doet dit door allerlei mappen langs te gaan en vervolgens nog niet versleutelde bestanden te versleutelen. Dit vereist echter de nodige rekenkracht van de computer, die daardoor zo goed als onbruikbaar wordt, zo meldt de website Bleeping Computer. Wat verder opvalt aan de ransomware is dat die alleen bestanden in bepaalde mappen versleutelt, in plaats van bestanden op het gehele systeem.

Daarnaast wordt er 50 dollar voor het ontsleutelen van de bestanden gevraagd, terwijl veel andere ransomware-exemplaren vaak honderden dollars eisen. Om slachtoffers tot betalen te dwingen laat de Exotic-ransomware een scherm met een aftelklok zien en wordt er gedreigd dat er elke 5 uur bestanden worden verwijderd. Na 72 zegt de ransomware alle bestanden te verwijderen. Volgens onderzoekers gaat het hier om een testversie die voor zover bekend nog niet in het wild is aangetroffen.

Waarom is Veracrypt een goed TrueCrypt-alternatief?

Twee jaar terug werd op mysterieuze wijze de stekker uit de ontwikkeling van TrueCrypt getrokken, wat veel ophef veroorzaakte en NSA-samenzweringstheorieën opleverde. Desondanks bleef het stil en zaten we lang zonder échte vervanger. VeraCrypt dient zich echter aan. Waarom is het een veilige keuze.

Natuurlijk is Veracrypt geen nieuwe encryptietool. Het bestaat al een tijdje. Onlangs hebben beveiligingsexperts de broncode van Veracrypt volledig doorgenomen. Hieruit bleek dat er acht kwetsbaarheden waren, die meteen gedicht worden.

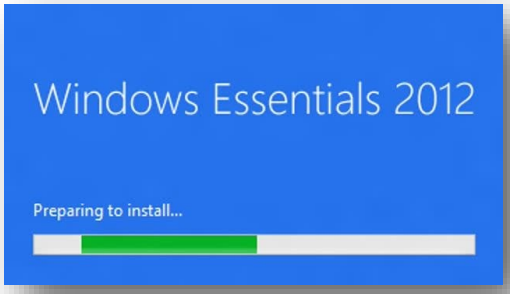
Veracrypt is een voortzetting op de laatste veilige versie van TrueCrypt (7.1a). Sindsdien is het versleutelprogramma doorontwikkeld onder de vlag van Veracrypt. Overigens is Veracrypt niet de enige. Zo is er bijvoorbeeld ook TrueCrypt.ch, wat bewust aan een veilig (neutraal) Zwitsers domein is gekoppeld. De Zwitserse variant lijkt echter wat stil te staan in z'n ontwikkeling.

Het blijft een discussiepunt. Is open source encryptiesoftware veiliger dan encryptiesoftware met een gesloten broncode? Bij open source software valt dat door experts te verifiëren, wat in de audit gedaan is. Bij gesloten programma's als Bitlocker moet je ontwikkelaar Microsoft erop vertrouwen dat de versleuteling waterdicht in elkaar zit en anderen (zoals veiligheidsdiensten) geen toegang verleend kan worden tot jouw persoonlijke gegevens.

Veracrypt maakt gebruik van een warrant canary. Dit houdt in dat ze melding geven wanneer ze door een overheid gedwongen worden mee te werken aan het afstaan van gegevens. De warrant canary is nog in tact, wat inhoudt dat ze (naar eigen zeggen) nog nooit gegevens af hebben moeten staan.

Einde ondersteuning Windows Essentials begin 2017

De ondersteuning op het Windows Essentials-programma van Microsoft wordt definitief stopgezet. Vanaf 10 januari 2017 is het niet meer mogelijk om de software te downloaden of te installeren. Windows Essentials - ook wel bekend als Windows Live Esssentials - bevatte diverse losse programma's voor bepaalde taken. Zo was er een aparte mailclient, Windows Live Mail, een eenvoudig videobewerkingsprogramma in de vorm van Movie Maker en een fotogalerie: Photo Gallery. Ook OneDrive was een van de onderdelen die met Windows Essentials werd meegeleverd.



Sinds de komst van Windows 10 zijn deze tools eigenlijk overbodig, omdat het besturingssysteem zelf al een deel van deze programma's bevat. Windows Movie Maker is daarop echter een uitzondering, want dit op zich prima programma heeft in Windows 10 geen vervanger gekregen. Windows Essentials werd officieel ook al niet meer ondersteund in Windows 10. In Windows 10 kun je nu je mail binnenhalen met de Windows Mail-app, foto's bekijken en bewerken kan met de Foto's-app.

Microsofts cloudtool OneDrive is sinds Windows 8.1 al een vast onderdeel van het besturingssysteem. In Windows 10 wordt deze tool regelmatig verbeterd en verder in het besturingssysteem geïntegreerd. Wie de software alsnog wil downloaden, kan dat nog steeds doen via de site van Microsoft.

Gratis scanner helpt gebruikers Internet of Things-apparaten

De gevolgen van onbeveiligde Internet of Things-apparaten op het internet zijn de afgelopen weken door verschillende grote ddos-aanvallen meer dan duidelijk geworden. Digitale videorecorders, ip-camera's en routers met standaard wachtwoorden blijken een eenvoudig doelwit voor aanvallers.

Beveiligingsbedrijf Bullguard lanceerde eerder dit jaar een gratis scanner die eigenaren van dergelijke producten moet helpen. Via de "IoT Scanner" kunnen internetgebruikers controleren of hun Internet of Things-apparaten eenvoudig via het internet gevonden kunnen worden en of het apparaat kwetsbaarheden bevat. De IoT Scanner maakt gebruik van informatie van de zoekmachine Shodan.io. Deze zoekmachine brengt allerlei op internet aangesloten apparaten in kaart.

Windows-oplichters hebben meer geluk bij jonge slachtoffers

De scam die via telefoon of pop-up probeert te waarschuwen voor een probleem met je computer is voor de meeste mensen niet meer dan een irritante onderbreking. Voor sommigen betekent het echter een dure affaire.

Volgens een ondervraging van Ipsos Public Affairs, gesponsord door Microsoft, zou twee derde van de duizend respondenten wereldwijd al te maken hebben gekregen met zulke scams. Ongeveer één op vijf legde niet meteen in, en bijna één op tien heeft geld gegeven aan de oplichters.

De scam komt meestal in de vorm van een telefoontje. Aan de lijn beweert iemand van Microsoft of een andere techgigant, dat er met je computer iets ernstigs aan de hand is, zoals een besmetting met malware. De beller probeert je dan een dure oplossing aan te smeren of vraagt om je computer op afstand te controleren, terwijl het doel in feite is om je zoveel mogelijk geld af te troggelen, en al dan niet je computer te infecteren.

Dat blijkt te lukken. Uit de resultaten van het onderzoek wordt bovendien duidelijk dat jonge mensen niet per se kritischer staan tegenover de valstrik dan hun oudere medemens. Ondervraagden tussen 25 en 34 zijn drie keer meer in de val getuind dan de respondenten tussen 55 en 64. Jongeren tussen 18 en 24 deden het niet veel beter. Ongeveer de helft van die groep luisterde naar wat de oplichter te zeggen had, in plaats van meteen het gesprek af te breken.

Hoewel de impact bij ondervraagden onder 34 schijnbaar groter is, duidt dat niet meteen op naïviteit. In tegenstelling tot ouderen, die de scam vooral via de telefoon kennen, worden jongeren ook meer online met het concept geconfronteerd, bijvoorbeeld door een pop-up, e-mail of een redirect naar een andere website.

Nieuwe infectiemethode ransomware maakt slachtoffers

Een nieuwe methode om ransomware af te leveren maakt de voorbije maanden erg veel slachtoffers. De schurken achter de software die je computer versleutelt en onbruikbaar maakt, gebruiken als vanouds e-mails, maar gebruiken een type bestand dat tot nu toe amper gebruikt werd voor kwalijke doeleinden. Het gaat om .WSF-bestanden (Windows Script Files) die in een zip-bestand toekomen.

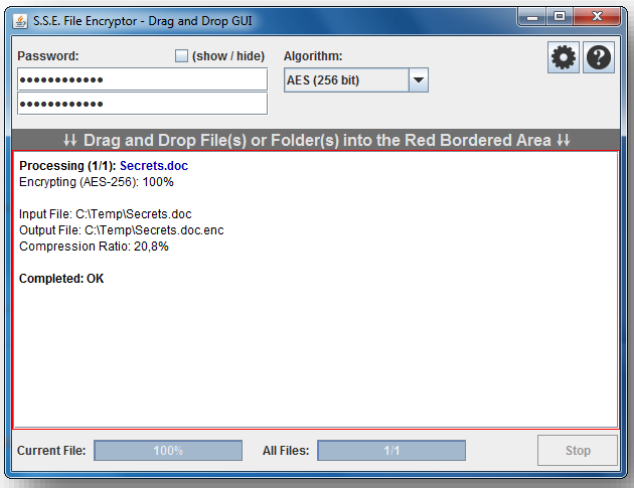
Het bestand proberen openen is genoeg om je hele computer te versleutelen. WSF-bestanden combineren verschillende types codering en worden slechts zelden tegengehouden door e-mailproviders en nog minder opgemerkt door anti-virusprogramma's. Dat maakt de bestandsextensie een erg populaire keuze voor criminelen.

Terwijl het WSF-trucje begin juni slechts 22.000 keer werd ontdekt en tegengehouden, steeg dat cijfer begin juli naar 2 miljoen keer. Dat betekent dat het aantal keer dat het bestand niet ontdekt werd, nog vele malen hoger moet liggen. In september lag het cijfer op 2,2 miljoen tegengehouden bestanden.

De huidige campagne, waar ook de beruchte variant Locky deel van uitmaakt, gebeurt onder het mom van een foutgelopen boeking van vliegtickets. Slachtoffers krijgen een bericht dat zegt dat er iets misliep en dat de ontvanger meer details vindt in het bijgevoegde zip-bestand. Van zodra je dat opent, is het kwaad geschied. De enige voorzorgsmaatregel die je dus kan nemen, is goed nadenken.

Snel afzonderlijke bestanden versleutelen

Sommige, privacygevoelige bestanden geef je liever wat extra bescherming mee om te vermijden dat derden die onverhoeds kunnen openen of inkijken. Dat roept dus om versleuteling. S.S.E File Encryptor is een tool die zich precies toelegt op het – stevig – versleutelen van afzonderlijke bestanden.



S.S.E File Encryptor vereist wel de installatie van Java RE, en is beschikbaar voor diverse platformen (JAR, voor Windows, Linux en macOS) – er bestaat trouwens ook een variant die zich ook vanuit de opdrachtregel laat aansturen. De werking (van de GUI-versie) is zeer eenvoudig. Je start het programma op en je vult het wachtwoord in waarmee je bestanden wilt versleutelen. Je kiest tevens het gewenste encryptie-algoritme. Standaard staat dit ingesteld op het stevige AES (256 bit), maar je kunt ook een ander algoritme aanduiden, waaronder Serpent (256 bit), Twofish (256 bit) of Blowfish (448 bit).

Vervolgens hoef je de bestanden die je wenst te versleutelen maar naar het programmavenster te verslepen. Zodra je een bestand in dit venster hebt geplaatst wordt er een geëncrypteerde versie (met extensie .enc) van het bestand in dezelfde map als het onversleutelde origineel geplaatst. Desgewenst moet je dit laatste dus zelf nog wel even verwijderen.Via de instellingenrubriek is het echter mogelijk een andere vaste locatie in te vullen zowel voor de versleutelde als voor de originele bestanden.

Een versleuteld bestand decrypteren doe je eigenlijk op precies dezelfde manier: naar het hoofdvenster verslepen, waarna het bestand onmiddellijk wordt ontsleuteld – desgevallend wordt je uiteraard wel eerst even om het bijhorende wachtwoord gevraagd.

Bedrijven halen elke vier seconden nieuwe malware binnen

Uit een onderzoek van Check Point Software Technologies blijkt dat iedere dag bijna een miljoen nieuwe malware op de wereld wordt losgelaten. Dit heeft een rechtstreeks verband met het aantal succesvolle malwareaanvallen op bedrijven. In 2014 werd er door 63 procent van de onderzochte bedrijven kwaadaardige bestanden gedownload. Vorig jaar was dit bij maar liefst 89 procent van de organisaties het geval.

Ook de frequentie waarmee malware wordt gedownload steeg exponentieel. In 2014 werd er elke zes minuten malware binnengehaald door bedrijven. Vorig jaar wisten virussen maar liefst elke 81 seconden op bedrijfsnetwerken binnen te glippen. Voor onbekende malware liggen deze cijfers zelfs nog hoger: elke vier seconden wordt er een onbekend virus gedownload.

Dankzij deze hoge downloadcijfers liggen de percentages van bedrijven die slachtoffer zijn gevallen aan malware eveneens hoog. 75 procent van de onderzochte organisaties had een bestaande botinfectie, terwijl er door 82 procent van de bedrijven een kwaadaardige website werd bezocht. Bovendien had 88 procent van de organisaties te maken met dataverlies en wordt bij maar liefst 94 procent van de bedrijven minstens één applicatie gebruikt met een hoog risico.

Britse geheime dienst wil internetprotocollen aanpassen

De Britse geheime dienst wil internetprotocollen aanpassen om spoofing- en ddos-aanvallen te voorkomen, maar critici zijn sceptisch en stellen dat de voorstellen gevolgen voor de privacy kunnen hebben. Om de protocollen aan te passen wil het GCHQ met internetproviders gaan samenwerken.

"We denken dat we ervoor kunnen zorgen dat een Britse machine niet aan ddos-aanvallen kan meedoen", zegt Ian Levy, technisch directeur van het GCHQ Nationaal Cyber Security Centre tegenover de Sunday Telegraph. "We denken dat we de onderliggende infrastructuur middels implemenatie-aanpassingen door internetproviders en communicatieserviceproviders kunnen repareren."

Zo wil het GCHQ aanpassingen aan het Border Gateway Protocol (BGP) en Signalling System 7 (SS7) doorvoeren die voor het routeren van verkeer worden gebruikt. De Britse geheime dienst zou zo willen voorkomen dat Brits verkeer voor ddos-aanvallen wordt ingezet en ook het tegengaan van sms-spoofing wordt al reden gegeven. De Internet Service Providers Association (ISPA), vertegenwoordiger van internetproviders, is sceptisch en stelt dat de problemen niet eenvoudig te verhelpen zijn, aangezien het om een oud en complex systeem gaat.

Cerber-ransomware versleutelt nu ook databases bedrijven

Een populaire ransomware-variant die eerst vooral tegen particulieren werd ingezet richt zich nu ook op bedrijven. Het gaat om de Cerber-ransomware waarvan de nieuwste versie databases kan versleutelen, zo meldt beveiligingsbedrijf McAfee. "Aanvallers beseffen dat consumenten misschien 300 tot 500 dollar voor hun bestanden betalen, maar bedrijven veel meer over hebben", zegt onderzoeker Matthew Rosenquist.

De nu ontdekte Cerber-variant kent drie belangrijke veranderingen, aldus McAfee. Zo verandert de ransomware de extensie van versleutelde bestanden naar vier willekeurige cijfers. Voorheen werden versleutelde bestanden van de extensie .cerber3 voorzien. De aanpassing zorgt ervoor dat het scannen naar versleutelde bestanden veel lastiger is geworden. Daarnaast zijn de betaalinstructies verbeterd en zien er volgens Rosenquist veel professioneler uit. "Dit kan slachtoffers meer vertrouwen geven dat ze met professionals te maken hebben en ze de sleutel voor het ontsleutelen van hun bestanden krijgen als ze betalen."

De belangrijkste aanpassing is echter dat de ransomware nu databaseprocessen probeert te stoppen zodat het de databases kan versleutelen. Rosenquist stelt dat dit een grote verandering is, aangezien databases voor veel organisaties belangrijke gegevens bevatten. Als de databasebestanden zijn geopend en in gebruik zijn zijn ze lastig te versleutelen. Cerber probeert daarom de databasesoftware te sluiten zodat het toch kan toeslaan. De Cerber-ransomware verspreidt zich onder andere via e-mailbijlagen, bijvoorbeeld als Word-document met kwaadaardige macro's.

Overheid doet opnieuw meer dataverzoeken bij Google

De Nederlandse overheid heeft in de eerste helft van 2016 bij Google 268 dataverzoeken ingediend, maar liefst 65% meer dan in dezelfde periode van 2015. Uit het Googles nieuwstetransparantierapport blijkt ook dat steeds minder verzoeken gehonoreerd worden: van 82% in 2014 via 74% in 2015 tot 67% in de eerste zes maanden 2016. Wereldwijd kreeg Google bijna 45 duizend dataverzoeken, waarvan 64% werd ingewilligd. De VS zijn nog steeds koploper met het indienen van dataverzoeken (bijna 15 duizend), gevolgd door Duitsland (8800 verzoeken) en Frankrijk (4300). Verzoeken kwamen er deze periode voor het eerst van Algerije, Wit-Rusland, Kaaimaneilanden, El Salvador, Fiji en Saudi-Arabië.

Fysieke landgrenzen gelden ook voor data

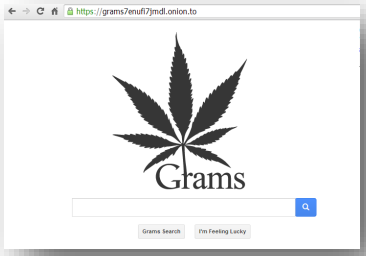
Wanneer je gegevens zijn gestald bij en Amerikaans tech-bedrijf, kan je er zeker van zijn dat je gegevens dankzij Amerikaanse wetgeving niet veilig zijn. Hierover ligt Micorsoft al jaren in de clinch met de Amerikaanse overheid. Laatstgenoemde eiste toegang tot e -mails van een klant op, terwijl deze mailtjes op een Ierse server staan.

Het leidde tot meerdere rechtszaken, waarbij Microsoft keer op keer bot ving. Tot een laatste hoger beroep, waarbij de rechter bepaalde dat gebruikersdata op een server buiten de VS niet opgeëist kunnen worden. Een belangrijke overwinning voor Microsoft, die daarmee vooral vertrouwen van klanten wint.

Maar ook voor de Europese burgers die door de zwakke verdragen tussen Europa en de VS en de dominantie van Amerikaanse techbedrijven, iets sterker staan als het aankomt op beveiliging van hun persoonlijke gegevens.

OM lanceert Tor-site met aliassen online drugshandelaren

Het Openbaar Ministerie en de politie hebben vandaag een website op het Tor-netwerk gelanceerd met de aliassen van personen die op illegale marktplaatsen actief zijn of inmiddels al zijn aangehouden. Het gaat zowel om de verkopers als kopers van drugs en andere verboden goederen.



Het is één van de Nederlandse acties onder de vlag van Operatie Hyperion, een wereldwijde actieweek op het Tor-netwerk die vorige week plaatsvond. De acties waren gericht tegen gebruikers van illegale marktplaatsen waar in verboden goederen, zoals drugs, wapens en hackingtools, wordt gehandeld. Via de Engelstalige Tor-site van het OM en de politie wordt duidelijk gemaakt dat er actief naar handelaren wordt gezocht.

"Verkopers en kopers van illegale goederen op het darknet zijn dus niet zo anoniem als zij zichzelf wanen", aldus het OM. Sommige van de verdachten maken gebruik van aliassen die overeenkomen met namen van bedrijven. "Die bedrijven zelf hebben echter niets met de verdenking te maken", zo stelt het Openbaar Ministerie.

Overheid gaat zich inzetten voor aanpak IoT-botnets

De overheid gaat zich inzetten om de problematiek van Internet of Things-botnets en onveilige IoT-apparaten zowel nationaal als internationaal aan te pakken. Dat heeft het Nationaal Cyber Security Center (NCSC) van het ministerie van Veiligheid en Justitie bekendgemaakt.

Aanleiding voor de aanpak zijn de recente ddos-aanvallen op dns-provider Dyn waardoor populaire websites slecht of onbereikbaar waren. De ddos-aanvallen werden via besmette IoT-apparaten uitgevoerd. Volgens het NCSC is de beveiliging van veel IoT-apparaten ondermaats doordat ze toegankelijk zijn via standaard wachtwoorden, die soms niet gewijzigd kunnen worden, en vaak niet of zeer lastig zijn te updaten met beveiligingsupdates.

De overheidsinstantie stelt dat onveilige IoT-apparaten aantrekkelijk voor cybercriminelen zijn, omdat dergelijke apparaten relatief eenvoudig zijn over te nemen en in tegenstelling tot doorsnee computers veelal continu online blijven. "Zolang dergelijke apparaten aan internet verbonden blijven, zullen ze deel blijven uitmaken van botnets."

Aanpak

Het oplossen van de ontstane problematiek is complex, gaat het NCSC verder. "Leveranciers van IoT-apparatuur hebben vooral het belang om deze apparaten zo snel mogelijk en tegen zo laag mogelijke kosten op de markt te zetten. Omdat gebruikers meestal zelf geen direct nadelige consequenties ondervinden van de onveiligheid van hun apparatuur, zijn deze lastig te motiveren om meer te betalen voor een veiliger apparaat."

Alleen met een gezamenlijke, internationale aanpak en samenwerking tussen overheden en bedrijfsleven kan op langere termijn de problematiek van IoT-botnets worden teruggedrongen, zo laat het Nationaal Cyber Security Center weten.

FBI prijst Amerikaanse cyberagent in Den Haag

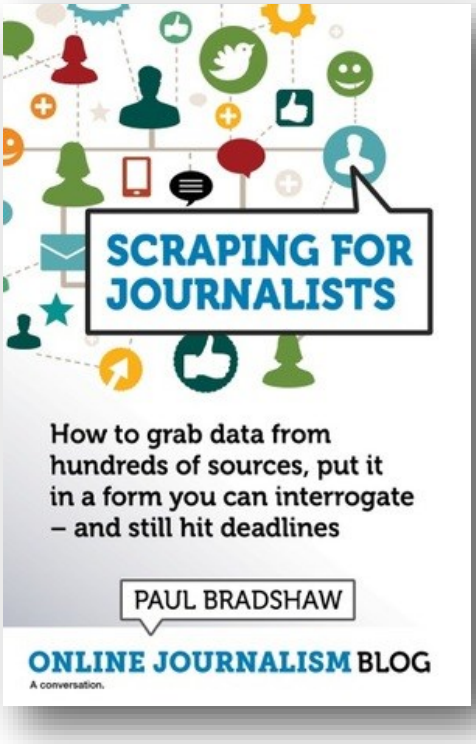
De Nederlandse ALAT doet het goed. De FBI zei vorige week zeer tevreden te zijn met het werk van de (in Den Haag gestationeerde)assistant legal attaché. ALAT's zijn FBI-medewerkers die zich bezighouden met het bestrijden van cyberdreigingen; ze zijn behalve in Nederland gestationeerd in Groot-Brittannië, Roemenië, Australië, Estland, Canada en Oekraïne.

Ze helpen bij jurisdictionele problemen, cyberwetgeving en juridische processen, delen kennis en kunde over cyberdreigingen en participeren in onderzoeken. 'Cyberagenten kunnen veelvoorkomende dreigingen identificeren en mogelijkheden vinden om deze dreigingen samen met onze internationale partners op te lossen', aldus een woordvoerder.

Is scrapen van een website computervredebreuk?

Bij scrapen wordt kort gezegd alle informatie van een website opgehaald met een geautomatiseerd proces. Vaak is dat bedoeld voor metazoekmachines zoals prijsvergelijkers, die overal de prijs vandaan halen om de beste match te kunnen tonen. Maar gescrapete informatie kan natuurlijk voor allerlei doelen worden gebruikt.

Over scrapen is juridisch veel te doen. Bronwebsites vinden het vaak niet leuk, en proberen er met gebruiksvoorwaarden, auteursrecht of databankrecht wat tegen te doen. In 2015 won Ryanair nog een zaak tegen een scrapende prijsvergelijker. Het Hof van Justitie bepaalde toen dat Ryanair in principe in haar voorwaarden scrapen mag verbieden. Een scraper mag dat dan niet doen (hoewel nog een open vraag is óf een scraper gebonden is aan die voorwaarden).



Die uitspraak is civiel recht, contractenrecht om precies te zijn. Als een scraper in strijd handelt met de voorwaarden, pleegt ze contractbreuk en moet ze de schade vergoeden. Maar dat is juridisch iets heel anders dan strafrecht, waarbij je boetes of celstraf krijgt.

Van het misdrijf computervredebreuk (art. 138ab Strafrecht) is sprake als je opzettelijk en wederrechtelijk binnendringt in een computersysteem. Het is niet vereist dat je een beveiliging kraakt; genoeg is dat je weet dat je niet mag zijn waar je bent.

Echter, bij scrapen kom je nergens waar je niet mag zijn. Je vraagt data op die openbaar en welbewust toegankelijk is gemaakt. Er worden geen URL's geraden of speciale queries gedraaid die eigenlijk niet de bedoeling zijn. Het gebruik van die data is niet de bedoeling, maar dat gebeurt een stap later. Ergo: geen strafbaar feit.

(info afkomstig van Arnoud Engelfriet, ICT jurist)

Beveiligingslek in babymonitor kan vreemden laten meekijken

Een netwerkcamera die vooral als babymonitor is bedoeld bevat verschillende kwetsbaarheden waardoor vreemden met de camera kunnen meekijken of via de microfoon met kinderen kunnen communiceren. Om welke camera het precies gaat laten onderzoekers van anti-virusbedrijf Bitdefender niet weten.

Het apparaat in kwestie beschikt over ingebouwde slaapliedjes, thermo- en luchtvochtigheidsmeter, microfoon en bewegings- en geluidsdetectiesysteem. Tijdens de installatie maakt de camera een eigen wifi-netwerk aan, waarmee de bijbehorende mobiele app op de smartphone of tablet verbinding maakt. Hierna vraagt de app om inloggegevens voor het lokale wifi-netwerk, waarna de camera hiermee verbinding maakt.

Het wifi-netwerk dat de camera opzet blijkt onbeveiligd te zijn. Gegevens tussen de app, het apparaat en de server worden daarnaast niet versleuteld uitgewisseld. Verder worden de inloggegevens van het lokale wifi-netwerk die de gebruiker invoert onversleuteld verstuurd. Als de mobiele app buiten het lokale wifi-netwerk verbinding met de camera maakt gebeurt dit via Basic Access Authentication. Een onveilige authenticatiemethode, tenzij die bijvoorbeeld in combinatie met ssl wordt gebruikt, aldus Bitdefender.

Gebruikersnaam en wachtwoord worden alleen gecodeerd en niet versleuteld verstuurd. Verder vindt de authenticatie van de camera op de server van de fabrikant plaats op basis van het mac-adres. Een aanvaller kan echter een ander apparaat met hetzelfde mac-adres registreren om zo de originele camera te imiteren. De aanvaller kan dit weer gebruiken om het wachtwoord van de gebruiker te achterhalen waarmee hij zelf op de echte camera kan inloggen.

"Iedereen kan net als de gebruiker de bijbehorende app gebruiken", zegt onderzoeker George Cabau van Bitdefender. "Dit houdt in dat als de ouders weg zijn de audio, microfoon en speakers kunnen worden ingeschakeld om met de kinderen te communiceren of ongestoorde toegang tot de live videobeelden uit de kinderkamer te hebben." De fabrikant is inmiddels ingelicht en werkt aan een update om de problemen te verhelpen. Wanneer de update beschikbaar komt is nog onbekend.

Zo versleutel je al je berichten op Facebook Messenger

Versleutelde communicatie is steeds meer een must. Nu veiligheidsdiensten steeds vaker in onze berichten willen duiken, worden chatapps zich steeds meer bewust hoeveel belang hun gebruikers hechten aan discrete communicatie. Whatsapp implementeerde eerder dit jaar daarom een volledige versleuteling van elk bericht dat vanuit de app wordt verstuurd.

Het bleek een beslissing waar Facebook later nog veel problemen mee zou krijgen. Onder meer in Brazilië werd een kopman van het bedrijf opgepakt omdat hij niet in staat was om berichten te decrypteren die verband hadden met een grote drugszaak. Misschien is dat meteen de reden waarom de encryptie van de eigen Facebook Messenger optioneel is, in plaats van standaard.

Messenger-gebruikers kunnen nu immers 'geheime gesprekken' voeren, die end-to-end versleuteld zijn, net zoals Whatsapp. Je moet echter eerst die optie inschakelen; heeft Facebook misschien schrik van meer politieke heisa? Hoe het ook komt: volledige encryptie is vanaf nu mogelijk voor iedereen die de grootste berichtendienst ter wereld gebruikt.

Om end-to-end encryptie in te schakelen, ga je als volgt te werk:

Open de applicatie en ga naar het laatste tabblad met je instellingen.

Scrol naar beneden tot je 'Geheime Gesprekken' ('Secret Conversations') ziet staan en klik erop.

Schakel 'Geheime Gesprekken' in om al je berichten te versleutelen.

Naast een volledige versleuteling van de berichten kan je een timer instellen. Zo is het mogelijk om een bericht te laten vervallen na een uur, enkele uren of één dag. De functie doet denken aan wat Snapchat doet met zijn foto's. De nieuwe functies zijn nu beschikbaar voor iedereen met de nieuwste versie van de app, vergeet dus niet te updaten.

Hoe opnieuw opstarten je computer kan redden

Zit er een computerchip in en loopt er iets mis? Dan zet je het ding maar beter even uit en opnieuw terug aan. Eenzelfde computer kan zich fataal misdragen het ene moment, en het andere moment na een reboot weer als nieuw presteren. Hoe komt het echter dat een eenvoudige ingreep als opnieuw opstarten complexe problemen kan verhelpen?

Stap voor stap

Er zijn veel redenen maar de belangrijkste heeft te maken met software. Een uitgeschakelde computer doorloopt een hele opstartprocedure die begint bij de bios op het moederbord. Die kijkt welke hardware er verbonden is. Vervolgens gaat het naar de master boot record op de opstartschijf. Daarin leest de computer waar het besturingssysteem zich bevind. Van daaruit vindt er een kettingreactie plaats: het OS wordt in het geheugen geladen en de computer wordt functioneel. Het besturingssysteem dient als manager tussen programma's en jouw input enerzijds, en de hardware anderzijds. Het OS verdeelt het geheugen, de processorkracht en alle andere beschikbare bronnen zodat iTunes vrolijk naast je browser kan werken terwijl ook Word open staat. De taak van het OS dezelfde, of je nu Linux, Mac OS, Windows of zelfs Android gebruikt.

Kleine vergissing

Het OS jongleert dus de hele tijd met taken en beschikbare systeembronnen: een huzarenstukje dat meestal goed gaat maar soms loopt er iets mis. Een taak of commando blijft onverwacht in het geheugen plakken en raakt ondergesneeuwd zodat je systeem de kluts kwijt speelt. Misschien was je flink aan het multitasken, of misschien voerde je net een update uit terwijl je favoriete programma al aan het opstarten was. Een situatie van extreme beleefdheid doet zich voor: één programma wacht braafjes op het andere om een taak af te werken, terwijl het tweede programma niet aan de slag wil gaan voor het eerste door de deur is gegaan.

Eenvoud

Wanneer je computer de kluts kwijt is, is een reboot gewoonweg de eenvoudigste optie. Bij het heropstarten begint je pc helemaal opnieuw en wordt alles terug in de juiste volgorde ingeladen. Tenzij er iets grondigs fout is met de software, is de kans klein dat hetzelfde probleem zich meteen opnieuw voor doet. Vandaag is heropstarten steeds minder nodig. Moderne besturingssystemen zijn beter dan ooit in het isoleren van probleemscenario's. Zo kan iTunes fataal vastlopen zonder dat het je hele Windows-pc meesleurt, en kan een tab in Chrome blijven hangen terwijl je browser actief blijft. Doet je computer of smartphone iets vreemds, dan is heropstarten in ieder geval altijd de eerste stap.

Warm en koud

Meestal volstaat een zogenaamde warme heropstart, waarbij je via Windows kiest voor een reboot. Je pc herstart zich in dat geval automatisch. Soms ben je echter genoodzaakt om de aan-uitknop furieus ingedrukt te houden tot je systeem uitvalt. Zo'n koude reboot heeft de naam beter te werken. Vroeger kwam zo'n koude reboot met wijze raad: "wacht zeker tot 30 seconden na het uitschakelen van de pc alvorens je het ding opnieuw inschakelt." Die 30 seconden dienden om de condensatoren van het systeem tijd te geven om leeg te lopen. 30 seconden was bij de meeste systemen sowieso al ruim genomen en is vandaag helemaal overdreven, maar het is ook nu nog een slecht idee om je desktop als knipperlicht te gebruiken.

Soms heeft een probleem niet met software te maken, maar lijkt een reboot toch te helpen. Meestal strooit een hardwaredeffect gerelateerd aan temperatuur dan roet in het eten. Een slechte koeling kan er voor zorgen dat kritieke onderdelen te warm worden en je pc kuren begint te tonen of zelfs uitvalt. Je systeem uitschakelen en even afwachten is in dat geval een (erg tijdelijke) oplossing.

Routers en modems

Niet alleen computers maar ook routers verlangen van tijd tot tijd dat je ze heropstart. Dezelfde redenen als hierboven spelen een rol. Een router is bovendien afhankelijk van een modem, en een model van de infrastructuur van je provider. Loopt er daar iets mis in de communicatie en gaat er een pakketje verloren, dan kan dat je verbinding helemaal scheeftrekken. Een router of modem resetten zorgt er voor dat het ding opnieuw een cyclus doorloopt waarbij het zich fris en monter komt aanmelden met de vraag naar een IP-adres, zodat je opnieuw aan de slag kan. Al naargelang de kwaliteit van je router, je modem of je verbinding moet je het ding vaak opnieuw opstarten, of helemaal niet. De reboot is in dit geval wederom de eenvoudigste manier om alle taken relevant voor een goede werking van de eerste tot de laatste opnieuw in de goede volgorde uit te voeren. Wat er ook aan de hand is: start je computer sowieso zelf opnieuw op als hij iets vreemds doet. Blijft hij kuren vertonen, zet hem dan nogmaals af en terug aan, en bel dat pas naar IT (of je neef die het familie-equivalent van IT is), de experts zullen je anders toch vragen om hetzelfde te doen.

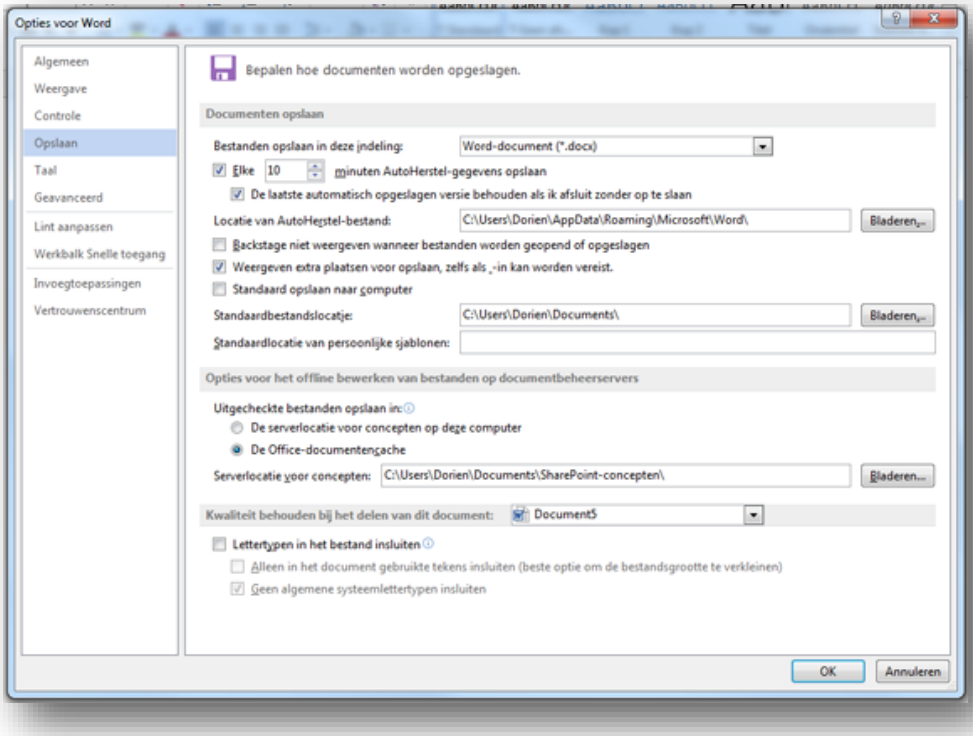
Locatie AutoHerstel-bestand in Word aanpassen

Wanneer Microsoft Word crasht, kunnen al je openstaande bestanden voor eeuwig verloren gaan. Daarom bevat Word de AutoHerstel-functie. Met deze feature kan je je bestanden regelmatig laten opslaan in een veilige map, zodat je in geval van onheil je documenten weer kan opvissen. Door een locatie in de cloud te kiezen, zijn je bestanden ook veilig wanneer je volledige computer het begeeft.

Stap 1 / Opties voor Word

De AutoHerstel-functie kan je onder de opties voor Word terugvinden. Open hiervoor een Word-document en klik links bovenaan op Bestand. In de linkerkolom zal je Opties zien staan. Klik hier op en een nieuw venster zal zich openen. Alle opties voor AutoHerstel kan je onder het submenu Opslaan terugvinden.

Stap 2 / AutoHerstel inschakelen



Alvorens je de locatie van je AutoHerstel-bestanden aanpast, dien je de functie in te schakelen. Ga hiervoor naar het submenu Opslaan van de Opties voor Word. Onder Documenten opslaan kan je de functie Elke x minuten AutoHerstel-gegevens opslaan terugvinden. Vink deze feature aan en kies hoe frequent je bestanden opgeslagen dienen te worden. Schakel eveneens De laatste automatisch opgeslagen versie behouden als ik afsluit zonder op te slaan in en je bestanden zullen te allen tijde worden opgeslagen.

Stap 3 / Locatie AutoHerstel-bestand

Ondanks het feit dat de AutoHerstel-functie nu is ingeschakeld, kan je nog steeds je bestanden kwijtraken wanneer je volledige computer crasht. Door deze back-ups op te slaan in de cloud kan je dit probleem gelukkig van de baan helpen. Ga wederom naar de Opties voor Word en kies voor Opslaan. Onder Documenten opslaan kan je de optieLocatie van AutoHerstel-bestand terugvinden. Klik op Bladeren en kies een map die tot je Dropbox, OneDrive, Google Drive, of andere clouddienst behoort.

Stap 4 / Standaard bestandslocatie

Wie helemaal het zekere voor het onzekere wil nemen, kan eveneens de Standaard bestandslocatie aanpassen. Deze functie kan je eveneens in het Opslaan-submenu bij de Opties voor Word terugvinden. Klik op Bladeren achterBestandslocatie en kies een map die tot je Dropbox, OneDrive, of Google Drive behoort. Op deze manier zal er te allen tijde een backup bestaan voor al je bestanden.

Cops in cyberspace

Facebook (inclusief Instagram) en Twitter verstrekken geen geo-data meer aan het bedrijf Geofeedia. Met software van Geofeediakonden Amerikaanse politiediensten en andere wetshandhavers locaties van mensen te vinden op basis van postings en tweets. De politie wist zo in 2014 en 2015 meerdere activisten op te sporen. De bedrijven zeggen dat Geofeedia geen toegang meer krijgt tot deze data. Facebook zegt dat hun gegevens werden misbruikt door Geofeedia, Twitter zegt de samenwerking voorlopig te hebben stopgezet. Eerder protesteerden al organisaties als de ACLU tegen het ongebreidelde gebruik van geodata door opsporingsdiensten. 'De platformen moeten meer doen om de vrijheid van meningsuiting van gekleurde activisten te beschermen en moeten stoppen het het beschikbaar stellen van hun surveillance aan de politie', zei ACLU-topvrouw Nicole Ozer. April jl werd bekend dat met name de CIA flink investeert in bedrijven als Geofeedia, Dataminr, Pathar en TransVoyant.

———————————————————

De politie heeft drie websites waarop illegaal vuurwerk werd aangeboden offline laten halen. Eind juni startte de politie, onder leiding van het Functioneel Parket in Rotterdam, een onderzoek naar de handel in illegaal vuurwerk via internet.

Daarbij kwam een 25-jarige man uit Aalst als verdachte in beeld. De verdachte in dit onderzoek bleek eigenaar te zijn van een aantal websites waarop, door middel van advertenties, illegaal vuurwerk aan consumenten te koop werd aangeboden. Zelf bood hij mogelijk ook illegaal vuurwerk aan op deze websites. Na maanden van onderzoek kwam de politie vanochtend in actie.

Een speciale aanhoudingseenheid uit Rotterdam deed een inval in de woning van de verdachte in Aalst. Daar werd hij aangehouden, net als zijn 23-jarige vriendin. Naast de arrestatie gebeurde er achter de schermen iets unieks, zo laat depolitie weten. De drie websites waarop de verdachte actief was zijn dinsdag door de politie in beslag genomen. De hostingpartij heeft de websites inmiddels volledig offline gehaald. Bezoekers krijgen de melding dat de politie de website in beslag heeft genomen.

———————————————————-

Soms gaat het goed, soms gaat het fout. Een tweet van een wijkagent uit Emmen heeft geleid tot flinke commotie. De agent schreef over 'gelukzoekende Marokkanen' die met de laatste trein richting Ter Apel wilden. 'Bus gemist. Fijne wandeling dan maar'. De tweet kreeg uiteraard veel reacties, vooral negatief. Twitteraars spraken van een 'domme uitspraak', van 'een racistisch korps daar in Emmen' en van 'een vreselijke oprisping'. Een agent kan zich niet 'openlijk verkneukelen aan het leed van mensen'. De politie Emmen liet de tweet verwijderen. Op facebook schreef de politie dat met de agent een 'stevig gesprek' is gevoerd. Woordvoerder Anthony Hogeveen zei dat het verwijderen van de tweet betekent 'dat we dit als politie niet moeten willen' en dat 'de betreffende collega hier goed van heeft geleerd'.

———————————————————

Een foto van drie jonge fietsendieven heeft tot commotie geleid . Op de foto, getwitterd door wijkagent Remy Hartog uit Barendrecht, staan de drie kinderen met hun achterkant in beeld. 'Gisteren zijn een 10, 12 en 16 jarige uit rdam aangehouden tz fietsendiefstal'. Vrijwel meteen ging de twittergemeenschap met de foto aan de haal. 'Schokkend' en 'walgelijk'. Advocaten hekelden de foto, het OM riep dat 'dit niet is zoals het hoort', en het nieuws haalde zelfs Editie NL. Maar de politie zei vooral 'te zoeken naar manieren om het publiek te informeren' over ontwikkelingen in buurt of wijk. In dat spanningsveld valt over elke politiefoto natuurlijk wel wat te zeggen maar bij deze foto ging het ook over de leeftijden. Bij kinderen onder de 12 wordt 'doorgaans' nog voorzichtiger opgetreden. Politiewoordvoerder Wim Hoonhout benadrukt dat het vooral om de boodschap gaat. 'De jongens zijn niet herkenbaar, dus hun belang wordt niet geschaad'. Ook zegt hij te willen wijzen op het feit dat fietsendieven niet altijd junks of zwervers zijn. Ook wijkagent Hartog zegt dat het niet om naming & shaming gaat maar om voorlichting en bewustwording. En al die commotie dan? Hoonhout zegt dat de politie de laatste jaren steeds transparanter is geworden en 'soms loop je dan voor bepaalde groepen en personen tegen grenzen aan'. Hij verwijst naar de huidige beeldmaatschappij waarin collega's beelden gebruiken om te laten zien wat ze doen maar daarbij ook tegen die grenzen oplopen.

———————————————————

Omdat facebook een 'laagdrempelig middel' is om informatie te delen én de politie 'graag in contact staat' met de wijkbewoners, heeft de politie Amsterdam-Centrum deze week getest of het mogelijk is meldingen te doen via dat facebook. Het gaat om meldingen uit postcodegebied 102, Wallen en omgeving. Zolang het niet om levensbedreigende situaties gaat, mogen burgers hun meldingen via facebook doen, via een speciaal opgezet evenement. Daar wordt benadrukt dat privacygevoelige informatie het best via een privébericht kan worden gedeeld.

———————————————————

Een virtuele rechercheur genaamd Sjerlok speurt voor verzekeraar Delta Lloyd op internet naar gestolen auto's, boten, sieraden en elektronica.

Met succes: volgens het bedrijf is er al voor tientallen miljoenen euro's aan gestolen spullen teruggevonden. Sjerlok zoekt bij een gestolen auto niet alleen op kenteken, kleur en type maar ook op foto en kleur van de bekleding, en dat op sites als Marktplaats, eBay en speciale autoverkoopsites.

Het systeem levert een top-10 die door mensen wordt bekeken en geanalyseerd. Een gespecialiseerd bedrijf haalt samen met de politie de auto dan weer op.

De makers van Sjerlok zeggen dat de software ook aan andere verzekeraars zal worden aangeboden.

Rechtspraak

Niet voor het eerst is een verdachte veroordeeld die een burgemeester op sociale media beledigde, zwartmaakte dan wel bedreigde. De man (51, uit Sint Maarten) die burgemeester Cees van der Knaap van de gemeente Ede op facebook betichtte van leugenachtigheid en
vriendjespolitiek, kreeg deze week een taakstraf van veertig uuropgelegd. Hij noemde Van der Knaap in een discussie over asielzoekerscentra 'meneer Schandknaap' en schreef dat die wel 'twintig keer op een leugen is betrapt'. Smaad, vond de officier. Ze eiste zestig uur taakstraf
waarvan twintig voorwaardelijk. De politierechter volgde die eis, ook al omdat de verdachte de tekst weer van facebook haalde en spijt betuigde.
In een andere gemeente, Bedum in Groningen, is deze week overigens een nep-twitteraccount ontdekt van burgemeester Henk Bakker. In diens bio staat dat hij sociale media 'eigenlijk
maar niks' vindt. 'Amen. Parodie'. Bakker staat sceptisch tegenover het gebruik van sociale media voor gemeenten en zegt van niks te weten. 'Het bevestigt voor mij de risico's van sociale media'.

———————————————————

De politierechter in Utrecht heeft 'treitervlogger' Kamal el A. (27, uit Hilversum) 300 euro boete opgelegd voor het beledigen van een agent en een cameraman van het NOS Journaal. De verdachte, online bekend als Ikvosonline, moet de agent verder 100 euro schadevergoeding betalen. In het filmpje is te zien hoe de vlogger NOS-verslaggever Gerri Eickhof en diens cameraman hindert bij het maken van straatinterviews. Op een gegeven moment schopt de cameraman de vlogger tegen zijn schenen trapt. Eickhof belt vervolgens de politie, de vlogger eist van de agent dat hij de journalisten aanpakt. Als de agent dat weigert, ontstaat natuurlijk een relletje. El A. filmt verder, roept onder meer de volledige naam van de agent maar ook dat deze wat hem betreft 'vergast' moet worden. 'Irritant gedrag, heel persoonlijk en bijzonder kwetsend', vond de officier van justitie die 600 euro boete en 300 euro schadevergoeding eiste. De advocaat van de vlogger vond de belediging bewezen maar de strafeis buiten proportie. Met succes: de rechter vond dat deels ook.

———————————————————

'Lokpedo' Danny D. (43, uit Koudekerk aan den Rijn) is veroordeeldtot drie jaar cel en tbs met dwangverpleging. De verdachte misbruikte in 2015 de (toen) 13-jarige Lisa, pleegde ontucht met een ander meisje en verleidde 15 meisjes tot webcamseks. Hij vond zijn slachtoffers online, via chatsites vooral. Daar deed hij zich voor als 14-jarige. 'Als ik had gezegd dat ik 41 ben, wil natuurlijk niemand met mij chatten'. De zaak kreeg grote aandacht toen Lisa verdween van de camping waar ze met haar ouders verbleef en vijf dagen later werd aangetroffen in een bus, op weg naar Danny. Het OM had zeven jaar en tbs geëist voor verkrachting en weglokking, maar de rechtbank vond de verkrachting niet bewezen; het seksueel misbruik wel. Volgens de rechter is het nog maar de vraag of de verdachte 'ooit nog op straat te zien zal zijn': zijn tbs-behandeling zal 'heel langdurig' zijn. De verdachte werd in 2011 al eens veroordeeld voor productie en bezit van kinderporno. Van die straf stonden nog zes maanden voorwaardelijk open. Hij stond nog onder toezicht van de reclassering toen hij online met de meisjes afspraken maakte.

———————————————————-

'Superhacker' Jair M. (22, uit Rotterdam) is in hoger beroepveroordeeld tot 240 uur taakstraf voor allerlei vormen van computercriminaliteit. De verdachte zette in 2013 een vwo-examen Frans op internet. De politie wist daarmee later examenfraude aan te tonen op een school in Rotterdam. Een rechtbank veroordeelde Jair, waarna hij in beroep ging. Het Hof legde de man 497 dagen celstraf op, waarvan 360 dagen voorwaardelijk. De andere 137 zat de verdachte in voorarrest uit. Volgens het Hof wist Jair via een door hem gemaakte nepsite malware te verspreiden, kon hij zo honderden mensen bespieden en privégegevens stelen. In één geval maakte hij het nog bonter: hij zette een geheim filmpje van een masturberend meisje op haar facebookpagina. 'De verdachte maakte zo een zeer ernstige inbreuk op haar persoonlijke levenssfeer'. Hij veroorzaakte veel leed 'uitgerekend in een kring van bekenden van het slachtoffer'.

———————————————————

Een man (26, uit Klazienaveen)
is veroordeeld tot veertig uur werkstraf voor het bedreigen van premier Mark Rutte en enkele andere Europese politici. De man dreigde op een aan Pegida gelieerde facebookpagina dat hij Rutte 'eens zou opzoeken' en hem wat zou aandoen. Hij schreef verder over 'bommen op Brussel' en het 'afknallen' van Europese regeringsleiders. Naar eigen zeggen was de bedreiging niet aan Rutte gericht maar aan iemand anders. Onzin, vond de rechter: bij het dreigbericht stond een foto van Rutte. De verdachte zegt inmiddels gestopt te zijn met sociale media.

———————————————————

De rechter in Almelo heeft een man (56, uit Vriezenveen)veroordeeld tot dertig uur werkstraf en twee weken voorwaardelijk (proeftijd drie jaar). De verdachte liet op het station zijn piemel zien aan een minderjarig meisje, in de trein masturbeerde hij voor haar. Het meisje maakte echter foto's van de man en zette die op facebook. De foto's werden massaal gedeeld waarop de politie een onderzoek startte. De man werd snel herkend, al was het maar omdat hij begin 2016 ook al voor schennispleging werd veroordeeld. De rechter vonniste daarom hoger dan het OM eiste.

———————————————————

Verschijningsvorm cybercrime	138ab *lid 1*	138ab *lid 2*	138ab *lid 3*	138b	139c *lid 1*	139d	139e	161 *sexies*	161 *septies*	350a *lid 1*	350a *lid 2*	350a *lid 3*	350b *lid1*	350b *lid2*
● Malware														
Malware maken en/of verspreiden	X					X		X	X	X	X	X	X	X
Malware (Trojaanse paarden) gebruiken	X	X			X			X	X	X	X	X	X	
● Computerinbraak														
Computerinbraak (hacking)	X		X								X			
Computerinbraak vervolg-handelingen		X	X		X	X	X	X	X	X	X	X		
Portscan						X								
Spoofing/cache poisoning	X	X		X	X	X	X	X		X	X			
Sniffing					X	X	X			X				
Draadloze netwerken hacken/ misbruiken	X	X	X	X	X		X	X		X	X			
Password guessing	X			X		X								
● Website aanvallen														
Veroorzaken open relay									X				X	
Wederrechtelijk open relay gebruiken	X							X		X				
Defacing/vernielen website	X							X	X	X			X	
Defacing/doorleiden internet-verkeer	X							X	X	X				
Cross-site scripting	X	X			X	X	X	X		X			X	
SQL-injecties	X	X						X		X				
● Botnets														
Botnet bouwen en beheren	X	X	X		X					X		X		
● Denial of Service														
DDoS-aanval				X				X		X			X	
● Social Engineering														
Phishing		X			X		X							
Vishing/Smishing		X			X									
● E-mail gerelateerd														
Wederrechtelijk open mail relay gebruiken	X							X	X	X				
Spamming (met DoS tot gevolg)				X				X	X				X	

Wetsartikel

Art. 138ab, lid 1 Sr Hacken: opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk

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

Art. 138ab, lid 3 Sr Hacken door tussenkomst van een openbaar telecommunicatienetwerk

Art. 138b Sr Het belemmeren van toegang tot of gebruik van een geautomatiseerd werk

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

Art. 139d, lid 1 Sr Plaatsen van opname-, aftap- of afluisterapparatuur; voorbereidingshandelingen

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

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

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

Art. 161sexies Sr Opzettelijk vernielen etc. van een geautomatiseerd werk of werk voor telecommunicatie; voorbereidingshandelingen

Art. 161septies Sr Vernieling etc. van een geautomatiseerd werk of werk voor telecommunicatie door schuld

Art. 231b Sr Identiteitsfraude

Art. 232 Sr Opzettelijk valselijk opmaken, vervalsen, gebruiken, etc. van betaalpas, waardekaart e.d.

Art. 240b Sr Kinderpornografie

Art. 248e Sr Grooming

Art. 273, lid 2 Sr Bekendmaking bedrijfsgeheimen; heling computergegevens ondernemingen

Art. 273d Sr Schending telecommunicatiegeheim

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

Art. 326c Sr Het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen

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

Art. 350a, lid 2 Sr Het feit gepleegd in lid 1 met tussenkomst van een openbaar telecommunicatienetwerk

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

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

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

Video

Tek Tok Late Night:

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

You Tube:

Doe jij het veilig online
Malware
WiFi ontvangst verbeteren
Internetfraude via de telefoon
Documentaire: Veiligheid en privacy
Herken een nep-hotspot
Gebruik wachtzinnen
Drive-by-downloads voorkomen
Hoe herken je een phishing mail
Beveiligd internetbankieren
Privacy—ik heb toch niets te verbergen
Webinar Computercriminaliteit
Mousejack
Gegijzeld door Ransomware. Wat nu?
Telefonische phishing

Help wanted:

Grooming
Sexting
Webcammisbruik
Bedreigd/gechanteerd
Kinderporno
Nepprofiel

Handig

Phishing- / valse e-mails melden:

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

ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

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

Tips voor veilig handelen op Marktplaats

Internetoplichting: controleer vooraf de (bank)gegevens van de verkoper via

www.mijnpolitie.nl/miocheck

Komt de verkoper voor op de website Opgelet op internet ?

Malware ID website met info omtrent verwijderen van infecties

PCrisk verwijderingsrichtlijnen voor spyware en virussen

Cookie Verwijderen kennisdatabase voor het verwijderen van adware, hijackers, ransomware, toolbars en pop-ups

Computer woordenboek

Veel meer handige tips vindt u op de Secure Computing website.