December 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. Tweede Kamer

Nederlandse internetgebruikers hebben nu al maanden met zogenaamde winacties van Ikea, Albert-Heijn, Kruidvat, NS en andere bedrijven te maken, die mensen proberen op te lichten,.

Overlast door zogenaamde winacties Ikea, Kruidvat en NS

Al in juli waarschuwde Ikea voor de malafide winacties, waarbij wordt geprobeerd om persoonlijke gegevens van gebruikers te verzamelen.

Ook Albert-Heijn waarschuwde dezelfde maand voor de winacties en het Kruidvat volgde in september. De zogenaamde winacties blijven nog altijd voor overlast zorgen, zo melden
de Fraudehelpdesk en Consumentenbond. "Consumenten die hun gegevens invullen, lopen een aantal risico's: vastzitten aan een abonnement, slachtoffer worden van phishing of aan het lijntje gehouden worden bij een duur 0909-nummer", aldus de Consumentenbond.

De organisatie vreest dat het einde nog niet in zicht is. "Als een bedrijf stappen onderneemt tegen prijsvragen die zogenaamd van hen afkomstig zijn, gaat dit soort misleiding weer verder met de naam van een ander bedrijf." Consumenten krijgen daarom het advies om nooit te reageren op bedrijven die zomaar iets weggeven. De misleidende prijsvragen kunnen consumenten flink op kosten jagen. De 'NS-dagkaartactie' lokte de aangeschrevenen naar een prijsvraagabonnement van 12 euro per week en de Ikea-prijsvraag stuurde deelnemers naar een 0909-nummer waar ze 200 vragen moesten beantwoorden.

Bron: Security NL

Index

Encryptie kan je communicatie privé houden en je bestanden beschermen tegen spiekende ogen, maar het kan zich ook tegen je keren.

Nieuwe ransomware neemt complete websites in gijzeling

De afgelopen jaren hebben online criminelen een nieuwe klasse malware ontwikkeld, genaamd ransomware, om geld te maken van deze encryptie. Dit doen ze door bestanden te versleutelen en ze op deze wijze voor losgeld in gijzeling te nemen. Alsof dat al niet erg genoeg was, hebben beveiligingsonderzoekers nu een nieuwe soort ransomware geïdentificeerd die zich richt op Linux-based web servers, waardoor ze complete websites kunnen gijzelen totdat het slachtoffer financieel over de brug komt.

De ransomware heet “Linux.Encoder.1” en beveiligingsbedrijf Doctor Web heeft gezien dat het zijn tanden heeft gezet in een handjevol websites tot nu toe. Slachtoffers lopen momenteel in de tientallen, maar elke keer dat het een website afsluit, eist de malware één Bitcoin in betaling. Dat is rond de 310 Euro, omgerekend.

Veel van de geïnfecteerde systemen werden besmet via een kwetsbaarheid in het Magneto CMS. Een patch werd op 31 oktober uitgerold om dit gat te dichten, maar niet alle gebruikers krijgen de nieuwste versie direct geïnstalleerd. De opbrengst van de eerste aanvalsgolf kan ook worden gebruikt om een nieuw lek te “kopen”, wat kan leiden tot een nog bredere aanval.

Net als bij andere ransomware oplichtingen worden alle gekoppelde volumes versleuteld nadat Linux.Encoder.1 toegang heeft tot de webserver. Dit wordt gedaan met een RSA-2048 sleutel die niet kan worden gedupliceerd. De Malware zoekt naar Apache, MySQL en Nginx installaties in de server voordat hij aan het werk gaat, waardoor belangrijke bestanden veilig worden gesteld: de bestanden die het slachtoffer het liefst terug wil. Het gaat op zoek naar bestanden als Windows executables, programma libraries, JavaScript documenten en meer.

In elke directory die wordt versleuteld laat Linux.Encoder.1 een tekstbestand achter genaamd README_FOR_DECRYPT.txt. dit is de losgeldbrief. Het legt uit dat de inhoud van de server versleuteld is, en om de bestanden terug te krijgen, je 1 Bitcoin moet betalen aan de aanvallers op een specifiek Bitcoin adres. Er staat een adres gelinkt aan een deep web met een Tor2Web redirect.

README_FOR_DECRYPT.txt

```
1  Your personal files are encrypted! Encryption was produced using a unique public key RSA-2048
   generated for this computer.
2
3  To decrypt files you need to obtain the private key.
4
5  The single copy of the private key, which will allow to decrypt the files, located on a secret
   server at the Internet. After that, nobody and never will be able to restore files...
6
7  To obtain the private key and php script for this computer, which will automatically decrypt
   files, you need to pay 1 bitcoin(s) (~420 USD).
8  Without this key, you will never be able to get your original files back.
9
10
11 ---------------------------------------
12
13 !!!!!!!!!!!!!!!!!!!!! PURSE FOR PAYMENT(ALSO AUTHORIZATION CODE):
   xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx !!!!!!!!!!!!!!!!!!!!!
14 WEBSITE: https://z54n57pg2el6uze2.onion.to
15
16 INSTRUCTION FOR DECRYPT:
```

Als het slachtoffer betaald, zeggen de aanvallers dat ze de sleutelcode zullen geven waarmee alle bestanden kunnen worden unlocked. Dat is als de aanvallers hun woord houden natuurlijk.

Het proces is wat minder verfijnd dan eerdere ransomware aanvallen, en de bestanden in kwestie kunnen van grotere commerciële waarde zijn. Dat maakt de kans dat de eigenaar betaald natuurlijk groter. De beste manier om deze oplichting te vermijden is om je beveiliging up to date te houden en een backup te hebben van de belangrijke bestanden op een andere locatie.

Bron: PC magazine

Index

Is het toegestaan dat derden je kenteken op een openbaar forum plaatsen samen met datum en tijdstip dat men je gespot heeft? Dat kan dan zijn om over je auto te praten, of om je uit te maken voor wegmisbruiker.

Is het toegestaan om kentekens op openbare fora te plaatsen?

Een kenteken wordt gezien als een persoonsgegeven, omdat het te herleiden is tot de eigenaar van de auto. Dat je daarvoor langs de RDW moet, is niet relevant. (En soms kan het ook zonder RDW: mensen kunnen een advertentie plaatsen waarin ze met naam en dergelijke hun auto te koop aanbieden.)

Een persoonsgegeven publiceren mag alleen als je dat onder de Wet bescherming persoonsgegevens kunt rechtvaardigen. Toestemming is de meest gehoorde rechtvaardiging, maar die is er in dit geval niet.

In principe kom je dan uit bij de restcategorie van de eigen dringende noodzaak. Je zegt dan, ik kan geen toestemming vragen, ik heb een legitiem belang en daarvoor is het een absolute noodzaak dat ik dit gegeven publiceer, bovendien heb ik zo veel mogelijk rekening gehouden met de privacy van de persoon over wie het gaat.

Het legitiem belang zou hem hier zitten in die discussie, dat is immers een beroep op de vrijheid van meningsuiting. In principe is dat al snel gerechtvaardigd, tenzij de discussie niet meer is dan belachelijk maken en afzeiken zonder enige werkelijke discussie of debat. "Deze auto is een wegmisbruiker" zou ik al net aan de goede kant van de grens vinden zitten, als de beelden dat duidelijk laten zien.

Alleen dat rekening houden met de privacy, wat moet je daar dan mee? Ik denk dat dat er toch al snel op neerkomt dat het nummerbord uitgeblurd moet worden. Dat is immers niet echt nodig voor de discussie over wegen misbruiken of om je mening over de auto te geven, positief of negatief. Natuurlijk, met nummerbord kunnen anderen de auto herkennen, maar hoe relevant is dat?

Arnoud Engelfriet is ICT-jurist, gespecialiseerd in internetrecht waar hij zich al sinds 1993 mee bezighoudt. Hij werkt als partner bij juridisch adviesbureau ICTRecht. Zijn site Ius mentis is één van de meest uitgebreide sites van Nederland over internetrecht, techniek en intellectueel eigendom.

Bron: Arnoud Engelfriet

Index

Er gaat een nieuwe versie rond van de hardnekkige ransomware trojan TeslaCrypt.

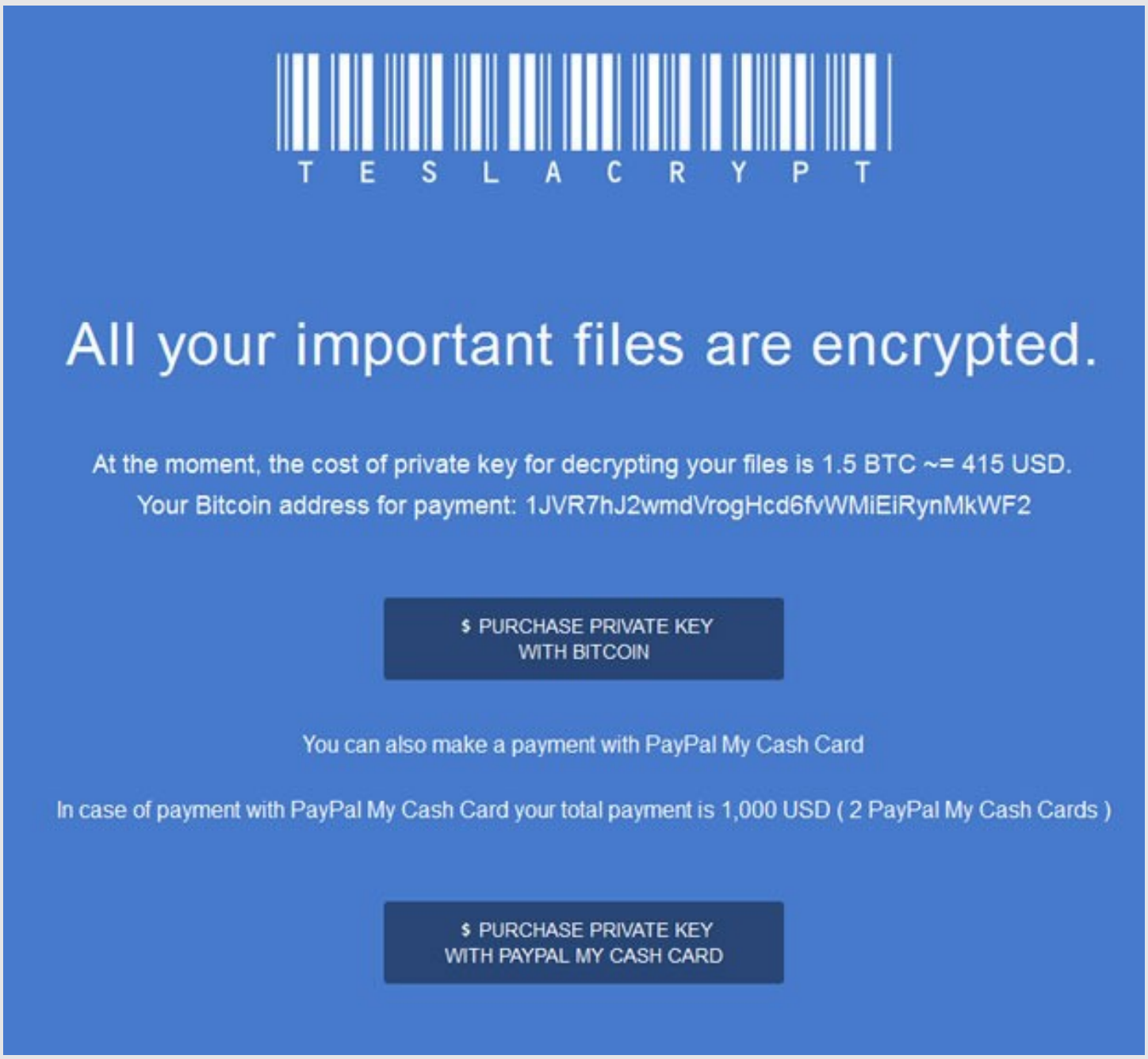
Nieuwe versie TeslaCrypt in het wild gesignaleerd

Hoewel er niet veel vernieuwd lijkt te zijn aan de software, is het erg lastig om ervan af te komen.De nieuwe variant, TeslaCrypt v2.2.0, versleutelt bestanden met de .ccc-bestandsextensie, zoals in eerdere versies ook gebeurde.

Wel nieuw is dat er meerdere namen voor de losgeld- notificatiebestanden worden gebruikt. Volgens berichten op fora kan die bestandsnaam variëren en ziet het eruit als '_how_recover_.HTML' of '_how_recover_.TXT'.

De ransomware TeslaCrypt werd eerder dit jaar voor het eerst aangetroffen en heeft het gemunt op bestanden met extensies die vooral met games te maken hadden. Om weer toegang tot de bestanden te krijgen, werd vaak 500 dollar geëist.

Volgens Bleepingcomputer is het vrijwel onmogelijk om de versleuteling van TeslaCrypt v2.2.0 ongedaan te maken zonder de cybercriminelen te betalen. Omdat bij versie 1 nog gebruik werd gemaakt van een symmetrische encryptiemethode, werd al snel een tool ontwikkeld om gegijzelde bestanden 'te bevrijden' zonder te hoeven betalen. Bij deze nieuwe variant werkt die tool helaas niet meer.



Bron: Security NL

Index

De Europese Commissie overweegt om links op internet onder het auteursrecht te laten vallen. Daarmee zou het zonder toestemming plaatsen van een hyperlink naar auteursrechtelijk beschermd materiaal strafbaar kunnen worden.

Europese Commissie wil auteursrecht op hyperlinks

Een an ander is gebaseerd op de voorlopige versie van een document waarin de Europese Commissie uiteenzet waar zij zich het komende jaar zoal op wil richten. Daarin staat dat de commissie op het gebied van auteursrecht duidelijker wil gaan definiëren wat wel en niet geldt als een nieuwe openbaarmaking. Als wordt besloten dat hyperlinks dat inderdaad zijn, moet iedereen die openbaar wil linken naar auteursrechtelijk beschermd materiaal daar eerst toestemming voor vragen.

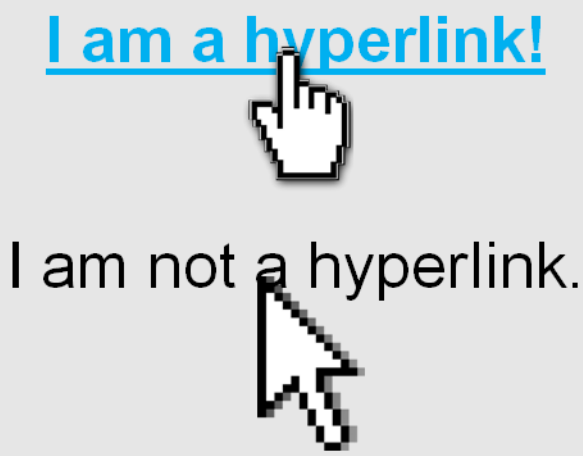
Er is sprake van 'een frontale aanval op de hyperlink, de bouwsteen waarop het internet dat we kennen is gebouwd.'

Volgens enkele Europese politci is dit idee een klap in het gezicht van de bestaande wetgeving, de geest van de wet en het gezond verstand. Het is niet voor het eerst dat de Europese Commissie een dergelijke maatregel overweegt.

Volgens ict-jurist Arnoud Engelfriet van juridisch adviesbureau ICTRecht hoeven internetters zich voorlopig geen zorgen te maken. 'Ik zou van mijn stoel vallen als deze voorstellen het daadwerkelijk gaan halen. Ze gaan lijnrecht in tegen uitspraken van het Europees Hof, dat duidelijk heeft bepaald dat hyperlinks geen inbreuk van auteursrechten kunnen zijn. Feitelijk gezien zou de Europese Commissie daar tegenin kunnen gaan, maar dat gebeurt vrijwel nooit.' En als de Europese Commissie er toch serieus mee aan de slag zou gaan, dan duurt het even voordat dergelijke wetgeving is geïmplementeerd. 'Dat gaat minstens vijf jaar duren', aldus Engelfriet. 'Maar ik denk dat hier voorbarig alarm is geslagen.'

Het strafbaar stellen van linken naar auteursrechtelijk materiaal is al langer onderwerp van discussie. De Duitse Eurocommissaris Günther Oettinger (Digitale economie en samenleving) pleitte vorig jaar nog voor een systeem waarbij internetbedrijven als Google een vergoeding zouden moeten betalen als ze auteursrechtelijk beschermde content verwerken. In 2013 mocht GeenStijl van de rechter geen link plaatsen naar naaktfoto's van Britt Dekker in de Playboy. Het hof draaide later de beslissing van de rechter dat er sprake was van auteursrechteninbreuk terug. Wel werd het weblog veroordeeld voor het onrechtmatig handelen tegenover Dekker en het mannenblad.

Engelfriet: 'Het ging toen om nog niet gepubliceerd materiaal, dat via diefstal was verkregen. Dan gelden andere regels. Maar het klopt dat bij de Europese Commissie op dit gebied de grenzen worden afgetast van wat wel en niet mag.'



Bron:

Index

Een bedrijf uit Enschede heeft een router ontwikkeld die gebruikers een advertentievrij internet belooft.

Nederlandse router belooft advertentievrij internet

De Zenrouter maakt gebruik van een DNS-filter dat uit meerdere openbare lijsten is samengesteld. "Tweemaal per week haalt de router een nieuwe versie op van het filter, vanaf onze eigen servers", zegt bedenker Martin Nobel.

De software heeft Nobel volledig in eigen beheer ontwikkeld, de hardware wordt als OEM bij een groothandel afgenomen. "De processor en wifi-chips zijn gangbare types, zoals die ook in routers van gerenommeerde fabrikanten zitten", aldus de Nederlandse routerbouwer. De dual-band-router ondersteunt de nieuwe draadloze standaard 802.11ac. Doordat de router zelf de advertenties blokkeert is het niet meer nodig om op aangesloten apparaten zoals laptops of smartphones een adblocker te installeren.

"Niet alleen advertenties worden tegengehouden, ook wordt het onmogelijk voor kwaadaardige software om via advertenties je toestellen te infecteren. Bovendien worden de zogeheten trackers geweerd. Zo is het voor al te nieuwsgierige bedrijven een stuk lastiger om je overal online te volgen", stelt Nobel. Door het blokkeren van advertenties wil hij dat het internet weer een bron van kennis en informatie wordt, "in plaats van een marketinginstrument."

De eerste exemplaren van de Zenrouter, die 60 euro kost, zijn per direct leverbaar. De routers die nu worden geproduceerd zijn vanaf januari 2016 verkrijgbaar. Dan zal het ook besteltraject geprofessionaliseerd zijn, waarbij de router via verschillende kanalen zal worden aangeboden.

Bron: Zenrouter

Index

Facebook gaat voortaan gebruikers rechtstreeks waarschuwen als er een sterk vermoeden bestaat dan hun account door een landelijke overheid is gehackt.

Facebook waarschuwt bij hacks door overheden

Dat schrijft hoofd beveiliging Alex Stamos op het officiële Facebook-blog.

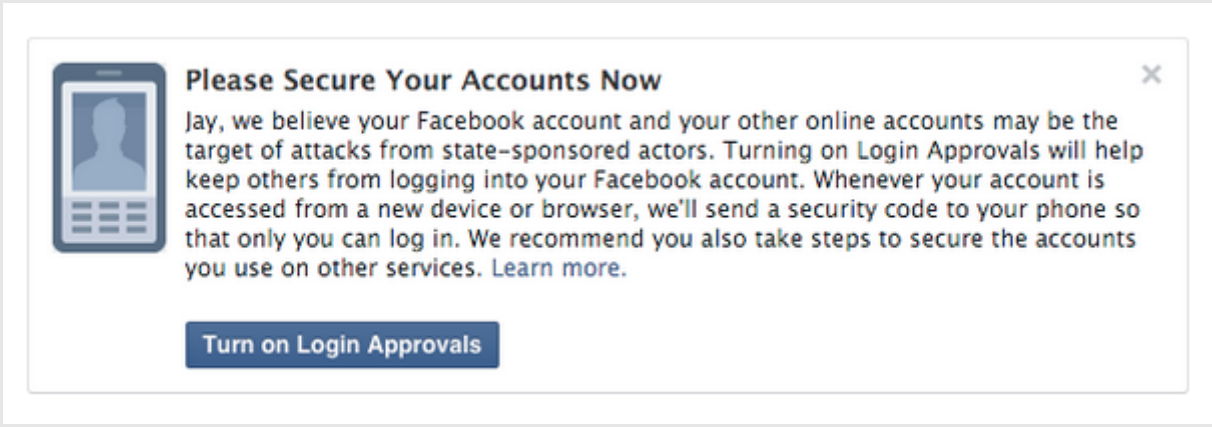
Via dit bericht wordt gevraagd om hun aanmeldingsproces extra te beveiligen. Elke keer als ze via een onbekend apparaat inloggen op Facebook, zullen ze per sms een code krijgen die ze moeten invullen, een tweetrapsverificatie genoemd. Op deze manier probeert Facebook een extra beschermingslaag in te bouwen.

"We hebben altijd al stappen ondernomen om accounts te beveiligen waarvan we vermoeden dat ze gehackt zijn. We hebben nu besloten om gebruikers zelf ook actief te gaan waarschuwen, omdat hacks die gepleegd zijn in naam van een overheid doorgaans geavanceerder en gevaarlijker zijn dan andere digitale inbraken."

- Alex Stamos, hoofd beveiliging Facebook

De melding zal alleen verschijnen als het vermoeden van Facebook ondersteund wordt door overtuigend bewijs. Hoe Facebook bepaalt of er sprake is van een overheidshack wil Stamos niet prijsgeven, om de methodes van Facebook te beschermen. Meestal kijken beveiligingsexperts onder meer naar de servers waar een bepaalde aanval vandaan komt, maar dit werkt niet altijd. Aanvallers kunnen namelijk moeilijk traceerbaar zijn en de beveiligers op een verkeerd spoor zetten.

Facebook is niet het eerste bedrijf dat gebruikers actief waarschuwt als hun account hoogstwaarschijnlijk door een land is gehackt. Google doet dit al sinds 2012 voor Gmail-gebruikers.



Bron: HCC

Index

Met Firefox 42 introduceert Mozilla zijn eerste officiële 64bit-browser voor Windows.

Firefox biedt bescherming tegen tracking

Het is nu mogelijk om in de privacy-modus websites geen trackingcookies meer te laten installeren, wat in de praktijk neerkomt op het blokkeren van banners.

Gebruikers met Windows en de 64bit-versie van Firefox 42 moeten het wel doen zonder ondersteuning voor Java en Silverlight. Mozilla kondigde kortgeleden al aan de ondersteuning voor npapi-plug-ins aan het eind van 2016 in alle versies van de browser te beëindigen. Het is niet mogelijk een 32bits versie te upgraden naar een 64bit-variant. Deze laatste zal rechtstreeks gedownload en apart geïnstalleerd moeten worden.

Ook is het privébrowsen aangepakt. Het is nu mogelijk om 'Bescherming tegen volgen gebruikers in privévensters' aan te vinken bij browsen in privacy-modus. De andere optie 'Websites vragen niet te volgen' is de oude 'Websites laten weten dat ik niet gevolgd wil worden'-optie. Het verschil zit erin dat de laatste optie vraagt niet te volgen, met andere woorden: de 'do not track'-functie. De bescherming tegen volgen maakt daarentegen gebruik van een door de anti-volgorganisatie Disconnect aangeboden lijst voor het herkennen en blokkeren van trackers. Als de functie gebruikt wordt, verschijnt er een schildpictogram in de adresbalk links naast het internetadres.

De ingebouwde wachtwoordmanager kan nu ook data en wachtwoorden van Microsoft Edge, Internet Explorer en Chrome importeren, waardoor switchen makkelijker moet worden. Net als in Chrome kan het geluid van tabs nu ook individueel gedempt worden en wordt de source code van een pagina niet meer in een los venster, maar in een aparte tab geopend. Ook heeft WebRTC enkele verbeteringen meegekregen, zoals ipv6-ondersteuning. Op het gebied van personalisatie is het nu mogelijk om een foto of ander plaatje toe te voegen bij de gebruikers. De hele lijst veranderingen is op de Mozilla-website te vinden.

Bron: HCC

Index

Met de nietigverklaring van Safe Harbor wordt online privacy weer een stukje ingewikkelder. Maar wie ligt er überhaupt wakker van privacy? ***(opninie door Jens de Wit, medewerker ZDnet Benelux)***

Waarom niemand wakker ligt van zijn privacy

Zijn we allemaal lui? Heeft het te maken met gemakzucht, nieuwsgierigheid of voyeurisme? Of zijn we gewoon allemaal dom? Wie een website bezoekt, geeft de toestemming om cookies te bewaren op zijn computer, we weten dat Facebook ons volgt doorheen onze ontdekkingsreis van het wereldwijde web en Google toont ons advertenties op basis van onze zoekgeschiedenis. We weten het, doen er niets tegen en toch hebben we het gevoel dat ons recht op privacy ons wordt afgenomen.

Reclame op maat

Ik heb het steevast een beetje moeilijk met mensen die moord en brand schreeuwen wanneer blijkt dat Facebook of Google weer een nieuw foefje heeft bedacht om advertenties aan te passen aan ons internetprofiel. Ik begrijp het probleem wel, maar ik trek er mij eerlijk gezegd niet al te veel van aan. Wat is er mis met wat reclame op mijn maat?

Ik heb maanden gezocht naar een audio interface om thuis zelf wat muziek op te nemen, en het antwoord werd mij ten slotte aangereikt door Facebook via een advertentie in de zijbalk. Gekocht, geprobeerd en tevreden. Cookies zijn bovendien niet enkel gericht om je koopgedrag te activeren, ze helpen je surfervaring vooruit door websites sneller te laden. In een tijd waarin onze technologie steeds sneller moet zijn, steeds praktischer en altijd maar gebruiksvriendelijk, zal je helaas enkele compromissen moeten slikken.

Wit, zwart en grijs

Wil dat dan zeggen dat je alles zomaar moet aanvaarden? Nee. Wie niets fout gedaan heeft, verdient het niet om gestalkt te worden door de NSA en aanverwanten. Let wel: dat is niet hetzelfde als 'om te lachen' praten over aanslagen en dan verbaasd zijn dat de politie voor je deur staat.

Wat ik wil zeggen, is dit: acties hebben gevolgen. Wie niets fout doet, heeft niets te vrezen. Wie dapper en zonder vrees decibels gaat produceren, zal dat altijd ondervinden. Des te meer in een tijd waarin angst en massahysterie de plak zwaait, aangezwengeld door IS en Poetin – kwestie van alle hete hangijzers erbij te betrekken. Wie echter zijn vrouw bedriegt op Asley Madison, heeft weinig morele grond om te klagen wanneer hij erbij gelapt wordt en zijn gegevens online ziet verschijnen. Bedrog kan altijd uitkomen.

"Acties hebben gevolgen"

Braaf schaap

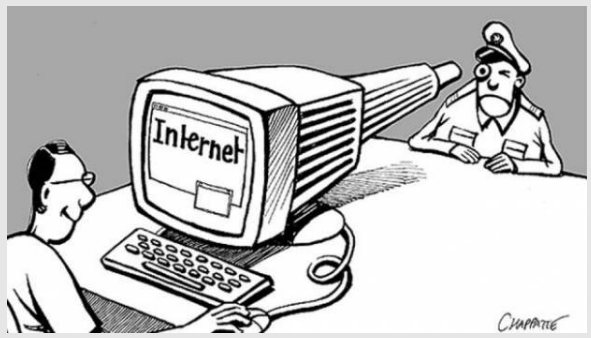
Wie liever niet gevolgd wordt door de NSA, de politie en anderen: niemand verplicht je om aanwezig te zijn op sociale media. Wanneer je je inschrijft, doe je dat onder hun voorwaarden, die jij, net als ik overigens, niet gelezen hebt. Ik begrijp dat het soms moeilijk is om te aanvaarden dat bedrijven als Facebook en Google kunnen doen wat ze willen, maar zolang we aanwezig blijven op hun platformen, geef je stilzwijgend je goedkeuring.

"Zolang je aanwezig blijft, ga je akkoord."

Maar wat dan met de verbreking van Safe Harbor? Nu Amerika niet langer een veilige datahaven blijkt voor onze privacygegevens, zal er dan veel veranderen? Dat lijkt mij alvast weinig waarschijnlijk. De Amerikaanse overheid heeft in het verleden al meermaals duidelijk aangegeven dat het zich niet veel aantrekt van internetrechten, met initiatieven als SOPA en PIPA, waarbij het piraterij wou verbieden, maar in se het halve internet kon afsluiten.

Welkom in de kudde

Daarnaast werkt Facebook aan een nieuwe privacyverklaring. Aangezien het nog steeds gegevens kan verzamelen indien het daar per individu de toestemming voor vraagt, zal het dat dan ook doen. En gaan wij dan weigeren? Weigeren betekent haast per definitie een afscheid van het populaire gezichtenboek. Ik ben een schaap, en ik zal de verklaring stilzwijgend goedkeuren. Maar kan dat kwaad? En moet ik daar wakker van liggen? En is dat dan omdat ik lui ben, de kudde volg of ben ik gewoon een Facebook-voyeur?



Bron: ZDnet

Index

Wat doe je als je een e-mailadres wil maken dat compleet geheim en naamloos is, zonder connecties met wat dan ook, en zonder het gedoe van het opzetten van je eigen server?

Op deze manier kun je anoniem e-mailen

Dit gaat verder dan alleen het versleutelen van je berichten (iets wat iedereen kan doen met een web-based e-mailaccount als Gmail door browserextensies te gebruiken als Secure Mail by Streak. Of, voor desktop email clients, GnuPG (privacy guard), of EnigMail), want daarmee scherm je niet de afzender af. Ook gaat het verder dan het gebruiken van een email service die secure sockets layer (SSL) encryptie gebruikt. Dat is de basis encryptie die op het web wordt gebruik om meekijken te voorkomen, zoals wanneer je aan het internetbankieren bent. Je weet dat deze beveiliging wordt gebruikt als er HTTPS in de URL staat, in plaats van http, of als je een slotje ziet staan in de adres of statusbalk. De drie grote webmailproviders (Gmail, Yahoo Mail en Outlook.com) ondersteunen HTTPS. (neem de HTTPS Everywhere extensie voor Firefox, Chrome, Opera of voor Android om ervoor te zorgen dat dit protocol standaard wordt gebruikt, mits aanwezig) .

Ook een pseudoniem als email (bijvoorbeeld anoniemepony12345@gmail.com) is zeker niet genoeg. Een keer inloggen, je IP adres wordt opgeslagen en dat kan genoeg zijn om je te traceren. Zo werd CIA directeur Petraeus in ieder geval destijds gesnapt.

Dit is wat je moet doen om een e-mailadres te creëren dat compleet naamloos en niet te identificeren is. Maar, beloof ons dat je na het lezen van dit artikel je verworven krachten alleen gebruikt om goed te doen!

STAP 1: BROWSE ANONIEM

Je wordt gevolgd door je webbrowser. Zo simpel is het. Cookies, en nu de niet te stoppen super cookies weten waar je geweest bent, wat je hebt gedaan, en dat willen ze maar al te graag delen. Tuurlijk, het gaat er allemaal om dat je gerichte advertenties ontvangt, maar het is geen lekker idee voor diegene die graag privé surft. De kunsten van je browsers incognito/privé modus zijn maar beperkt; sites registreren nog steeds je IP adres bijvoorbeeld.

Als je echt privé op het web wil browsen (en in die tijd een ditto emailaccount wil aanmaken), heb je de Tor Browser nodig, een Mozilla-based browser, beladen met veiligheidsmaatregelen van het Tor Project.

Als je Tor niet kent: Het werd vroeger de Onion Router genoemd, en draait er om je anonimiteit te garanderen. Dat doet het door al het verkeer dat je naar het internet stuurt door zoveel servers te laten springen, dat men aan de andere kant nooit kan weten waar jij je nou echt bevind. Met deze browser duurt het langer om een website te laden dan met Firfox of Chrome, maar dat is de prijs die je betaalt voor anonimiteit.

De Tor Browser is beschikbaar in 15 talen, voor Windows, Mac en Linux. Het is autonoom en draagbaar, wat betekend dat je het kan draaien vanaf een USB stick als je het niet wil installeren. En het is compleet gratis. Zelfs Facebook heeft een Tor-veilig adres om de locatie van haar gebruikers te beschermen en laat gebruikers toegang krijgen tot het sociale netwerk op plekken waar dat illegaal is of geblokkeerd, zoals China.

Krijg alleen niet de indruk dat Tor je 10000% anoniem houdt en beschermt. Vorig jaar gingen criminelen daar vanuit, en faalden. Maar, het is een stuk veiliger dan open surfen.

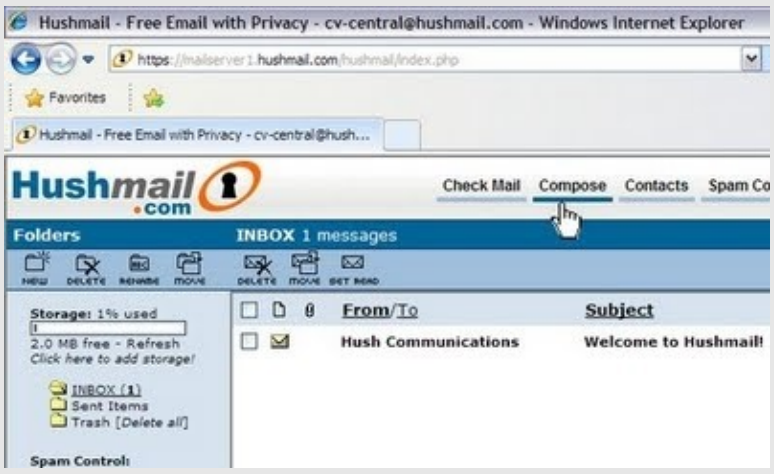
ANONIEME EMAIL

Je kan nu natuurlijk een relatief anoniem Gmail account aanmaken. Moet je alleen wel liegen als een bidprentje. Dat betekent een volledig Google account creëren, maar niet je echte naam gebruiken, liegen over je locatie, je verjaardag of wat je maar kan gebruiken om in te loggen (terwijl je de Tor browser gebruikt natuurlijk). Op een gegeven moment zal je Google moeten voorzien van een andere identificatiemethode, zoals een third-party emailadres of een telefoonnummer.

Voor de telefoon optie kun je een prepaid telefoon kopen, en wederom glashard liegen over je persoonlijke informatie, of een app als Burner of Hushed gebruiken.
Wat betreft de third-party email optie: er zijn anonieme email services die je kan gebruiken. Dus eigenlijk hoef je helemaal niet te leunen op Gmail, maar dat is even ter wille van het voorbeeld. Het punt is, nu je al zover bent is er geen reden meer om te stoppen. Gebruik een ècht anonieme web based email service om je berichten te versturen.

Bron: PCmag

Index



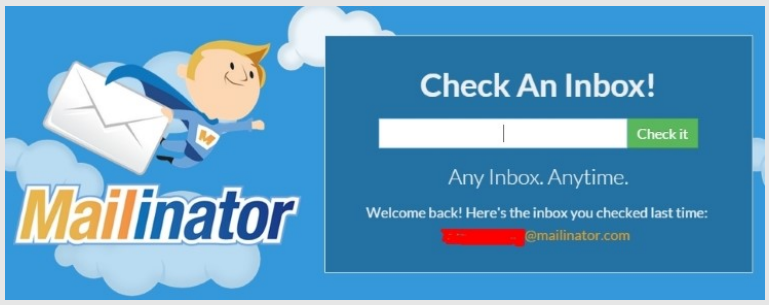
Hushmail baseert zijn bestaansrecht op eenvoud in gebruik, ontbreken van advertenties en ingebouwde encryptie tussen gebruikers. Om dat allemaal te kunnen gebruiken moet je natuurlijk wel betalen (vanaf 34,99 dollar per jaar voor 1 GB aan data). Er is ook een gratis versie met 25 MB opslag, maar dan moet je elke drie weken je inloggegevens verversen. Bedrijven kunnen Hushmail gebruiken voor 5,24 dollar per maand. En jij kan hem proberen met de gratis trial.

Een opmerking alleen: Hushmail heeft in het verleden wel eens gegevens aan de FED overgeleverd. In de terms of service staat ook duidelijk dat Hushmail niet gebruikt mag worden voor “illegale activiteiten”, dus ze zullen zich niet verzetten tegen digitale huiszoekingen. Maar daar zijn ze op voorhand in ieder geval wel eerlijk over.

Hide my ass is een breed gewaardeerd VPN network service die zijn gebruikers in staat stelt over content te beschikken die geblokkeerd wordt op hun locatie. Daarnaast bieden ze natuurlijk een stuk meer privacy; vandaar de naam. Vanaf 11.52 dollar per maand kun je van de service gebruik maken.

Als extraatje kun je gebruik maken van zijn Anonymous email service. In feite is die open voor iedereen, daar hoef je niet voor te betalen. Je krijgt dan een @hmamail.com adres die je kan instellen op een houdbaarheid van 24 uur, een week, een maand, een half jaar of een jaar. Er is een countdown klok die aangeeft hoe lang je je mail nog kan inzien. Wanneer je je inschrijft vraagt HMA om een bestaand e-mailadres zodat je een notificatie kan krijgen wanneer je een bericht op je anonieme account ontvangt, maar dit is niet verplicht. De interface wint alleen geen prijzen.

Guerrilla mail levert je een tijdelijk mailadres. Technisch gezien zal het adres voor altijd bestaan en nooit meer opnieuw worden gebruikt. Alle berichten die je ontvangt op dit adres zijn slechts een uur beschikbaar. Je krijgt een bizar e-mailadres dat je zult moeten kopiëren en plakken om te kunnen gebruiken. Je kan ook je eigen domeinnaam gebruiken, maar dat gaat je natuurlijk niet echt onder de radar houden. Guerilla mail is de perfecte manier om een e-mailadres te creëren om je in te schrijven voor een ander, meer permanent-maar-toch-anoniem e-mailadres, of om een snel, anoniem mailtje te sturen. Je kan zelfs bijlages versturen van maximaal 150MB. Gecombineerd met het gebruik van de Tor browser ben je zo goed als onzichtbaar.



Mailinator’s gratis wegwerp email heeft een strakke interface, maar die ga je waarschijnlijk niet eens nodig hebben. Wanneer je op het web gevraagd wordt om een e=mailadres, verzin je gewoon een naam met @mailinator daarachter. Vervolgens bezoek je de site, voer je diezelfde naam in en kun je kijken wat er naar dat adres is gestuurd. Er is alleen 1 probleem. Als iemand anders diezelfde naam verzint hebben jullie allebei toegang tot die inbox. Er zijn geen wachtwoorden, en je kan ook niks sturen. In de FAQ staat ook dat wanneer je een email ontvangt van mailinator, het een gegarandeerde scam is. Deze is voor de snelle service signups, en alleen te gebruiken met de meest obscure naam die je kan verzinnen.

Bron: PCmag

Index

Iedereen heeft recht op privacy. Sommigen denken die te kunnen verzekeren door allerlei privacygevoelige data op hun pc te verbergen. Hier verschillende methodes om gegevens af te schermen, maar ook forensische technieken die allerlei 'verborgen' informatie weten op te vissen.

Data verbergen op je eigen pc doe je zo

In dit artikel een hele reeks bekende en minder bekende technieken waarmee je je eigen data naar anderen toe kunt afschermen of verbergen. De focus ligt echter net zo zeer op technieken waarmee jij - of erger nog: iemand anders op jouw pc - dergelijke informatie alsnog kunt bovenhalen. Zulke operaties horen tot het domein van forensisch onderzoek. In principe houden alleen politie-instanties zich met dergelijke analyses bezig, denk aan de Groep Digitale Recherche van de KLPD in Nederland of de Federal Computer Crime Unit (FCCU) in België, maar niemand weerhoudt je om dergelijke technieken zelf uit te proberen.

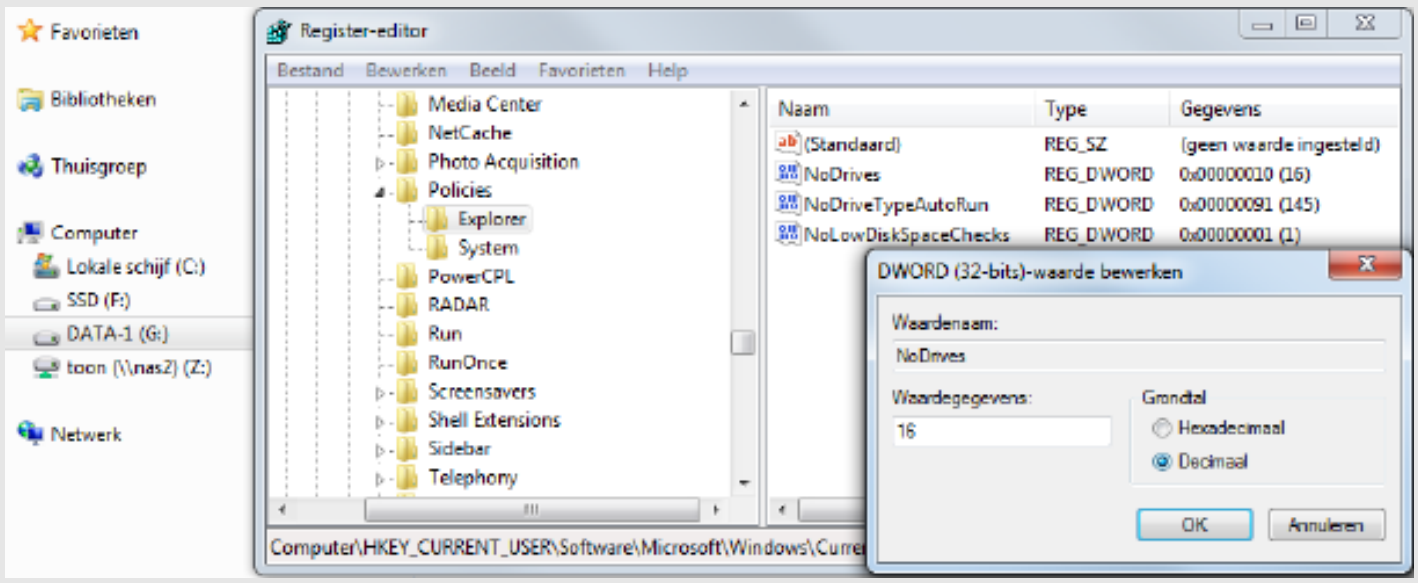
Uiteraard doe je dat uitsluitend op je eigen pc of op het systeem van iemand die je daartoe expliciet de toestemming heeft gegeven. In andere gevallen zijn zulke operaties wettelijk verboden en dus strafbaar. Dit soort onderzoek kan namelijk vanuit technisch oogpunt best wel leerzaam zijn en het laat je bovendien toe vergeten of verloren gewaande gegevens te herstellen. Enkele technieken uit het forensische domein zijn immers nauw verwant aan dat van dataherstel.

Profielmappen

Een van de meest voor de hand liggende en dus veelgebruikte methode om eigen data af te schermen zit stevig ingebakken in Windows: de profielmappen van een Windows-account met wachtwoord. De inhoud van deze mappen is in principe alleen zichtbaar voor wie zich met dat account aanmeldt, aangezien het ingebouwde ACL-beleid (Access Control Lists) uitsluitend toegang verleent aan de geautoriseerde gebruiker. Deze methode is echter lang niet waterdicht. Iemand hoeft zich alleen maar met een administrator-account aan te melden om deze beveiliging te omzeilen. Hij hoeft slechts naar jouw map te navigeren (C:\Users\), het contextmenu te openen en door met rechts te klikken te kiezen voor Eigenschappen \ Beveiliging \ Geavanceerd \ Eigenaar \ Bewerken (of Wijzigen) om de controle van je map aan zijn account toe te wijzen. Denk overigens niet dat je safe zit wanneer jij de enige administrator van dat systeem bent! In dat geval hoeft iemand het systeem slechts op te starten van een live bootmedium (bijvoorbeeld Ubuntu, samengesteld met behulp van de gratis tool YUMI en via de bestandsbrowser naar die map te navigeren. Aangezien Windows niet is opgestart, zijn de ACL-machtigingen langs deze weg niet langer geldig en liggen je data voor het grijpen.

Verborgen stations

Er zijn verschillende technieken waarmee je schijfstations aan het oog van de nietsvermoedende gebruiker onttrekt. Sommige tools, zoals Secret Disk (zie ook kader 'Security through obscurity'), maken daarbij gebruik van een virtuele schijf waarvan de bijhorende bestandsnaam niet-toegelaten tekens bevat, zodat Windows dat bestand niet te zien geeft. Je kunt echter ook zelf stations verbergen, bijvoorbeeld vanuit het Windows Schijfbeheer. Druk op Windows-toets+R en voer het commando diskmgmt.msc uit. Klik met de rechtermuisknop op het datavolume in het visuele overzicht, kies Stationsletter en paden wijzigen en druk vervolgens op Verwijderen. Of je regelt zo'n verdwijntruc via een registeringreep. Start Regedit op, navigeer naar HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer en creëer de DWORD-waarde NoDrives. Om het A:-station te verbergen, geef je die waarde het (decimale) getal 1 mee, voor B: vul je 2 in, voor C: 4, voor D: 8, enz. Met het getal 67108863 maak je alle stations in één keer onzichtbaar.



NoDrives met waarde 16: station E: is niet langer zichtbaar in Windows Verkenner.

Bron: Computer Totaal

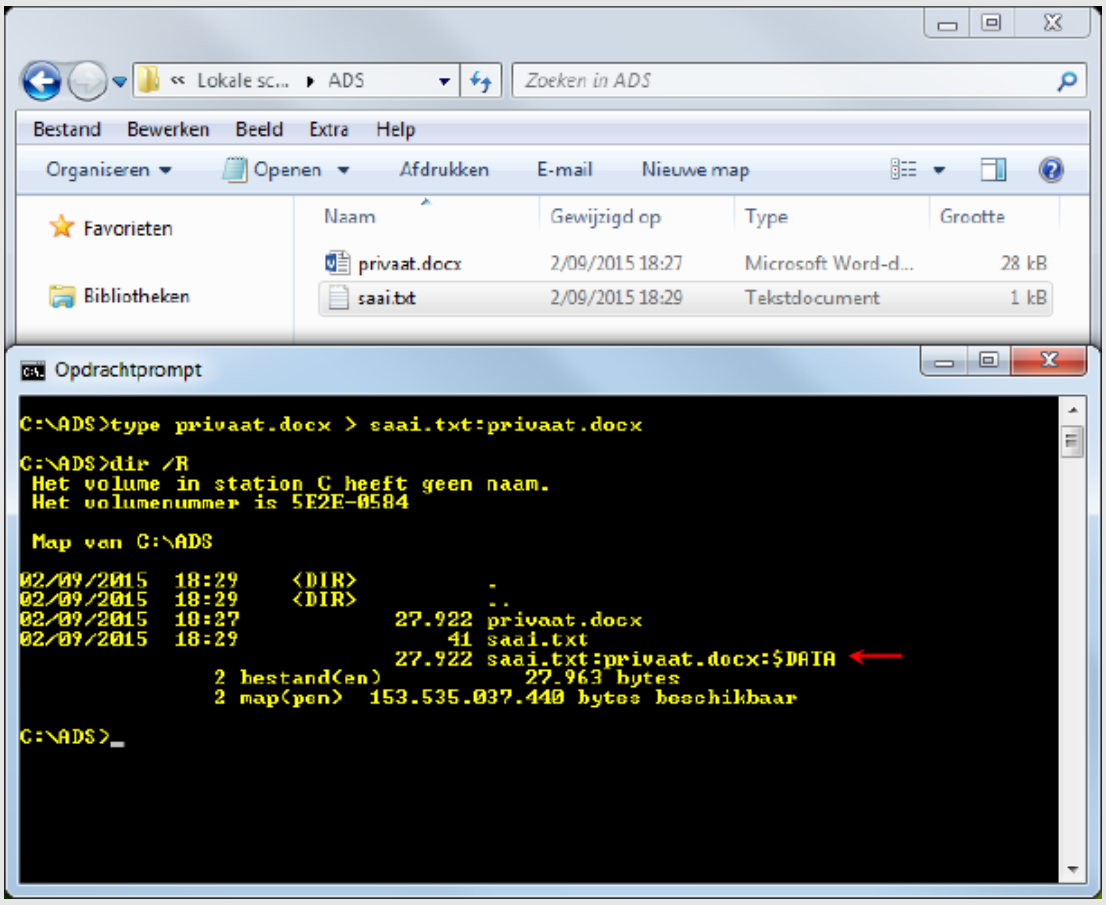
Index

Echter, deze verdwijntechnieken zijn snel genoeg ongedaan gemaakt. Het volstaat om je met een beheerdersaccount aan te melden en de procedure om te draaien. Of iemand start je systeem op met een live medium als Gparted om alsnog de aanwezigheid van zo'n verborgen volume te detecteren. En voor wie nog dieper wil graven: met een fysieke schijfeditor als het gratis Active@ Disk Editor (beschikbaar voor Windows en Linux) ontmasker je zo alle schijftrucjes en krijg je de data op zowat elke schijf netjes blootgelegd.

Alternate data streams

Elk besturingssysteem bedient zich van een of andere bestandsindeling om je data op een gestructureerde manier te bewaren, zodat ze naderhand altijd snel terug te vinden zijn. Bij Windows is dat op harde schijven standaard NTFS. Dit systeem heeft verschillende extra's die je niet terugvindt in een eenvoudiger systeem zoals FAT32. Een van de minder bekende extra's is de ondersteuning van de zogenoemde bestandsvorken, ook wel alternate data streams (ADS) genoemd. Het komt erop neer dat een bestand uit meerdere delen is opgebouwd: de eigenlijke gegevensvork en een of meer vorken met extra data.

Heb je bijvoorbeeld al gemerkt dat Windows je een uitvoerbaar bestand dat je van het internet hebt gedownload, niet laat installeren zonder een beveiligingswaarschuwing te geven? Ook deze informatie bevindt zich in een bestandsvork. Echter, ook andere software kan data verbergen in zo'n bestandsvork, zelfs malware, zoals de Trojaan Rustock. En wat software kan, kunnen gebruikers ook. Een klein experiment maakt dat duidelijk. Creëer eerst een willekeurig Word-document (privaat.docx) en een onschuldig tekstbestand (saai.txt). Ga daarna naar de opdrachtprompt en voer het volgende commando uit: type privaat.docx > saai.txt:privaat.docx. Het resultaat? Het Word-bestand wordt in een bestandsvork van het tekstbestand geplaatst, ook al is daar in Windows Verkenner (qua bestandsgrootte) niets van te merken. Het originele Word-document mag je nu zelfs verwijderen.



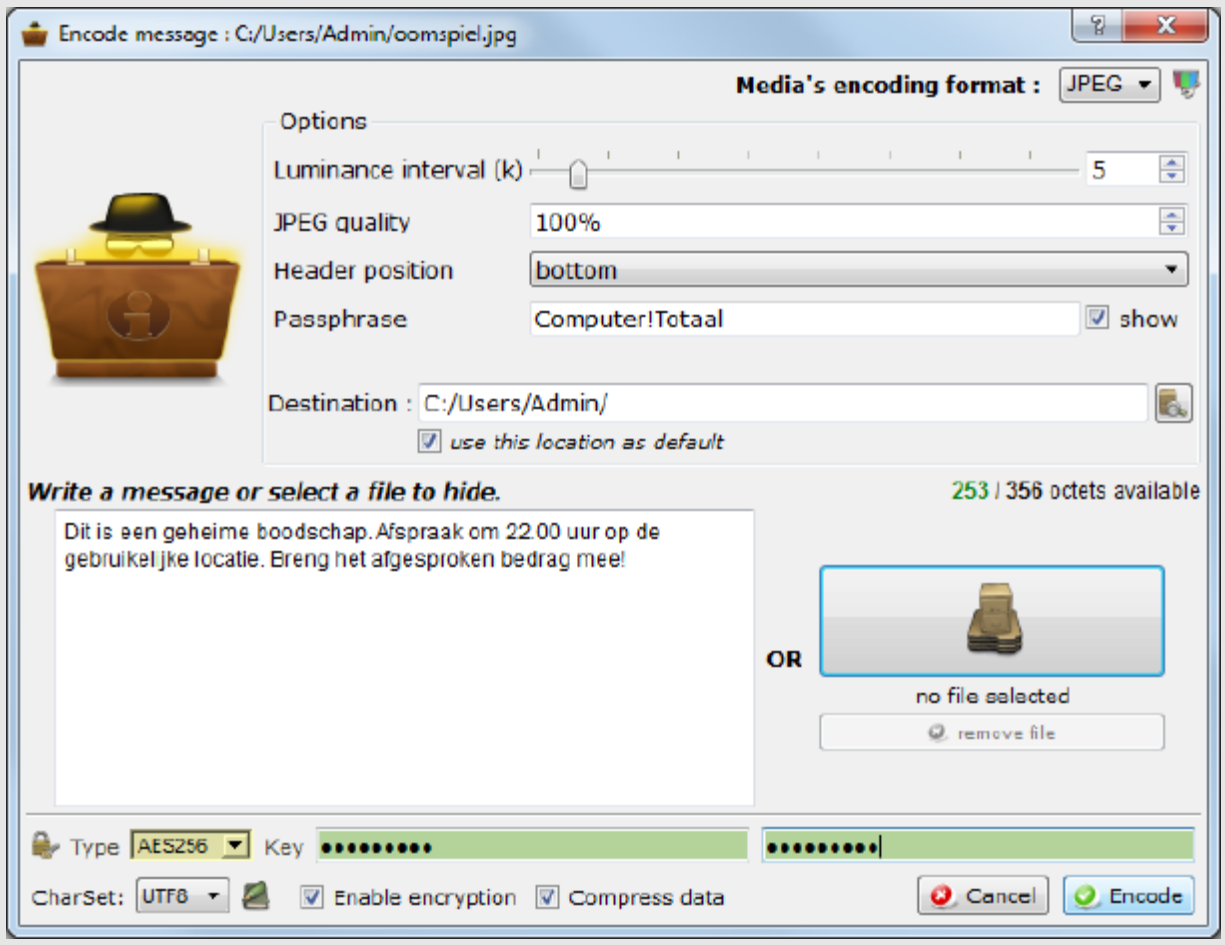
Met een eenvoudig commando hang je stiekem een document aan een ander onschuldig ogend bestand.

Het lijkt er wel op dat data die je op deze manier verbergt, grondig aan het oog is onttrokken. Dat is echter maar schijn, want sinds Windows Vista volstaat het opdrachtregelcommando DIR /R om alle ADS-data zichtbaar te maken, inclusief de grootte en de naam. Of beter nog, je installeert een gratis tool als AlternateStreamView. Wanneer je hier de gedetecteerde ADS met de rechtermuisknop aanklikt en de optie Geselecteerde streams exporteren naar selecteert, kun je de verborgen data netjes weer opslaan in een afzonderlijk bestand.

Steganografie

De ADS-methode kun je tot op zekere hoogte rekenen tot de steganografische technieken. Immers, steganografie is het verbergen van informatie in onschuldig ogende objecten. Heel vaak betekent dat het opnemen van een (geheim) bestand in een totaal ander bestand (de zogenoemde 'carrier' of drager) waarbij toevallige ontvangers geen flauw benul hebben van de verstopte inhoud. Gratis steganografische tools zijn bijvoorbeeld StegoStick en SilentEye. We bekijken SilentEye nader: deze tool draait onder Windows, OS X en Linux en ondersteunt onder meer bmp, jpg en wav als dragers.

Je selecteert eerst de drager, waarna je op de knop Encode drukt. Vervolgens tik je de boodschap in of voeg je het bestand toe dat je wilt verbergen. Zolang het getal in de regel ... octets available groen kleurt, kan de carrier de grootte van de boodschap of het bestand op een 'veilige' manier verwerken.

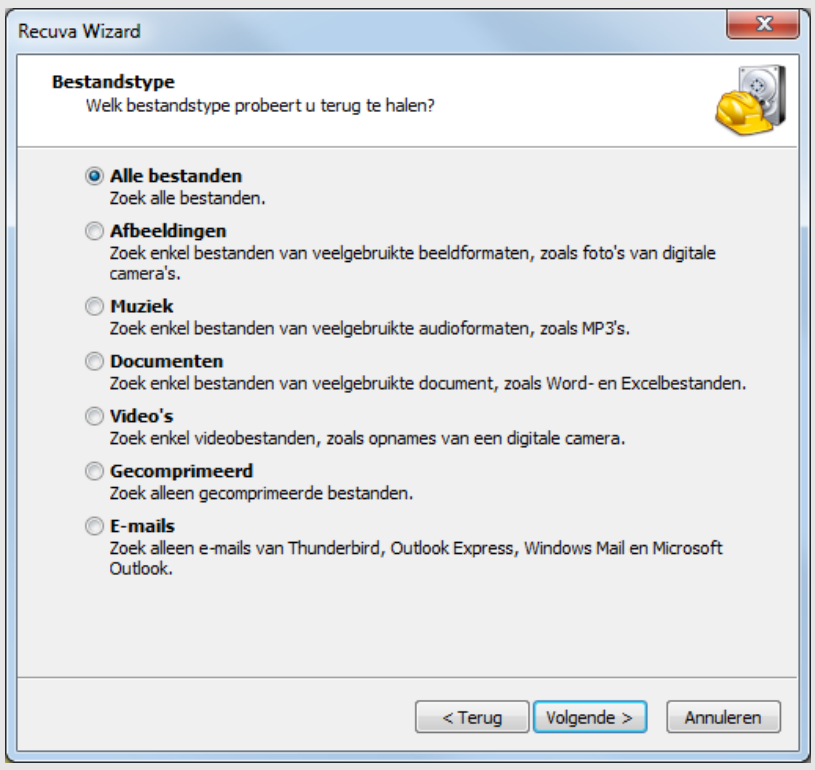


Steganografie: technologie met een zeker James Bond-gehalte.

Op zich is zo'n steganografische techniek wel veilig, althans zolang derde partijen niet weten dat het om een drager gaat en niet zomaar om een onschuldig mediabestand. Ervaren forensisch onderzoekers kunnen echter na grondige analyse van de bytepatronen van zo'n carrier wel vaststellen dat er extra gegevens verborgen zijn. Om die reden doe je er goed aan de data in de carrier niet zomaar te verstoppen, maar die eerst ook te versleutelen. Gelukkig biedt SilentEye zo'n mogelijkheid: zet een vinkje bij de optie Enable encryption, kies het gewenste algoritme (zoals AES256) en tik een goede encryptiesleutel (wachtwoord) in. De bedoelde ontvanger moet hiervan natuurlijk ook wel op de hoogte zijn. Hij hoeft dan maar de knop Decode in te drukken en het bijhorende wachtwoord in te vullen.

Verwijderde bestanden

Met een onderwerp als 'verwijderde bestanden' komen we vanzelfsprekend heel dicht in de buurt van dataherstel. Veel gebruikers zijn er nog altijd van overtuigd dat data effectief verdwenen zijn zodra ze die bijvoorbeeld in de prullenbak hebben gegooid en de prullenbak vervolgens hebben leeggemaakt. Niets is minder waar: zolang het vrijgegeven datagebied niet met andere data is overschreven, zijn die met de juiste tools of de nodige kennis nog terug te halen. Dat geldt overigens ook wanneer je een partitie opnieuw formatteert: ook deze gegevens zijn in principe nog te herstellen. Een degelijk en gratis programma waarmee je verloren gewaande bestanden kunt terughalen is bijvoorbeeld Recuva.



Het wizard-aangestuurde programma Recuva maakt het makkelijk om gewiste bestanden weer boven water te halen.

Bron: Computer Totaal

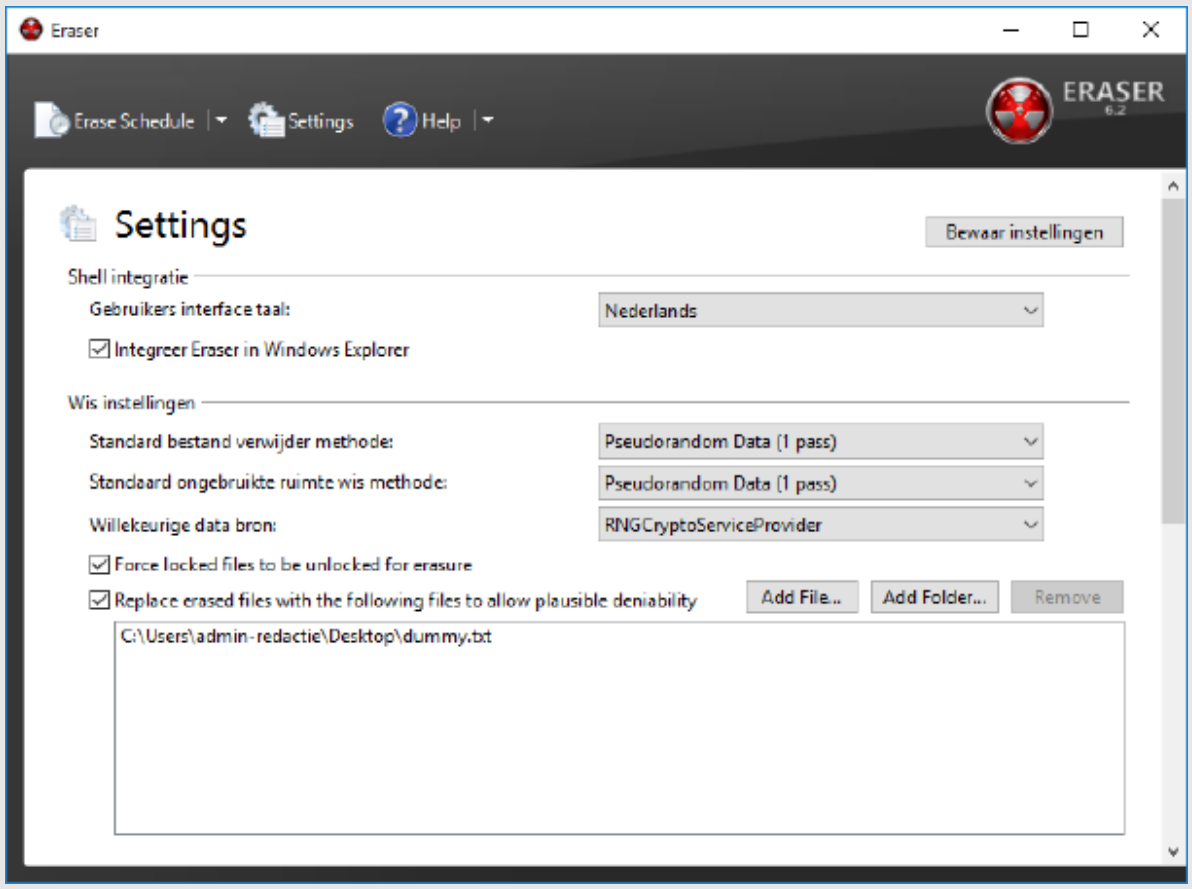
Index

Bestanden verwijderen geeft dus geen garantie dat die daadwerkelijk ook verdwenen zijn. Wil je (meer) zekerheid dat die gegevens effectief niet meer terug te halen zijn, dan moet je de data digitaal versnipperen: dusdanig overschrijven met een patroon van pseudo-willekeurige data dat de oorspronkelijke data onherstelbaar zijn. Een populair product waarmee je specifieke bestanden en mappen echt veilig kunt wissen, is Eraser. Gebruik overigens tijdens de installatie van Eraser de Custom-optie om te bepalen of je Eraser wilt integreren in je Windows Verkenner-menu's of om de Nederlandse vertaling aan te zetten. Een handige tool (geïnstalleerd op een live-medium) om complete partities en schijven te versnipperen is DBAN.

Snippersporen

Je moet niet uit het oog verliezen dat forensisch onderzoekers met behulp van een fysieke schijfeditor gemakkelijk kunnen aantonen dat bepaalde datagebieden 'versnipperd' zijn, precies omdat daar pseudo-willekeurige datapatronen terug te vinden zijn. Wil iemand plausibel kunnen ontkennen dat er versnippersoftware is gebruikt, voorziet Eraser in de mogelijkheid om die versnipperde schijfclusters naderhand met specifieke (dummy) bestanden te overschrijven.

Het is overigens een misvatting dat je datagebieden absoluut meerdere keren moet overschrijven om te vermijden dat er met gespecialiseerde apparatuur (zoals de NSA en dergelijke die ongetwijfeld bezitten) nog restmagnetisme van je oude data zou op te vissen zijn. Volgens specialisten is dat echter zo goed als onmogelijk gezien de extreem hoge datadensiteit op moderne schijven: er is gewoonweg te weinig ruimte tussen de sporen op zo'n schijf om dat te kunnen doen.



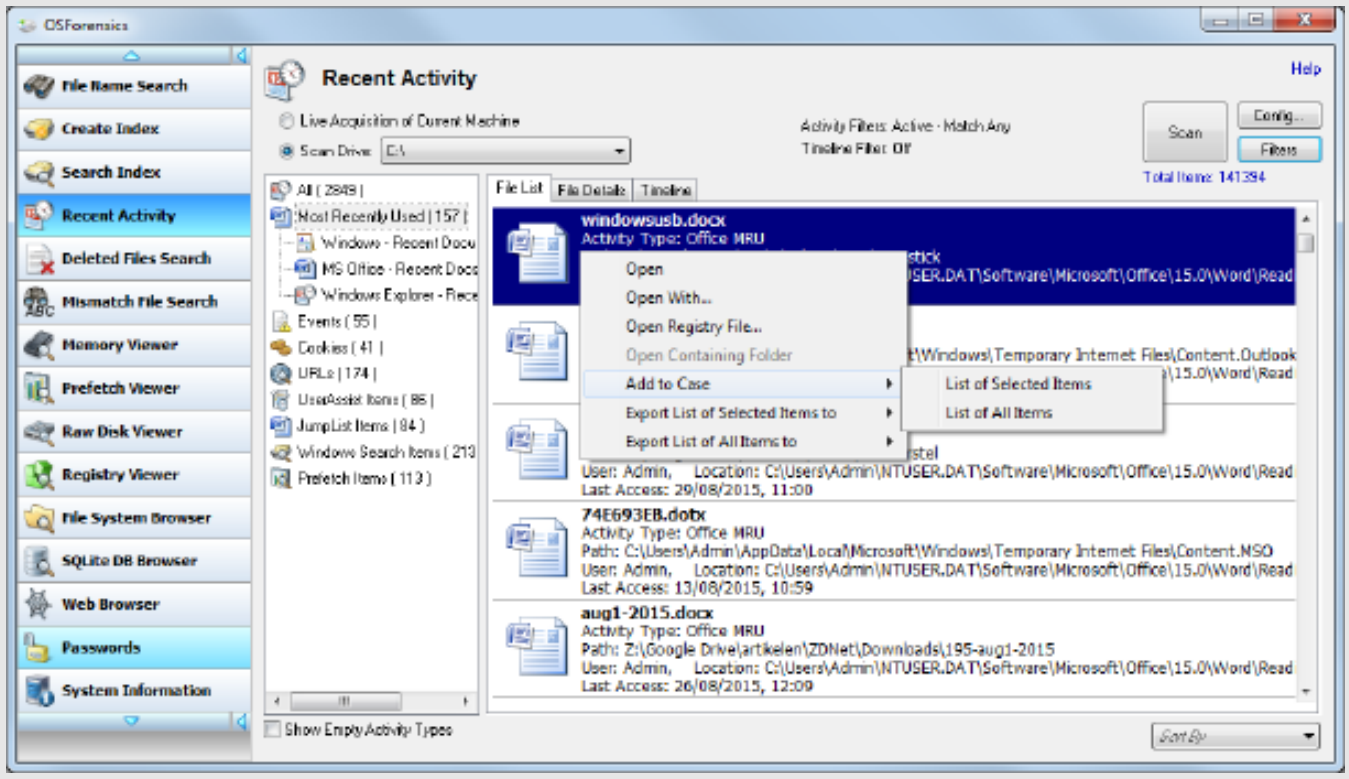
Bij het (standaard) versnipperen laat je 'sporen' na in de vorm van pseudo-willekeurige datapatronen. Dummy-bestanden kunnen dat maskeren.

Anderzijds moet je ervoor opletten dat je bij het grondig wissen juist geen datagebieden overslaat, zoals de zogenoemde 'slack' (letterlijk: overtollige ruimte). Dat is de ruimte tussen het einde van een datacluster (bijvoorbeeld een gebied van 8 sectoren van elk 512 MB) en het einde van een bestand dat in dat cluster is opgeslagen. Het valt namelijk niet uit te sluiten dat er in die ruimte nog gegevens van eerder gewiste bestanden staat die je wellicht ook graag verwijderd had gezien. Eraser kan echter ook deze slack-ruimte wissen: selecteer bij Target Type de optie Unused disk space en plaats een vinkje bij Erase cluster tips. Tijdens deze procedure worden alleen maar oude, reeds 'verwijderde' data gewist. Dat neemt niet weg dat vooraf een back-up maken een verstandige zet is.

OS Forensics

We hebben al heel wat technieken en locaties aan bod laten komen waarmee je data kunt verbergen (en vaak ook detecteren), maar er zijn vast nog wel gegevens waarvan je niet meteen had vermoed dat die op je computer te vinden waren of waarvan je in elk geval niet wilt dat iemand met toegang tot je pc die kan inkijken. Met een gratis tool als OSForensics krijg je daar meteen een aardig idee van. Dit forensisch programma heeft bijna dertig categorieën. Een van deze categorieën is Install to USB, waarmee je de tool ook onderweg in kunt zetten.

De meeste rubrieken zijn er echter op gericht telkens andersoortige gegevens bloot te leggen, die anders vaak lastig terug te vinden zijn. Er is bijvoorbeeld een reeks 'viewers' waarmee je het actuele geheugen van de pc kunt onderzoeken, of specifieke delen van het Windows-register, of de ruwe data op een harde schijf inclusief bootsectoren. Verder vist deze tool ook heel wat wachtwoorden van programma's en sites op en is het mogelijk zoekopdrachten uit te voeren op eerder verwijderde data. Of wat dacht je van de rubriek Recent activity die je in detail vertelt wat er zoal op de computer is gebeurd binnen een bepaald tijdsframe, zoals geopende documenten, gedownloade bestanden, gebruikte wachtwoorden en cookies. Het is overigens ook mogelijk een image van schijf te maken en die vervolgens ook weer in het programma in te laden voor nadere analyse. Zo'n image zorgt er namelijk voor dat je door je forensisch onderzoek niet ongewild wijzigingen aanbrengt op de onderzochte schijf, wat vooral voor officiële forensische analyses van belang is.



Het pc-gebruik dag aan dag blootgelegd door OSForensics.

Nog meer forensische tools

OSForensics is slechts één voorbeeld van een forensische tool die ook beginners vlot weten te hanteren. Er zijn er echter meer, zoals het eveneens gratis Win-UFO. Wanneer je bij het opstarten van deze portable tool de opdracht geeft meteen een rapport samen te stellen, krijg je na enige tijd een uitgebreid HTML-rapport te zien, met onder meer de namen van alle gebruikersaccounts, een overzicht van de actieve processen, alle geïnstalleerde programma's en hotfixes enzovoort.

Je kunt vanuit het hoofdvenster echter ook achter specifieke informatie aan gaan, met rubrieken als Browser History, Log Viewers en Password Recovery. Elk van deze rubrieken bevatten dan specifieke tools die (meestal) netjes in Win-UFO zijn geïntegreerd.

Een andere gratis forensische tool is het opensource Autopsy: een grafische schil rond de forensische softwarecollectie The Sleuth Kit. Deze tool installeert zich als een soort webserver die je vanuit je browser kunt benaderen, via poort 9999.

Win-UFO: talrijke rubrieken met telkens een reeks bijhorende tools.

Bron: Computer Totaal

Index

Hackersgroep Anonymous is zich sinds de aanslagen in Parijs op vrijdag 13 november meerdere keren in het nieuws gekomen. Zo verklaarde het collectief Islamitische Staat (IS) de oorlog in een videoboodschap en maakte het een lijst openbaar met gegevens van jihadi's. Wie zijn deze hackers en waarom verschijnen ze elke keer in het nieuws?

Vijf dingen die je moet weten over de Anonymous-hackers

1. Waar kennen we Anonymous van?

Anonymous is bekend geworden door een reeks databases die het hackerscollectief online zette en de DDoS-aanvallen die het uitvoerde. Anonymous verwierf in 2010 wereldwijde bekendheid toen de actiegroep het platleggen claimde van de website van het Zweedse Openbaar Ministerie. Het zou een wraakactie zijn geweest voor de arrestatie van WikiLeaks-oprichter Julian Assange.

Wat volgde was een reeks van aanvallen op banken, bedrijven en religieuze organisaties. Maar ook de website van pedofielenclub Martijn is doelwit geweest van hackers die opereerden onder de vlag van Anonymous. Na de recente aanslagen in Parijs verklaarde Anonymous IS de oorlog in een videoboodschap, maakte de groepsocial media-accounts van jihadi's openbaar en verving het collectief een propagandawebsite van IS door een advertentie voor een webshop met antidepressiva

2. Wie zijn Anonymous?

Omdat we te maken hebben met een anonieme groep, is het onmogelijk om te spreken van een organisatie: het is een groep hackers die zich uitgeeft onder één en dezelfde naam. Toch beweren experts dat Anonymous als groep bestaat in een los-vast verband, omdat er bijvoorbeeld een geverfieerd YouTube-account bestaat.

De hackers moeten anoniem opereren, omdat ze in bepaalde zaken vervolging riskeren. Internetdeskundige Brenno de Winter: ,,Want de rechercheteams zitten al jarenlang achter de groep aan. Ook zouden de hackers achter Anonymous bepaalde banden hebben met WikiLeaks. De veronderstelling is dat enkele gasten achter Anonymous zijn gelieerd aan WikiLeaks.''

3. Waarom komt Anonymous elke keer in het nieuws?

Volgens De Winter eisen de hackers bewust zaken op, die voor reuring zorgen in de maatschappij. ,,Ze hebben namelijk een aantal relevante hacks gepleegd.'' Wat dat betreft hanteren de hackers een heel mooie framing, zegt De Winter. ,,Ze zijn geen organisatie, maar roepen tegelijkertijd wél emoties op. De vaagheid is een deel van het mysterie: het is een vage, ondoordringbare club.''

4. Wat heeft Anonymous bereikt?

Met het vervangen van een propagandawebsite van IS door een advertentie voor een webshop die antidepressiva aanbiedt, zorgt Anonymous in ieder geval voor humor, beweert De Winter. ,,Slik een pilletje en de wereld ziet er meteen een stuk beter uit.'' Daar ligt wellicht ook de kracht van de groep hackers: de angst in de maatschappij ondermijnen en een glimlach toveren op de gezichten van mensen. ,,Zo'n hack met pilletjes Prozac is bijzonder nuttig.''

Maar dient Anonymous een maatschappelijk doel? De Winter denkt van niet. ,,Als Anonymous terreurnetwerken in kaart zou brengen, zou het collectief heel nuttig zijn. Dat gebeurt echter niet.'' Hij vindt het handelen van de hackers juist gevaarlijk, omdat ze dwars door onderzoeken van bijvoorbeeld inlichtingendiensten heen lopen en daarmee de nationale veiligheid in gevaar brengen. ,,Het recht in eigen hand nemen hoort niet bij een rechtsstaat.''

Het handelen van Anonymous geeft ook veel onrust, zegt De Winter. ,,Ze houden zich bezig met heel complexe materie. Die lijst met gegevens van jihadi's bijvoorbeeld: je kunt je afvragen of het publiceren daarvan wel zo effectief is. Zo'n lijst maakt het voor inlichtingendiensten moeilijk te bepalen wie daadwerkelijk gevaarlijk is en wie niet.'' Volgens De Winter ontneemt zo'n lijst inlichtingendiensten de ruimte om hun werk goed te doen.

5. Wat is de toekomst van Anonymous?

,,Het is ingewikkeld om aan te geven hoe de toekomst van Anonymous eruit ziet'', stelt De Winter. Wel is hij ervan overtuigd dat er een steeds belangrijker wordende taak is weggelegd voor hackers in het algemeen. ,,Ze zijn inmiddels in onze informatiesamenleving onmisbaar.'' Volgens de internetdeskundige kan hacken een goed doel dienen, maar is het tegelijkertijd moeilijk voor hackers om de consequenties van hun handelen te overzien.

Bron: Volkskrant

Index

Anonymous voert oorlog tegen de terroristen van Daesh. In de hoop zoveel mogelijk jihadisten van het net te verwijderen, leert Anonymous jou hoe je kan helpen.

Zo hack je een terrorist

Anonymous maakt jacht op de leden van Daesh en dat zullen ze geweten hebben. Even voor de duidelijkheid: Daesh is de naam die meer en meer mensen gebruiken om de legitimiteit van IS als 'staat' af te zwakken. Het terroristenkamp kan er niet mee lachen, evenmin kunnen ze zich vinden in de acties de hacktivistengroep Anonymous momenteel uitvoert.

Sinds de aanslagen in Parijs wist de anonieme hackersgroepering maar liefst 5500 jihadisten van het internet te verwijderen. Een groot deel hiervan in de vorm van Twitter-accounts. De eerste reactie van Daesh was om de hacktivisten 'kinderlijke idioten' te noemen. Ondertussen hebben enkele leden van Anonymous een aantal gidsen online gezet die beginners moeten helpen bij het hacken van potentiële terroristen.

Witter dan wit

Onder het motto "Daesh, witter dan wit" proberen ze zoveel mogelijk mensen te mobiliseren om het internet weer op te poetsen. Een eerste gids die gepubliceerd werd leert nieuwelingen Twitter-accounts hacken, een tweede leert hen hoe ze IS-accounts kunnen opsporen en een derde leert hen hoe ze websites van de organisaties kunnen vinden.

Wie iets van waarde heeft gevonden, wordt uitgenodigd om het te delen op het forum. Daarnaast verschijnen er geregeld websites die tools bevatten om dergelijke websites plat te leggen met behulp van DDoS- en MITM-aanvallen.

Niet zo diep

Daesh zelf is ondertussen gevlucht naar het Deep Web, met behulp van de beruchte TOR-browser. De organisatie die Anonymous uitscheldt voor idioten, blijkt echter zelf niet al te slim te zijn. Zo bevatten de IS-websites momenteel vele beveiligingsgaten die ervoor zorgen dat gebruikersgegevens worden gespiegeld op de website aan de oppervlakte, waardoor hackers en veiligheidsdiensten alsnog vele gebruikers zouden kunnen identificeren.

Waar Anonymous historisch vooral digitaal ten strijde trok om internet (porno)censuur tegen te gaan of een of andere schofferende beweging zoals Scientology tegen de schenen te schoppen, richt het hackerscollectief zijn pijlen nu op terreurbeweging IS. Operation Paris is er op gericht leden van de terroristengroepering op te sporen en gisteren boekte Anonymous z'n eerste succes. 5.500 twitteraccounts van IS werden offline gehaald.

Critici vrezen echter dat Operation Paris het werk van de veiligheidsdiensten tegenwerkt. Die verkiezen misschien wel om terroristen live aan het werk te zien via sociale media. De repliek van Anonymous: "IS baseert zijn propaganda op het verspreiden van zijn acties via twitter en facebook. Met gewelddadige video's en beelden willen ze terreur verspreiden. Hun propaganda stoppen is een effectieve manier om IS te verzwakken."

Bron: ZDnet

Index

Terreurgroep IS heeft een online helpdesk waar iedereen terecht kan voor technische vragen wat betreft encryptie en andere secure communicatietactieken.

IS heeft 24-uur helpdesk voor online terreur

IS heeft de hulplijn in het afgelopen jaar opgericht en bouwt hem nu gestaag uit, ontdekte het Combating Terrorism Center (CTC), een onafhankelijke onderzoeksorganisatie van het Amerikaanse leger. Hij wordt bemand door een groep vrijwilligers en zeker zes technische experts. Hij is 24 uur per dag en 7 dagen per week bereikbaar. De techneuten lijken volgens het CTC universitair geschoolde informatici.

Jihadisten en aspirant-jihadisten kunnen er terecht met vragen over alles van het uploaden van IS-propagandafilmpjes op YouTube tot complexe technieken om ongezien met terroristen te communiceren. Versleutelde communicatie speelt daarbij een belangrijke rol. Hoe de helpdesk er precies uitziet - of het bijvoorbeeld een website is op het 'dark web' - heeft het CTC niet bekendgemaakt.

Net als bijvoorbeeld Al-Qaida verspreidt de groep al enige tijd handleidingen en trainingsmaterialen. Maar wie er in zijn eentje niet uitkomt, kan nu dus hulp op maat krijgen.

Daarmee weet IS de drempel volgens het CTC aanzienlijk te verlagen. Nieuwkomers hoeven geen andere jihadisten meer te kennen om zich bij de terreurgroep aan te sluiten. Het is overigens onduidelijk hoeveel IS-sympathisanten van de helpdesk gebruikmaken.

Serieuze klanten worden aan het werk gezet
Wie een paar keer contact heeft opgenomen met de helpdesk en serieus geïnteresseerd lijkt om zich bij IS aan te sluiten, wordt volgens het CTC doorverwezen naar hogergeplaatste IS-strijders. Zij kunnen de aspirant-jihadist helpen bij het rekruteren van anderen, maar bijvoorbeeld ook bij het financieren en beramen van een aanslag.

De helpdesk is slecht nieuws voor terreurbestrijders, stelt CTC-terreuranalist Aaron Brantly tegenover NBC News. Hij heeft als doel om (aspirant-)jihadisten al in een vroeg stadium aan het zicht te onttrekken. Zo lang jihadisten elkaar fysiek ontmoeten, met elkaar bellen of met elkaar communiceren op sociale media, kunnen ze afgeluisterd worden. De helpdesk zorgt ervoor dat ze al vroeg 'gaan communiceren via versleutelde één-op-één-gesprekken, en het is extreem moeilijk om daar toe door te dringen'.

De CIA wijst er al enige tijd op dat jihadstrijders zo vaardig worden met versleuteling dat inlichtingendiensten geen grip meer op hen kunnen krijgen. Een deel van hun communicatie is nu 'exceptioneel' goed beveiligd, merkte CIA-directeur John Brennan maandag al op.

Belgische inlichtingendienst spreekt geen Arabisch
Welke rol technisch vernuft en zware versleuteling hebben gespeeld bij het voorbereiden van de aanslagen in Parijs is niet bekend. In België, waar een deel van de vermoedelijke daders heeft gewoond, hebben de inlichtingendiensten in ieder geval problemen van een heel andere orde. Ze hebben 'nauwelijks tot geen' Arabischsprekenden in dienst, meldde De Morgen maandag.

"Dat is een gigantisch probleem", stelde burgemeester Hans Bonte van Vilvoorde in de Vlaamse krant. "Noem dit gerust een van de grootste uitdagingen van onze staatsveiligheid." Volgens minister Koen Geens heeft het er deels mee te maken dat de lat voor sollicitanten hoog ligt. "Die moeten eerst gescreend worden. Maar we maken er werk van."

Bron: ZD net

Index

Een Britse minister waarschuwt voor online dreigingen van IS. Er wordt daarom meer geïnvesteerd in inlichtingendiensten om potentiële 'cyberterroristen' in de gaten te houden. Hoe reëel is het dat de terreurgroep ook online iets gaat opblazen?

Hoe gevaarlijk is het Cyber Kalifaat?

Online aanslagen kunnen enorm veel impact hebben. Denk aan een aanval op de interne systemen van ziekenhuizen of vliegvelden. Precies voor die aanvallen waarschuwt George Osborne, de Britse minister van Financiën: "Laten we duidelijk zijn: IS gebruikt het internet al voor het verspreiden van propaganda, radicaliseren van moslims en het plannen van operaties. Ze zijn er echter nog niet in geslaagd om mensen te doden door vitale infrastructuren aan te vallen."

Hoe reëel zijn dergelijke online aanvallen van IS op belangrijke infrastructuren? Vier vragen over de online dreigingen van het zogeheten Cyber Kalifaat.

Hoe gebruikt IS het internet?
IS zet het internet op drie manieren in: het verspreiden van propaganda, radicaliseren van moslims en plannen van operaties. Propaganda wordt onder andere verspreid middels een eigen online magazine Dabiq (ook beschikbaar in het Engels en Frans), openbare Telegram-kanalen (zoals Khilafah News) en Twitter-profielen. Er is zelfs een online helpdesk voor jihadisten zijn die 24/7 beschikbaar is. Het radicaliseren van moslims en plannen van operaties is lastiger waar te nemen. IS gebruikt allerlei kanalen om met elkaar te communiceren, van de PlayStation 4 en Telegram tot allerlei andere kanalen. Daarnaast speelt 'offline communiceren' ook nog steeds een grote rol. De AIVD zegt de komende jaren juist veel te verwachten van human intelligence, waarbij spionnen infiltreren in de wereld van radicaliserende moslims. Communicatie tussen terroristen zou steeds vaker offline plaatsvinden.

Welke 'online aanslagen' heeft IS tot nu toe gepleegd?
IS heeft vooralsnog weinig online aanvallen van betekenis uitgevoerd. Het Cyber Kalifaat, de hackersdivisie van de terreurgroep, heeft meerdere keren lijsten vrijgegeven met inloggegevens en persoonlijke gegevens van (meestal willekeurige) Twitter-gebruikers. Dit gebeurde ook bij medewerkers van de CIA, FBI en het Amerikaanse leger. Deze lijsten bleken echter veel oude informatie te bevatten, waardoor het lijkt alsof IS informatie die is buitgemaakt bij hacks in het verleden als nieuwe hacks presenteert. Een geslaagde internetaanval lukte op de website, Facebook- pagina en zenders van de Franse televisiezender TV Monde. De aanval kwam na de aanslag op Charlie Hebdo, waarbij de hackers een foto plaatsten met de tekst 'Je suis IS' - een verwijzing naar de steunbetuiging 'Je suis Charlie'. De zenders gingen voor zelfs even op zwart. Na een korte tijd werden de zenders, website en Facebook-pagina weer hersteld.

Hoe reëel is de online dreiging van IS?
Volgens Pim Volkers, vicepresident van het Nederlandse beveiligingsbedrijf Fox-IT, zijn er op dit moment geen duidelijke aanwijzingen voor grootschalige jihadistische online aanvallen. "Maar dat betekent niet dat het niet kan gebeuren. Je ziet dat er tussen de Franse en Britse Syriëgangers ook hoogopgeleiden zitten, en er hoeft er maar één een achtergrond in IT te hebben. Als zo'n slim persoon al jaren bezig is met computers en hij toegang krijgt tot het kapitaal van IS, zou dat wel degelijk dreigingen kunnen opleveren." De vermeende leider van het Cyber Kalifaat, Junaid Hussein, is in augustus van dit jaar omgekomen.

De online aanvallen hoeven niet per se door IS te worden uitgevoerd. "Dat kan ook door een huurling worden gedaan", zo legt Volkers uit. "IS heeft enorm veel geld. Je ziet in het Oostblok soortgelijke situaties, waar hackers worden ingehuurd om online aanvallen uit te voeren. In veel gevallen houden dergelijke criminelen geen rekening met wie hen betaalt en voeren ze gewoon de opdracht uit. Als IS zich dan richt op vitale infrastructuren, zoals banken, kerncentrales en andere nutsbedrijven, dan kunnen ze vanuit Raqqa met een online aanval belangrijke onderdelen van de samenleving ontwrichten."

Bron: RTL-Z tech

Index

Terroristen van IS zouden de PlayStation 4 van Sony hebben gebruikt om te communiceren. Waarom gebruiken ze een console voor communicatie en is deze datastroom zo lastig om in de gaten te houden?

Daesh/IS en Playstation 4

Hoe communiceer je via de PlayStation 4?

De PlayStation 4 biedt twee verschillende manieren om te communiceren: via chat of spraak. Beide werken via het PlayStation Network, dat de consoles van Sony met elkaar in verbinding brengt. Je kunt als PlayStation-bezitter vrienden toevoegen op basis van hun gebruikersnaam of e-mailadres en hen berichten versturen. Dit werkt via de console met een eigen chatvenster of met de officiële app van PlayStation. Via de app is het ook mogelijk om te chatten met je smartphone of tablet.

Bij een zogeheten Party kun je andere PlayStation-vrienden uitnodigen om een groepsgesprek te starten. Bij de console wordt standaard een controller met een microfoon en oortje geleverd, waarmee gamers met elkaar kunnen communiceren. Deze vorm van communicatie vindt meestal plaats tijdens online gamen, waardoor je tijdens het spelen met teamgenoten kunt praten

Hoe is communicatie van het PlayStation Network beveiligd?

De communicatie binnen het PlayStation Network wordt versleuteld. Dit gebeurt bij heel veel communicatievormen, van telefoneren tot berichtjes versturen. Sony wil niet vertellen hoe de encryptie wordt ingezet, maar het is aannemelijk dat de communicatie tussen consoles en de servers van Sony wordt versleuteld. Bij deze vorm van encryptie kan Sony wel de communicatie inzien. "De encryptie van de communicatie via de PlayStation 4 is voor de inlichtingendiensten heel lastig te breken", aldus Jambon.

Het zou voor een inlichtingendienst mogelijk zijn om bij Sony een aanvraag in te dienen om informatie van een specifiek account op te vragen. Dit gebeurde ook bij de aanslag op Charlie Hebdo. De Franse autoriteiten kregen binnen 45 minuten de inhoud van twee e-mailinboxen van de e-maildiensten van Microsoft. Dit is in de meeste gevallen de standaard variant van informatie opvragen. Bij Sony zou je in zo'n geval de chatgeschiedenis kunnen opvragen.

Het is ook mogelijk om een tap te plaatsen op dergelijke communicatie. De inlichtingendienst moet dan nog wel de communicatiestroom ontsleutelen om de inhoud in te zien. Dit kan doordat Sony de sleutel geeft of door eigenhandig de encryptie te kraken.

Sony laat weten dat het altijd meewerkt met de autoriteiten zodra het een melding van verdachte activiteiten ontvangt. "De PlayStation 4 maakt het voor vrienden en gamers mogelijk om samen te spelen. Maar zoals bij alle moderne verbonden apparaten, kan het apparaat ook worden misbruikt", zo meldt Sony in een verklaring. Het Japanse bedrijf wil niet zeggen of het IS-activiteit heeft opgemerkt of dat het stappen gaat ondernemen om dergelijke praktijken aan te pakken.

Waarom is deze communicatie lastig in de gaten te houden?

Het is niet ongebruikelijk dat inlichtingendiensten de communicatie van verdachte gamers in de gaten houden. Uit gelekte documenten door Edward Snowden blijkt hoe de Amerikaanse en Britse geheime diensten online pc-games als World of Warcraft en Second Life infiltreren om achter communicatie van terroristen te komen. In dergelijke games kwamen terroristen samen om in een virtuele wereld voorbereidingen voor aanslagen te treffen. In de documenten wordt melding gemaakt dat het mogelijk was om de (spraak)communicatie tussen online gamers af te tappen en te kraken, maar deze informatie is inmiddels verouderd.

IS maakt volgens de Belgische minister van Binnenlandse Zaken Jan Jambon gebruik van een soortgelijke tactiek, alleen dan via PlayStation Network. De PlayStation-console wordt normaliter gebruikt om mee te gamen, terwijl geheime diensten veelal de kanalen in de gaten houden waarmee wordt gecommuniceerd. Denk aan WhatsApp, telefoongesprekken of e-mail. Door de console als communicatiemiddel in te zetten, hebben de terroristen van IS hun communicatiestromen kunnen maskeren als 'normale gamesessies'.

De PlayStation verbindt met de servers van Sony. Alle data, van het online gamen tot het communiceren met andere teamgenoten, gaat via deze datastroom. Het is voor een geheime dienst dus lastig in te zien wanneer er met vrienden een online game wordt gespeeld, en wanneer terroristen van IS tijdens het online gamen een aanslag voorbereiden.

Daarnaast werkt de PlayStation zonder telefoonnummer. Vaak worden de mobiele telefoons van doelwitten in de gaten gehouden, omdat de verdachten deze veelal bij zich hebben en gebruiken om te communiceren. Bij het in de gaten houden van een mobiele telefoon kunnen bijvoorbeeld ook de locatiegegevens worden buitgemaakt. Een PlayStation biedt op het eerste gezicht veel minder bruikbare informatie voor een geheime dienst. Het gebruik van de PlayStation 4 laat zien dat terroristen vaak creatieve manieren vinden om met elkaar te communiceren. Zo gebruikt IS naast de PlayStation naar verluidt ook een openbaar kanaal op de chat-app Telegram om met sympathisanten in Europa te communiceren. Dergelijke communicatievormen tonen aan dat IS op digitaal gebied niet achterloopt en naar nieuwe manieren blijft zoeken om onopgemerkt te communiceren.

Bron:

Index

Door de aanslagen in Parijs laait de discussie weer op over de invloed en de 'gevaren' van versleuteling. De terroristen zouden namelijk communiceren via kanalen die niet te volgen zijn door inlichtingendiensten. We maakten een overzicht van de discussie rondom encryptie, en de link met de aanslagen.

Discussie over encryptie laait op na aanslagen in Parijs

De PlayStation 4 als hét communicatiemiddel van Daesh/IS ?

Al snel na de aanslagen begonnen journalisten de eerste puzzelstukjes in te vullen, en één belangrijk puzzelstukje draaide om de PlayStation 4. De terroristen zouden de aanslag namelijk hebben beraamd via het PlayStation Network op de PlayStation 4. Door op die manier te communiceren konden ze niet worden afgeluisterd, zoals bleek uit het eerste bericht daarover op Forbes.

Later bleek dat wel mee te vallen. Forbes had een eerdere uitspraak van een minister verkeerd begrepen en plaatste nog een rectificatie, maar het nieuws ging al snel rond op sociale media onder de noemer 'te mooi om kapot te checken.'

“Er worden steeds meer methoden van encryptie toegepast op gewone apps en apparaten”

Vervolgens werd de 'onkraakbaarheid' van de PS4 onder de loep genomen. Communicatie via het PlayStation Network zou bijna niet te kraken zijn, want het zou gebruik maken van ingewikkelde versleuteling. Die uitspraak komt echter van een Belgische minister, niet bepaald de meest betrouwbare bron voor nieuws over cryptografie. Daarom worden de uitspraken over encryptie van het PlayStation Network in twijfel getrokken.

Zorgen om encryptie

Toch leidt de opkomst van meer encryptie wel degelijk tot zorg bij onder andere inlichtingendiensten.

Het gaat dan met name om apps als Telegram of Signal, speciale chat-apps die zichzelf onderscheiden vanwege de privacyvriendelijke features die erin zitten. Zo kun je met Telegram geheime gesprekken beginnen, en bij Signal zelfs alle chats standaard versleuteld.

Daarnaast richten ook 'gewone' apps zich steeds meer op veiligheid - een indirect gevolg van de NSA-onthullingen van Edward Snowden. Neem bijvoorbeeld WhatsApp (950 miljoen gebruikers), dat sinds vorig jaar eind-tot-eind-encryptie aanbiedt voor chats tussen Android-toestellen. Ook Apple's iMessage is eind-tot-eind versleuteld, en de harde schijf van een iPhone of iPad is beveiligd met encryptie. In Android 6 Marshmallow is die schijfversleuteling ook niet langer meer opt-in, maar opt-out. Dat betekent dat een telefoon alleen af te lezen is wanneer je de swipe- of pincode invoert - zelfs Apple en Google kunnen telefoons anders niet uitlezen.

De vraag is of encryptie wel echt een probleem is voor veiligheidsdiensten. Die hebben er weliswaar moeite mee om sommige communicatie uit te lezen, maar van de andere kant waren de aanslagplegers al wel bekend bij de autoriteiten. Het probleem is vaak niet dat terroristen niet te volgen zijn - het is gewoon moeilijk om daarop in te blijven spelen.

Vernuftige methodes

Inlichtingendiensten en politici zeggen nu dat de uitspraken van Snowden hebben bijgedragen aan het gebruik van encryptie onder jihadisten. Daarbij lijken ze te impliceren dat de jihadisten niet doorhadden dat ze afgeluisterd konden worden vóór de onthullingen (in juni 2013), maar dat is uiteraard niet waar.

Sterker nog, jihadisten en terroristen gebruiken al jaren vernuftige methodes om anoniem te blijven op internet. Al in 2013 bleek dat terroristen samenkwamen in de game World Of Warcraft of in Second Life om daar aanslagen te beramen. Niet dat WoW nou zo veilig was, maar het was één van de laatste plaatsen waar de veiligheidsdiensten onderzoek naar deden.

Uit een recent rapport kwam naar voren dat de strijders van IS gebruik maken van niet minder dan 120 verschillende vormen van communicatie. Die lopen uiteen van doodgewone telefoongesprekken met wegwerptelefoons en -simkaarten tot forums op het Onion-web die alleen met Tor te bereiken zijn.

“Inlichtingendiensten pleiten direct voor een verbod op encryptie.”

De internationale 'war on encryption'

In veel landen is de 'war on encryption' al langer aan de gang. Vooral in Engeland is versleuteling een belangrijk thema voor premier Cameron. Hij pleit er al jaren voor om versleuteling illegaal te maken in Groot-Brittannië. Die plannen gingen aanvankelijk zelfs zo ver dat apps als WhatsApp of Snapchat verboden zouden moeten worden in het land.

Bron: PCMweb

Index

Toen de Franse president Hollande zijn land toesprak, kort na de aanslagen in Parijs, nam hij geen enkele keer het woord IS, ISIS of een andere term in de mond die vaak gebruikt worden om de terreurbeweging aan te duiden. In plaats daarvan gebruikte hij het woord 'Daesh'. Waarom?

Waarom 'Daesh' in plaats van IS?

De naam van IS is een punt van discussie sinds de terreurbeweging het wereldnieuws domineert na de opmars van de beweging in Syrië en Irak. Eerst noemde de beweging zichzelf ISI, een afkorting van Islamitische Staat in Irak (in het Arabisch: Dawlat al-Iraq al-Islamiyyah), na het veroveren van gebieden in Irak. Daarvoor stond de beweging simpelweg bekend als de Iraakse tak van Al-Qaida.

Na het uitbreken van de Syrische burgeroorlog werd de groep ook actief in Syrië en plakte het 'Al-Sham' achter haar naam - een historische naam voor Syrië. Daarmee kreeg de beweging de naam ISIS - Islamitische Staat in Irak en (Groot-)Syrië.

Al-Sham refereert in sommige vertalingen alleen weer aan een groter gebied dan Syrië - namelijk de Levant - dat naast Syrië ook Libanon, een deel van Jordanië en Turkije, Israël en de Palestijnse gebieden beslaat. Daardoor werd de beweging ook geregeld ISIL genoemd, waarbij de 'L' staat voor Levant.

IS zelf heeft overigens altijd in het midden gelaten op welk territorium de beweging precies doelt met Al-Sham, aangezien de groep naar eigen zeggen niet denkt in contemporaine grenzen. Nadat de beweging vorig jaar juni een eigen kalifaat uitriep in de veroverde gebieden in Irak en Syrië noemt de terreurgroep zichzelf Islamitische Staat, oftewel IS.

In de loop der jaren zijn al die verschillende namen voor de terreurgroep door elkaar gaan lopen. Zo noemde premier Rutte de terreurgroep zaterdag tijdens een persconferentie na de aanslagen in Parijs nog ISIS. De Amerikaanse president Obama noemt de groep, samen met veel Amerikaanse media, consequent ISIL. Veel Nederlandse media, zoals de Volkskrant, NRC Handelsblad en de NOS gebruiken IS of Islamtische Staat.

En nu is er dus 'Daesh', gebruikt door de Franse president en recent ook door de Amerikaanse minister van Buitenlandse Zaken John Kerry tijdens de Syrië-top in Wenen.

Maar eigenlijk is ook die naam er altijd al wel geweest. Daesh is namelijk het Arabische acroniem voor 'al-Dawla al-Islamiya fi Iraq wal-Sham' (DAIISH). 'En dat is eigenlijk gewoon de oude naam van IS, wat neerkomt op Islamitische Staat in Irak en de Levant', zegt arabist Leo Kwarten.

“Als je er al niet de doodstraf voor krijgt, dan krijg je er zeker tientallen stokslagen voor.”

Waarom dan toch de naam Daesh gebruiken als naam voor de terreurgroep, als de feitelijke betekenis niet anders is vergeleken met andere namen voor IS? Op die vraag gaf de Franse minister van Buitenlandse Zaken Laurent Fabius in september vorig jaar al antwoord.

Hij pleitte voor Daesh en riep op te stoppen met het gebruik van de naam Islamitische Staat. Allereerst omdat 'dit een terroristische groep is, en geen staat', zei Fabius. Verder vervaagt het woord 'islamitisch' volgens Fabius de scheidslijn tussen de terreurgroep en de islam in het algemeen. Het woord Daesh zou voornamelijk in het Westen minder snel de associatie met de islam oproepen.

Daar komt bij dat IS de naam Daesh als een belediging zou zien. Dat bevestigt arabist Kwarten. 'Het is er een verboden woord. Als je er al niet de doodstraf voor krijgt, dan krijg je er zeker tientallen stokslagen voor. Ze zien zichzelf als een staat. Het woord Daesh suggereert dat ze een beweging zijn. Dat is een belediging.'

Ondertussen wordt de term Daesh steeds vaker gebruikt, voornamelijk door politici. Franse en Turkse politici gebruiken de naam al langer. In Nederland diende DENK-Kamerlid Tunahan Kuzu dit jaar een motie in om de beweging voortaan Daesh te noemen. Kuzu kreeg geen steun voor zijn motie.

In juni stuurden 120 leden van het Britse Lagerhuis, gesteund door de Britse premier David Cameron, de BBC een brief met het verzoek voortaan Daesh te gebruiken. De Britse omroep wees dat verzoek af, omdat daarmee de onpartijdigheid van de omroep in het geding zou komen. Cameron had er vooraf al weinig vertrouwen in de BBC naar Daesh te bewegen. 'Maar dan vind ik ISIL nog beter dan Islamitische Staat, want de beweging is voor mij niet islamitisch en ook geen staat', zei Cameron.

Bron: Trouw

Index

In de chaos die volgde op de aanvallen in Parijs was het voor veel families moeilijk te achterhalen of hun geliefde veilig was.

Facebooks Safety Check massaal gebruikt in Parijs

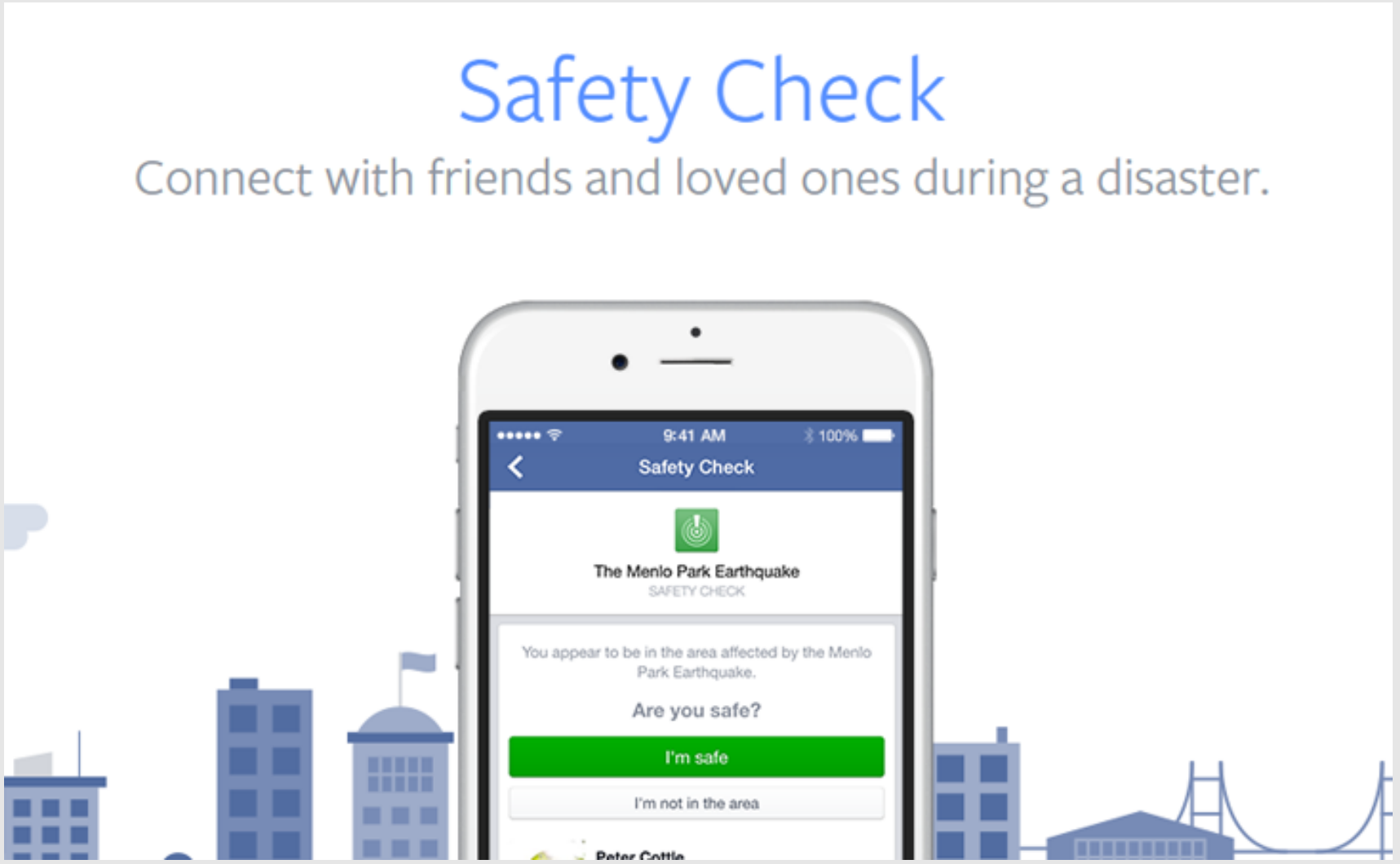
Na de aanvallen in Parijs besloot Facebook zijn Safety Check voor het eerst aan te zetten bij een gebeurtenis die geen natuurramp was. Meer dan 4 miljoen mensen maakten gebruik van de tool om familie en vrienden te laten weten dat ze veilig waren en maar liefst 360 miljoen gebruikers kregen de geruststellende notificaties. In de chaos die volgde op de aanslag, bood de tool op deze manier houvast voor veel ongeruste mensen, al kreeg Facebook ook kritiek op zijn beslissing om Safety Check in Parijs te gebruiken.

“We zijn erg verdrietig over wat er is gebeurd in Parijs, maar er is ook een hoofdstad die Beirut heet. Deze stad werd deze week aangevallen door terroristen. Waarom activeerde Facebook de Safety Check niet in Libanon, Mark Zuckerberg?” Schreef Wadih Constantine in een Facebookpost en ook andere Facebookgebruikers hadden soortgelijke bedenkingen.

Continu verbeteren

Safety Check werd vooralsnog echter slechts een aantal keer gebruikt en dit telkens bij natuurrampen. De tool wordt dan ook nog steeds bijgeschaafd en Facebook hoopt Safety Check in de toekomst bij meer tragische gebeurtenissen te kunnen inzetten. “In het geval van natuurrampen gebruiken we een aantal criteria, waaronder de schaal en impact. Tijdens een lopende crisis, zoals een oorlog of epidemie, is Safety Check in zijn huidige vorm niet bruikbaar. Er is namelijk geen duidelijk start- en eindpunt, waardoor het jammer genoeg onmogelijk te bepalen is wanneer iemand daadwerkelijk veilig is,” schreef Alex Schultz van Facebook.

“We besloten om Safety Check in Parijs te activeren, nadat we erg veel activiteit op Facebook zagen tijdens de gebeurtenissen. Dit was de eerste keer dat Safety Check werd geactiveerd voor iets anders dan een natuurramp. Er moet een eerste keer zijn voor alles en voor ons was dit Parijs,” besluit Schultz.



Bron: ZDnet

Index

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

Schatkist

Naslag:

- Handleiding Twitter
- Gebruik tweetraps authenticatie
- Windows 10 installatie
- Online verdwijnen
- Centraal cloudbeheer
- Online kopen
- Cybersecurity 2015
- Stickware
- Netwerk in de knoop

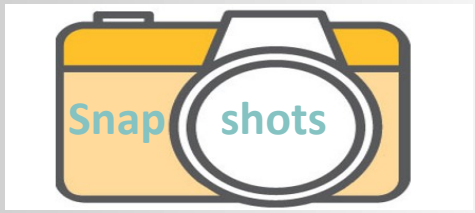
Software:

- 360 Total Security
- AS SSD benchmark
- Cdex
- Cleanmaster
- CPU-Z
- Emsisift Emergency Kit
- KillDiskSuite
- Mp3Gain
- MultiCommander
- SyneiSystemUtilities

Bonus:

- DoubleYouAB— Faithless Insomnia rmx
- DoubleYouAB— ReeAnna 2015 rmx
- DoubleYouAB— Summer Hardstyle 2015
- DoubleYouAB— 1.11 Armin rmx
- DoubleYoyAB— FedeLeGrandMix
- DoubleYouAb— Return to Tubular Bells
- DoubleYouAB— TrancePhonic 2015
- DoubleYouAB— Summermix 2015

Index



Van alle Nederlanders is 52% bezorgd over de veiligheid die ze online hebben. Volgens het CBS passen mensen vooral op met wat ze op sociale media plaatsen: vier op de tien doet dit soms niet, uit angst dat er wat mee gebeurt. Een op de vijf zegt wel eens iets niet gedownload te hebben uit angst voor virussen en dergelijke, een op de zes is bang voor internetbankieren. Het aantal daadwerkelijke incidenten is echter veel langer: slechts acht procent zegt wel eens iets vervelends te hebben meegemaakt. De meeste zorgen zijn er bij mensen tussen 25 en 65 jaar, ook al zijn zij niet vaker slachtoffer.

———————————————————

Bij verzekeraar Delta Lloyd is al sinds 2013 een speciaal team bezig met het terugvinden van gestolen spullen, schrijft de Automatiseringsgids. Daarvoor wordt sinds kort het systeem Sjerlok gebruikt, dat in geval van diefstal of vermissing online zoekt naar die objecten. Sjerlok koppelt de gevonden informatie aan de claim, monitort het dossier en communiceert automatisch met derden, zoals politie en onderzoekbureaus.

———————————————————

Onder druk wordt alles vloeibaar. Waar sociale media als Facebook, Twitter en YouTube lang geroepen hebben dat het niet hun taak is om racistische berichten van internet te verwijderen, lijken ze nu bereid om méér verantwoordelijkheid te nemen. Overleg tussen de bedrijven en minister Lodewijk Asscher (Sociale Zaken) heeft onder meer opgeleverd dat er een directe lijn komt tussen deze bedrijven en het Meldpunt Internet Discriminatie (MiND). De bedrijven gaan behalve MiND ook andere maatschappelijke organisaties helpen om ‘een stevig tegengeluid te ontwikkelen tegen racisme’, zoals in veel andere EU-landen ook al gebeurt.

———————————————————

De rechtbank in Groningen heeft een man (62, uit Emmen)veroordeeld tot één dag celstraf en 120 uur werkstraf voor het bezit van kinderporno. De man had in totaal 144 bestanden opgeslagen in SkyDrive, de clouddienst van Microsoft. Dat bleek minder veilig dan de man had gedacht: Microsoft ontdekte met de speciale software PhotoDNA de bestanden en meldde dit bij de politie. Bij huiszoeking werd op verschillende computers kinderporno aangetroffen. De man werd tien jaar geleden ook al veroordeeld voor kinderporno. Hij moet daarom nu ook toestaan dat de politie zijn computers onaangekondigd mag controleren.

———————————————————

De ándere kant van de vluchtelingendiscussies op facebook …EenVandaag meldt dat vluchtelingen uit Syrië en Irak fanatiek op sociale media zoeken naar oorlogsmisdadigers die naar Europa proberen te vluchten. De groep verspreidt foto’s van mensen die actief meededen aan de oorlog in Syrië, inclusief de locaties waar ze nu zouden verblijven. Al was het maar om te voorkomen dat vluchtelingen die zijn gemarteld, hun martelaars tegenkomen in een azc. In veel azc’s in Nederland en omringende landen zouden oorlogsmisdadigers te vinden zijn, soldaten en milities die streden voor president Assad. In het programma vertelt Syriër Salem Kurdi over de online speurtocht. ‘Eigenlijk zijn die oorlogsmisdadigers heel dom. Ze hebben jarenlang foto’s van zichzelf op facebook gezet, omdat ze zich veilig voelden’. Kurdi zegt alles op alles te zetten om de identiteit van deze mannen te openbaren. IND-directeur Rob van Lint is blij met alle informatie. ‘Nederland mag geen vluchthaven voor oorlogsmisdadigers worden’.

———————————————————

Gisteren nog in de inbox: waarom we onze waardebon van vijfhonderd euro bij de Zeeman nog niet ingewisseld hebben. De Consumentenbond heeft onlangs weer gewaarschuwd voor de hausse aan berichten waarin de ontvanger een waardebon of dagkaart wint. ‘Gratis met de NS’ of ‘Voor 500 euro winkelen bij Ikea’ beloven de afzenders die via facebook, WhatsApp of e-mail hun slag proberen et slaan. De nepprijsvragen zijn volgens de bond afkomstig van bedrijven in Curaçao (VOC Global) en Bulgarije (Mons Management). Wie reageert of meedoet, loopt het risico een duur abonnement af te sluiten, een duur 0909-nummer te moeten bellen of anderzins opgelicht te worden. Zo leidt de NS-dagkaartaanbieding naar een loterij van 12 euro per week en moeten winnaars van de Ikea-prijsvraag telefonisch maar liefst tweehonderd vragen beantwoorden.

———————————————————

Een botnet uitschakelen is één ding maar cybercrime houdt pas echt op als er arrestaties zijn. Beveiliger Trend Micro zegt dat naar aanleiding van het platleggen van het Dridex-botnet, door FBI, NCA en Europol. Het botnet, opgezet om geld van online bankrekeningen te stelen, is echter nog steeds actief omdat niet alle servers uitgeschakeld zijn. Er is slechts één persoon opgepakt, een systeembeheerder. Anderen gaat nog gewoon door. Voor Trend Micro reden om te pleiten voor meer actie. Dit soort acties ‘zorgen ervoor dat de minst effectieve dreigingen worden verwijderd en cybercriminelen van hun fouten kunnen leren. Arrestaties zijn dan ook nodig om echt een einde aan cybercrime te maken’.

———————————————————

Gebruikers met een iPhone of iPad die gesteld zijn op hun privacy, kunnen de spraakassistent Siri beter uitzetten als ze hem toch niet gebruiken. Experts van Trend Micro stellen namelijk dat iemand op een iPhone of iPad waarop Siri is geactiveerd, binnen 30 seconden achter de volledige naam, e-mail, telefoonnummer en een profielfoto kan komen. Het maakt daarbij niet uit of het toestel geblokkeerd is.

Gegevens

Wie een toestel in handen heeft, kan met zijn stem allerlei gegevens opvragen, zoals de naam, contactgegevens en zelfs afspraken in de agenda. Door het commando ‘what is my name’ uit te spreken bijvoorbeeld, dreunt Siri de volledige naam van de eigenaar op. En zo zijn er nog een aantal opdrachten die Siri uitvoert, zelfs als de smartphone of tablet geblokkeerd is.

Privacy

Het is volgens Trend Micro een zwak punt van Siri waar gebruikers al langer over klagen op internetfora. Volgens Trend Micro zijn niet alleen de privacy van de bezitter van de iPhone of iPad in het geding, maar ook de contacten van die persoon.

Apple laat in een reactie aan het beveiligingsbedrijf weten dat gebruikers Siri wel kunnen uitschakelen op het geblokkeerde scherm. Dit kan via het Instellingenmenu en dan via de optie ‘Touch ID & wachtwoord’ en vervolgens ‘Siri’. Daar kan de persoonlijke assistant worden uitgeschakeld.

———————————————————

Index

Twitteraccounts, een facebookpagina, een YouTube kanaal en een bodycam – de politie Amsterdam gaat met haar tijd mee. ‘Mensen zeggen niet voor niks: de digitale wereld’, zegt hoofdagent Niels uit het team Overtoomse Sluis. ‘We willen kijken hoe we op dat soort vlakken ook ons gezicht kunnen laten zien’. Niels sprak naar aanleiding van het boek van Albert Meijer cs. Meijer, hoogleraar Publieke Innovatie, ziet ‘heel veel enthousiaste agenten’ op sociale media. ‘Ook het beleid van de politie is er steeds meer op gericht dat het een goed idee is om sociale media te gaan gebruiken’. De aanwezigheid op sociale media zorgt ‘in de regel’ voor een imagoverbetering en kan bijdragen aan het vertrouwen in de politie.

———————————————————

Burgeropsporing in Zeeland: de facebookpagina’s van Emté-supermarkten in Vlissingen en Koudekerke bevatten ‘meer winkeldieven dan aanbiedingen’. De zaken werden herhaaldelijk bezocht door winkeldieven en volgens eigenaar Kees Vader is de maat vol. Dat je dan als winkeldief herkenbaar op facebook komt, is ‘risico van het vak’. De foto’s worden massaal geliked en gedeeld, voorlopig zonder succes. Volgens Vader zijn de dieven geen amateurs en ook in andere plaatsen actief. De politie zegt de actie ‘niet handig’ te vinden maar dat het ook niet verboden is.

———————————————————

Ook al zijn er richtlijnen die geweld tegen hulpverleners zwaarder bestraffen, de man die een agent op facebook onterecht beschuldigde van betrokkenheid bij de dood van arrestant Mitch Henriquez, is
evengoed vrijgesproken. Tegen verdachte Michael van der K. (27) was achttien maanden celstraf geëist, waarvan acht voorwaardelijk, omdat hij een foto van een wijkagent op facebook plaatste, zogenaamd de moordenaar van Henriquez. De foto werd ruim 8500 keer gedeeld en voorzien van commentaren als moordenaar, leugenaar en racist. De officier van justitie vond dat de berichten op facebook ‘de grenzen van de vrijheid van meningsuiting duidelijk overschreden’ en dat ‘wel degelijk suggesties [zijn] gewekt die een geweldsexplosie kunnen veroorzaken’. Maar de rechtbank in Den Haag vond dat er geen sprake was van opruiing. Verdachte ‘Kras’ had weliswaar de foto geplaatst maar niet opgeroepen tot strafbare feiten. Dat de agent werd bedreigd, wekenlang niet kon werken en ‘het plezier in zijn leven totaal verloren’ is, tja, daar kon de verdachte ook niks aan doen. Het was, zo zei hij in de rechtbank, nooit zijn bedoeling om haat te zaaien of om iemand te bedreigen. ‘Ik heb het gedaan omdat de emoties heel hoog opspeelden’. Van der K. werd wel veroordeeld – drie maanden onvoorwaardelijk – omdat hij stenen naar de ME gooide.

———————————————————

Claudia en Elroy zijn de twee gelukkigen die een ‘inkijkdienst’ mogen meemaken bij de politie Rotterdam-Charlois. Het team hield een facebookactie die een groot succes werd. Met een foto van vijf ‘knappe’ vrouwelijke agenten werd gevraagd wie er een dienstje wilde meedraaien. Bij 2500 likes zou de actie doorgaan. Dat aantal werd snel bereikt zodat een extra inkijkdienst is gepland.

———————————————————

Op internet en sociale
media circuleert momenteel een nepbericht over zwarte pieten die gevaarlijk snoepgoed zouden uitdelen. Opvallend is dat boven het bericht het logo van politie.nl staat; de politie zou adviseren om geen snoepgoed aan te nemen. Maar op Politie.nl is zo’n bericht helemaal niet te vinden, een woordvoerder spreekt daarom van een hoax. ‘Het bericht is niet van de politie‘. Van wie wel, is nog onduidelijk. De politie zegt dat mensen die twijfelen aan zulke mails altijd op de site kunnen kijken: als het bericht daar niet staat, ‘kan er worden uitgegaan van een nepmelding’.

———————————————————

De rol van facebook en andere sociale media in de wereld van mensensmokkelaars en vluchtelingen. Die smokkelaars blijken massaal op facebook actief, met advertenties en tips. ‘Toeristenjacht. Van Istanbul naar Griekenland. Twintig minuten’, staat er bijvoorbeeld onder een foto van een snelle boot. ‘Speciale prijs voor groepen’. Op de facebookpagina ‘Smokkel vanuit Turkije naar de meeste Europese landen’ wordt zelfs vervoer per jetski aangeboden. Tien minuten op zee, 2300 euro. De pagina’s zien er net zo gelikt uit als die van échte reisbureaus, compleet met slogans als ‘jullie veiligheid is ons motto’ en ‘jullie aankomst is ons doel’. Sommigen bieden zelfs kinderkorting: vervoer gratis voor 0-4 jarigen, half geld voor 12-minners. Sociale media blijken een steeds belangrijkere rol te spelen in de wereld van mensensmokkelaars, zegt Andrea di Nicola, een Italiaanse criminoloog die twee jaar lang onderzoek deed naar smokkelnetwerken. volgens Di Nicola wordt vooral facebook ‘ongelooflijk veel gebruikt’. Dat is ook logisch: ‘uiteindelijk zijn smokkelaars ook gewoon ondernemers’. Voorjaar 2015 vertelde een van de smokkelaars al aan de BBC dat zijn omzet tegenwoordig voor 40% via sociale media wordt behaald. Bang om gepakt te worden zijn ze niet, de smokkelaars. De meesten vermelden hun telefoonnummer, hun volledige naam, gedetailleerde prijsinformatie maar ook ervaringen van eerdere klanten. Bij Europol worden dergelijke sites continu gemonitord. Door twee gespecialiseerde teams, maar zonder veel succes. Het is vechten tegen de bierkaai, aldus een woordvoerder van Europol. ‘En de Turkse overheid zit ons ook niet echt op de hielen’, aldus een Syrische smokkelaar. ‘Ze pakken je alleen als ze je op heterdaad betrappen’. En dus post ook deze smokkelaar weer een bericht op facebook over zijn successen: filmpjes van vluchtelingen die in zijn bootjes de overkant hebben gehaald, foto’s waarop ze allemaal de duim omhoog steken. Wie het gehaald heeft, schrijft op de pagina’s weer recensies – net als bij Iens en Zoover. De smokkelaars letten ook op de seizoenen. Nu het weer slechter wordt, adverteren ze met regenkleding, poncho’s, taxi’s en zelfs huurappartementen in Athene.

———————————————————

Index

opgelet op internet.nl

Actuele phishingmails:

klik hier

Phishing- / valse e-mails melden

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

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

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

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

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

POLITIE Meldpunt internetoplichting

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

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

Antwoord

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

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

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

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

Cybercrime wetsartikelen

Wetsartikelen voor computercriminaliteit in enge zin

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

Voor cybercrime in enge zin zijn de volgende wetsartikelen beschikbaar:

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

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

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

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

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

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

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

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

————————————————————

Haatzaaien.

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

Haatzaaien staat niet als zodanig in het wetboek.

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

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

————————————————————

Cyberstalking.

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

Relevante wetsartikelen zijn:

Artikel 285b WvSr: belaging.

Artikel 138a WvSr: computervredebreuk.

Artikel 266 WvSr: belediging.

————————————————————

Grooming.

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

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

————————————————————

Handel in mensen of foute goederen.

Verschijningsvormen:

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

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

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

Relevante artikelen zijn:

Artikel 273a WvSr mensenhandel.

Artikel 416 WvSr opzetheling.

Artikel 417 WvSr opzetheling (gewoonte).

Artikel 274 WvSr slavenhandel.

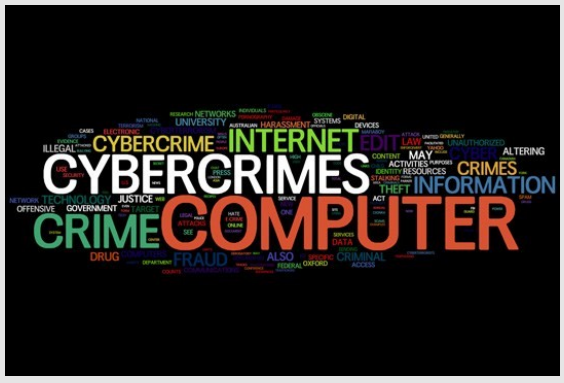
Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



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