

Mijn geeltjes ? Kijk op compubuy.jouwpagina.nl



Januari 2015

JAARGANG 4

Secure

Computing

In dit nummer oa:

Bouwmarkten mogen
beelden delen

Silkroad weer online

Spellingscontrole is
gevaarlijk

Privacy by design

E-books doorverko-
pen?



Veel lees(r)plezier

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



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:

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

[Opstellen: bouwmarkten mogen beelden met politie delen](#)

[Kun je e-books op legale wijze doorverkopen?](#)

[Zo bescherm je jouw identiteit bij een ID-kopietje](#)

[Thuisrouters: tikkende tijdbommetjes](#)

[Whatsapp nu ook voor op je desktop](#)

[Versleuteld synchroniseren](#)

[Pordroid gijzelt je smartphonebestanden](#)

[Silk Road weer online](#)

[Selfies gelinkt aan psychopathie en narcisme](#)

[Geavanceerde malware is haast niet tegen te houden](#)

[Je pc wordt vaker aangevallen dan ooit tevoren](#)

[Spellingscontrole is gevaarlijker dan je denkt](#)

[Expert waarschuwt voor overdrijven van cyberterrorisme](#)

[ENISA doet aanbevelingen voor privacy by design](#)

[Schatkist](#)

[Snapshots](#)

[Cops in Cyberspace](#)

[Handig](#)

[Wetsartikelen](#)

Opstelten: bouwmarkten mogen beelden met politie delen

Bouwmarkten die camerabeelden met de politie delen van klanten die verdacht gereedschap kopen overtreden hiermee niet de privacywetgeving, zo heeft minister Opstelten laten weten.



Verschillende bouwmarkten in Ede, Wageningen, Barneveld en Veenendaal zijn een project begonnen waarbij ze politie vrijwillig met camerabeelden laten meekijken. Het gaat dan om beelden van klanten die "verdacht" gereedschap aanschaffen, zoals grote schroevendraaiers, breekijzers en beitels. Volgens Opstelten zagen de deelnemende bouwmarkten het als hun "maatschappelijke verantwoordelijkheid" om de politie informatie te verschaffen over aankopen die naar hun inschatting verdacht zijn en mogelijk te maken hebben met de voorbereiding van een inbraak.

De bouwmarkten bepalen daarbij zelf welke voorvallen ze onder aandacht van de politie willen brengen naar aanleiding van verdacht gedrag of verdachte interesse voor onlogische combinaties van gereedschap, merkt Opstelten op. "Zo blijkt uit ervaringen van de bouwmarkten onder meer dat de grootste exemplaren voorhamers slechts enkele keren per jaar bij een vestiging worden verkocht en dat een aanzienlijk deel van die aankopen verdacht is." De minister stelt dat het project gericht is op het opwerpen van barrières voor het aanschaffen van gereedschap dat bij inbraken wordt gebruikt.

Privacy

PvdA-Kamerleden wilden weten in hoeverre door het bekijken van camerabeelden en het gebruiken van verkoopgegevens de privacy van klanten wordt geschon-

den. Daarop laat de minister weten dat de bouwmarkten een privacyreglement hebben waarin staat dat er cameratoezicht plaatsvindt en betaalgegevens worden geregistreerd. De politie is daarnaast op grond van de Wet politiegegevens bevoegd om kennis te nemen van aangeboden tips.

"Van een ongeoorloofde schending van de privacy is dan ook geen sprake. Overigens worden door de politie geen gegevens in de vorm van kassabonnen of camerabeelden meegenomen. Hoe effectief deze aanpak in de praktijk is, ook in relatie tot de benodigde inspanning, zal een evaluatie over een langere periode moeten uitwijzen", besluit Opstelten. De bouwmarkten werden vanwege het cameraproject genomineerd voor de Big Brother Awards. Uiteindelijk besloten Gamma en Karwei van deelname aan het project af te zien.



Kun je e-books op legale wijze doorverkopen?

Tom Kabinet maakt legale e-books aantrekkelijker door weder-verkoop te faciliteren, aldus de site. Dit is echter inbreuk, stellen de uitgevers in een rechtszaak.



Sinds vorig jaar zomer de marktplaats voor tweedehands e-books Tom Kabinet online is, ligt de site met uitgevers overhoop. Op een sommatie om de activiteiten te staken ging Tom Kabinet niet, dus volgde een kort geding. De rechter gaf in eerste instantie, enigszins verrassend, Tom Kabinet het voordeel van de twijfel.

Illegaal aanbod is onrechtmatig

Het Hof Amsterdam trekt daar nu een streep door. Het wordt de site verboden om een platform te bieden waarop illegaal gedownload e-books kunnen worden verkocht; dat is in elk geval onrechtmatig.

Aangezien Tom Kabinet het aanbieden van illegale e-books tot nog toe op geen enkele wijze technisch kan voorkomen, moet de marktplaats dicht, in elk geval voorlopig.

Maar het Hof durft zich niet te branden aan de basisvraag of het verhandelen van tweedehands e-books eigenlijk mag of niet. Dat moet in de bodemzaak worden uitgediscussieerd, al dan niet door vragen te stellen aan het Europese Hof.

Waar draait het in de kern om? Tom Kabinet is een platform dat verkopers van e-books koppelt aan kopers. "We hebben hetzelfde doel als de uitgevers: het illegaal downloaden van e-books verminderen. Als je e-books ook weer kunt verkopen worden ze per saldo goedkoper en wordt het legale aanbod dus aantrekkelijker. Dat is nu te duur", legt Marc Jellema van Tom Kabinet uit.

Baanbrekend EU-vonnis over uitputting

"Tom Kabinet heeft als uitgangspunt, dat consumenten eerst moet worden duidelijk gemaakt dat illegaal downloaden een vorm van stelen is. Het is heel gewoon geworden, om 2000 e-books op een memorystickje van vrienden te krijgen. Niemand denkt er meer bij na dat dit broodroof is van schrijvers. Deze mentaliteitsverandering

die we nastreven, tezamen met een schriftelijke verklaring van een verkoper dat hij het boek dat hij aanbiedt wist zodat het enige exemplaar naar de koper gaat, garandeert in onze ogen het uitputtingsbeginsel", licht mede-initiatiefnemer Judith Marien toe.

Dat uitputtingsbeginsel geldt voor papieren boeken, maar dus ook voor e-books, vindt Tom Kabinet. Het vindt daarin steun in een baanbrekend arrest van het Europese Hof uit 2012, die de wederverkoop van Oracle softwarelicenties door Usedsoft legaal verklaarde.

De uitgevers hebben hun rechten dus uitgeput. Om ze toch tegemoet te komen, zal Tom Kabinet zo'n vijf cent per verkocht tweedehands e-book geven. Jellema: "We willen graag samenwerken met de uitgevers, maar desnoods gaan we zelfstandig door. We zijn niet uit op een juridische strijd, al zou duidelijkheid hierover wel fijn zijn."

E-books zijn geen software

Die duidelijkheid is er eigenlijk al, stelt Christiaan Alberdingk Thijm, advocaat van de verenigde uitgevers, het NUV. "Deze zaak is juridisch niet heel ingewikkeld. Het Usedsoft-arrest van het EU-Hof gaat heel specifiek over softwarelicenties. Het gaat in die zaak primair om de software-richtlijn. En die gaat niet op voor e-books. Het aanbod daarvan is niet vatbaar voor uitputting. Daarnaast is er het economische argument. Een papieren boek en een e-book zijn echt totaal verschillend, ook functioneel. Kortom: Tom Kabinet maakt inbreuk op de rechten van de uitgevers."

Uiteindelijk drijft Tom Kabinet op twee cruciale beloften van verkopers. Ten eerste: de herkomst van het e-book is legaal; en ten tweede: de verkoper wist het oorspronkelijke bestand van zijn computer nadat het e-boek is geüpload

naar Tom Kabinet. Geen van beide worden gecontroleerd door de site.

Op basis van vertrouwen

Bij verkoop van een 'tweedehands' e-book treft Tom Kabinet wel technische maatregelen. Er wordt dan een digitaal watermerk aangebracht vlak voordat de koper het e-book kan downloaden. "Deze watermerken worden opgeslagen in een database. Dit is allemaal ter bescherming van de koper en verkoper. Biedt iemand het e-book illegaal op internet aan? Dan kan het watermerk aantonen wie de boef is. Op deze manier doet Tom Kabinet al wat in zijn vermogen ligt om legaal doorverkopen en daardoor goedkoper lezen van e-books mogelijk te maken. Tom Kabinet vertrouwt erop dat de verkopers de uitgangspunten van Tom Kabinet respecteren", aldus de site.

De uitgevers hebben daar in elk geval geen vertrouwen in. Zij kunnen zelf ook niet achterhalen of boeken verkocht via Tom Kabinet verder worden verspreid, omdat zij niet over de database met gewatermerkte bestanden van Tom Kabinet beschikken.

90 procent e-books illegaal

Advocaat Alberdingk Thijm: "Het draait uiteindelijk alleen maar op de verklaringen van de eindgebruikers. Maar de kans dat iemand die illegale e-books heeft zich wel netjes aan de beloften van Tom Kabinet houdt is niet heel groot. Vergeet niet: 90 procent van de e-books in omloop zijn illegaal. Het risico op piraterij is hier dus levensgroot. En dat risico is ook niet vergelijkbaar met de Usedsoft-zaak. Daar was de herkomst helemaal niet in vraag. Bovendien kan Oracle ook na wederverkoop de geldigheid van de softwarelicentie verifiëren."

Zo bescherm je jouw identiteit bij een ID-kopietje

De gevaren van identiteitsfraude bij het afgeven van een kopie van je identiteitsbewijs blijven vaak onbelicht. Deze nuttige app van de overheid maakt hier een einde aan.

De mobiele app KopieID maak een veilige kopie van je identiteitsbewijs, paspoort en ook officiële documenten zoals bankafschriften, loonstroken en post met adressen erop. Gevoelige informatie kan met de app worden doorgestreep en voorzien van een handig watermerk..

De gevolgen van identiteitsfraude met een ongemarkeerde ID-kopie kunnen groot zijn. De verhalen waarbij een op het oog onschuldig kopietje rondslingerde en werd misbruikt zijn talrijk. Kwaadwillenden die jouw identiteit stelen kunnen met de gegevens op je identiteitsbewijs in ons land namelijk een lening aanvragen, telefoonabonnement afsluiten of een huis of auto op jouw naam registreren.

Daarom is nu de mobiele app KopieID beschikbaar. Hoewel reeds uitgebracht in november 2014, kampte de app met behoorlijk wat kinderziektes. Zo was het watermerk niet doorzichtig genoeg en kregen veel gebruikers de foto niet scherp.

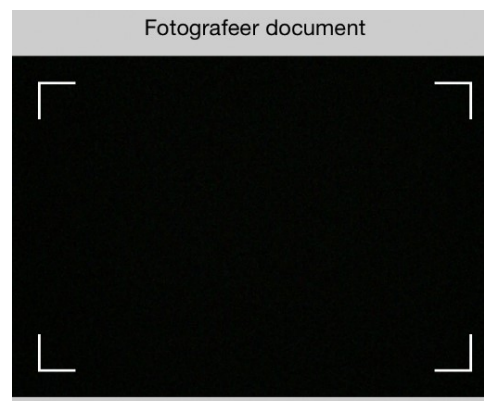
Die zijn nu met de eerste grote update grotendeels verleden tijd, al is de app nog lang niet uitontwikkeld. De app van het ministerie van Binnenlandse Zaken kan worden gedownload op Android, iOS en Windows Phone.

Hoe werkt 'het nieuwe kopiëren' van je identiteitsbewijs?

Stap 1: Fotografeer je document

Er verschijnt een handig kader in het scherm van je mo-

biele telefoon of tablet. Dit helpt je bij het nemen van de foto van je document. Zorg dat je deze er zo groot mogelijk op krijgt. Dat voorkomt gepriegel bij volgende stappen.



Stap 2: Markeer je BSN

Door middel van een eenvoudige swipe over je scherm is gevoelige informatie markeerbaar. Er ontstaat een zwarte streep waar je maar wilt. Markeer uiteraard altijd je BSN-nummer wanneer deze niet noodzakelijk is. Denk verder aan adressen, namen of cijfers die je privé wilt houden.



[Annuleer](#)

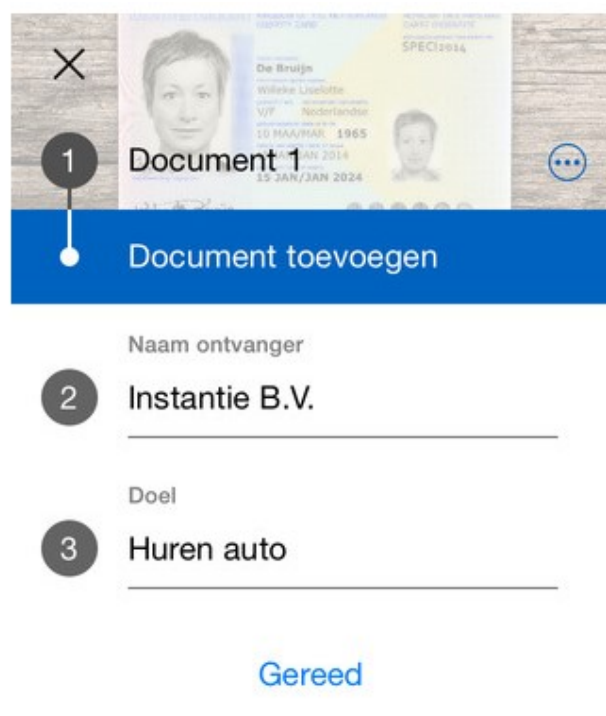
[Gereed](#)

[Index](#)

Zo bescherm je jouw identiteit bij een ID-kopietje (2)

Stap 3: Ontwerp je watermerk

Bij deze stap vul je twee belangrijke zaken in. Ten eerste voor wie de kopie bedoeld is, bijvoorbeeld je werknemer, onderwijsinstelling of auto-verhuurbedrijf. Als twee waarvoor de kopie nodig is, dus bijvoorbeeld een arbeidscontract, inschrijving of huurovereenkomst. Deze informatie verschijnt inclusief aanmaakdatum als watermerk op je document.



Document 1

Document toevoegen

Naam ontvanger

2 Instantie B.V.

Doel

3 Huren auto

Gereed

Stap 4: Verstuur je document

Tot slot krijg je de mogelijkheid om je veilige kopie direct te versturen via het bekende menu van je besturingssysteem. Mail je kopie zo naar jezelf of direct naar de bewuste instantie. Je kunt bij stap 3 ook meerdere kopies tegelijkertijd versturen via 'Document toevoegen'.



Thuisrouters: tikkende tijdbommetjes

Opnieuw claimde een hackersgroep deze week toegang te hebben tot een grote schare thuisrouters. 'Lizard Squad' zegt de routers in te zetten voor duizenden DDoS-aanvallen.



Volgens beveiligingsonderzoekers heeft de hackersgroep toegang tot de routers verkregen door gebruik te maken van de zwakke standaard wachtwoordbeveiliging die menig thuisrouter kent en die door de gebruiker niet wordt aangepast. Eenmaal binnen configureert [Lizard Squad](#) de routers als [DDoS-wapen](#) in een grootschalig botnet, zo schreef beveiligingsonderzoeker Brian Krebs eerder.

[Thuisrouters](#) zijn al langer een punt van zorg. Zo bleek in februari vorig jaar dat de firmware van vele routermodellen van Asus makkelijk was te kraken, werden in september honderdduizenden routers van de Braziliaanse internetprovider GVT gekaapt en kwam in december uit onderzoek van bureau Check Point naar voren dat 200 routermodellen van gerenommeerde fabrikanten als D-Link, Huawei, TP-Link en ZyXEL kwetsbaar zijn door een lek in de ingebouwde webservermodule van de apparaten.

Dit zijn slechts enkele voorbeelden van de lange lijst incidenten met thuisrouters. De apparaten zijn voor hackers een lucratief doelwit omdat ermee toegang kan worden verkregen tot netwerken die vanaf het internet niet te benaderen zijn en een hack veel lastiger te detecteren is dan op een PC; thuisrouters draaien immers geen antimalware of antivirussoftware.

Hackers kunnen thuisrouters niet alleen inzetten voor DDoS-aanvallen maar de devices

ook bijvoorbeeld gebruiken voor het onderscheppen van internetverkeer en het manipuleren van DNS-tabellen, wat bijvoorbeeld leidt tot diefstal van inloggegevens van internetbankieren en phishing.

Security? Meh.

Helaas gaan de problemen nog verder dan routers. Ook kabelmodems, webcams en netwerkprinters zijn eenvoudig te kraken. In oktober waarschuwde het securityteam van beveiliging ProLexic nog dat naar schatting 4,1 miljoen van zulke apparaten wereldwijd kwetsbaar zijn omdat ze onveilig zijn geconfigureerd.

Probleem is vaak dat consumenten niet de moeite nemen om hun device aan te passen naar veiliger instellingen en ook het patchen wordt niet gedaan. Zo lang leveranciers de apparaten niet op afstand (over-the-air) bijwerken en standaard onveilige services en poorten open laten staan, wordt dit probleem zeker niet opgelost.

Het is te hopen dat de constante stroom aan onheilspellende berichten bewustzijn bij consumenten creëert en leveranciers ertoe noopt meer rekening te houden met aanvallen van buitenaf. Maar beide lijken utopieën, gezien consumenten ook nog steeds niet leren van de gevaren van e-mail, gebruik van onveilige wachtwoorden en de risico's bij internetbankieren en routerfabrikanten verwikkeld zijn in een strijd om het meest goedkope (lees: onveilige) product. De marges zijn zo klein dat

security nauwelijks aandacht krijgt, en zeker niet als het apparaat al verkocht is.

Internet of Everything? Internet of Ellende

Gebeurt er niets, dan is het leed niet te overzien, waarschuwt de bekende Amerikaanse technologiejournalist Glenn Fleishman op de site van MIT Technology Review. Hij waarschuwt voor de gevaren die de massa's intelligente apparaten zullen brengen als deze en masse de huiskamer binnendringen.

Lampen, broodroosters, wasmachines en alarminstallaties zijn vanaf 2020 allemaal met internet verbonden - dat belooft Samsung onlangs op de elektronica-beurs CES - en met beveiliging wordt weinig rekening gehouden, enerzijds vanwege het ontbreken van standaarden hiervoor en anderzijds vanwege het bieden van gemak aan de consument dat prioriteit geniet.

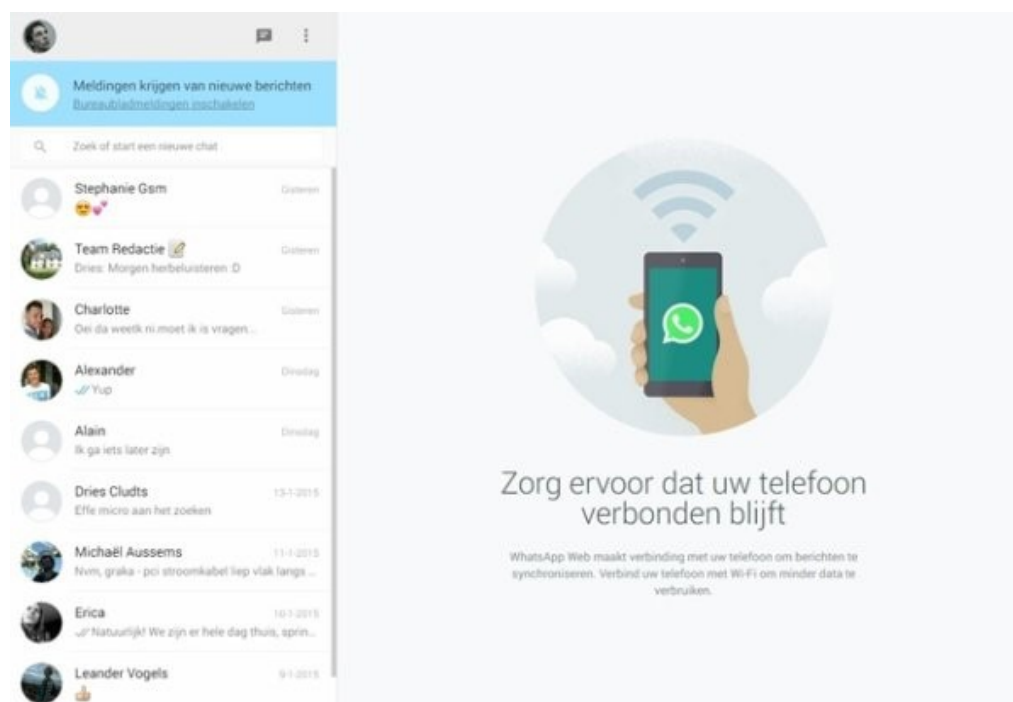
Naar schatting leiden enkele tientallen miljoenen routers op dit moment een sinister dubbelleven op internet, maar als de voorspellingen van bureaus als IDC, Gartner en Forrester kloppen, groeit de hoeveelheid (kwetsbare) apparaten komende vijf tot tien jaar naar een markt van 20 tot 50 miljard devices. Dat zijn nogal wat zombies om je bedrijfsnetwerk tegen te beschermen.

Whatsapp nu ook voor op je desktop

WhatsApp is niet langer beperkt tot smartphones. De berichtendienst, die sinds kort in handen is van Facebook, heeft een webversie gelanceerd zodat je kan chatten via de browser.



Met de nieuwe webversie breidt WhatsApp zijn bereik uit naar nog meer toestellen. De dienst was reeds als applicatie beschikbaar op de meeste mobiele platformen, maar door de uitbreiding naar de browser kan je nu ook via je laptop of desktop whatsappjes sturen. Momenteel telt WhatsApp al meer dan 600 miljoen gebruikers.

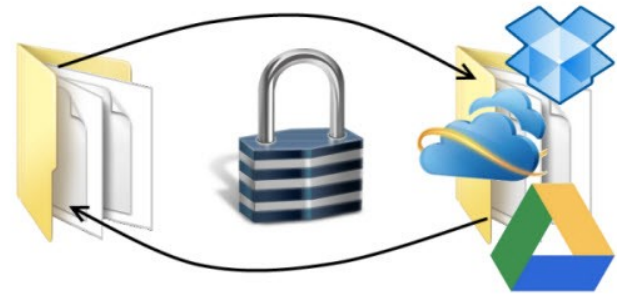


De webversie werkt niet losstaand, maar in combinatie met de mobiele app. Je smartphone moet dus met het internet verbonden zijn. De browser spiegelt de conversaties op je smartphone, zodat je ze kan lezen en beantwoorden via je pc. Aanmelden op de webversie gebeurt via een QR-code die je met je smartphone moet inscannen.

Er zijn voorlopig wel nog enkele beperkingen aan de webversie. Ten eerste werkt de service alleen in de Chrome-browser. Ten tweede is er geen ondersteuning voor de iPhone wegens beperkingen van het iOS-platform. Op Android, Windows Phone en Blackberry wordt de browsersversie wel ondersteund.

Bestanden versleuteld synchroniseren

CryptSync lijkt een doorsnee synchronisatietool, maar er is meer: in de tweede map worden automatisch alle data gecomprimeerd en versleuteld.



Sommige gegevens houd je wellicht liever verborgen voor derden – zeker wanneer je die ergens in de cloud bewaart. Encryptie is dan de zekerste manier om dat te doen. [CryptSync](#) heeft hiervoor een wat aparte aanpak: deze tool synchroniseert twee mappen maar wel zodanig dat slechts één van beide wordt versleuteld.

Het idee achter CryptSync ([beschikbaar voor Windows 32- en 64-bits](#)) is even wettig, maar het blijkt wel efficiënt. Allereerst geef je aan welke map je “originele” bestanden bevat – deze worden door de tool niet versleuteld. Vervolgens duid je de map aan die een versleutelde kopie van je originele bestanden moet bevatten. Uiteraard voorzie je hiervoor een stevig wachtwoord. Veel meer hoeft je eigenlijk niet te doen: CryptSync zorgt automatisch voor een synchronisatie in twee richtingen. Anders gezegd: bestanden die nieuw of gewijzigd zijn in de ene map worden vanzelf ook aangepast in de andere.

Je kiest zelf of ook de bestandsnamen mee moeten worden [geëncrypteerd](#). Houd er dan wel rekening mee dat de bestandsnamen ongeveer dubbel zo lang worden: om te voorkomen dat je besturingssysteem niet met de lange bestandsnamen overweg kan, beperk je de originele namen veiligheidshalve best wel tot maximaal 120 tekens. Het is tevens mogelijk bepaalde bestanden niet mee te laten synchroniseren of niet mee te laten encrypteren.

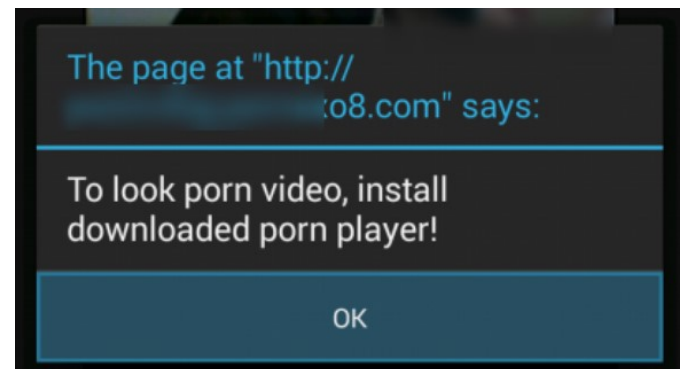
Standaard wordt [7-Zip](#) voor de encryptie gebruikt, wat meteen inhoudt dat je bestanden in de versleutelde map worden gecomprimeerd (zodat ze ook minder schijfruimte in beslag nemen). Handig aan deze aanpak is dat je niet noodzakelijk CryptSync moet hebben geïnstalleerd om de versleutelde bestanden weer in te lezen. Je kunt die net zo goed openen met 7-Zip of een andere, compatibele compressietool. CryptSync voorziet nog in een alternatieve vorm van encryptie gebaseerd op GnuPG. In dit geval worden de bestanden niet gecomprimeerd en kunnen ze zelfs iets meer schijfruimte dan de originele data in beslag nemen.

Het is uiteraard ook mogelijk een map te kiezen in bijvoorbeeld de lokale opslagruimte van je account bij [Google Drive](#), [Dropbox](#), [OneDrive](#) of andere cloudopslagdiensten. Ook die map wordt dan automatisch versleuteld. Niets weerhoudt je overigens om twee of meer paren mappen te creëren, telkens met dezelfde originele map: dat zorgt ervoor dat de bestanden automatisch naar de twee (of meer) ingestelde doelmappen worden gekopieerd en versleuteld.



Porndroid gijzelt je smartphonebestanden

Nieuwe ransomware voor Android houdt flink huis, dankzij porno, social engineering en schaamte. Gebruikers worden verleid om een zogenaamde videoplayer te installeren, maar zijn daarna gepakt.



Porndroid is de naam van de malware die eenmaal binnen op Android-apparaten alle data van gebruikers gijzelt. De ransomware versleutelt die bestanden en eist dan losgeld. Android-gebruikers worden slachtoffer door slimme social engineering die inspeelt op hun behoefte aan pornovideo's. Porndroid bevat namelijk een nepmelding om een videoplayer te installeren, die dan de eigenlijke ransomware is.

Met makkelijke installatie-instructies

De nepmelding van het zogenaamde PornPlayer Team belooft gemakkelijke, voor mobiel geoptimaliseerde toegang tot porno, zonder ads. De gretige gebruiker krijgt duidelijke instructies voorgeschoteld hoe de 'videoplayer' te installeren, langs de permissies en beschermingsmaatregelen van Android. De malware wordt namelijk geïnstalleerd vanaf een 'externe bron' en niet een officiële app store. De gebruiker moet daarvoor in Android wel permissie geven.

Zodra de app goed en wel geïnstalleerd is, versleutelt het de gebruikersdata en schotelt het zijn slachtoffers een nep FBI-melding voor. "Op basis van een volledige scan van uw device zijn enkele verdachte bestanden aangetroffen en uw aanwezigheid op de verboden pornografische websites is vastgesteld", aldus de waarschuwing. "Om deze reden is uw device vergrendeld."

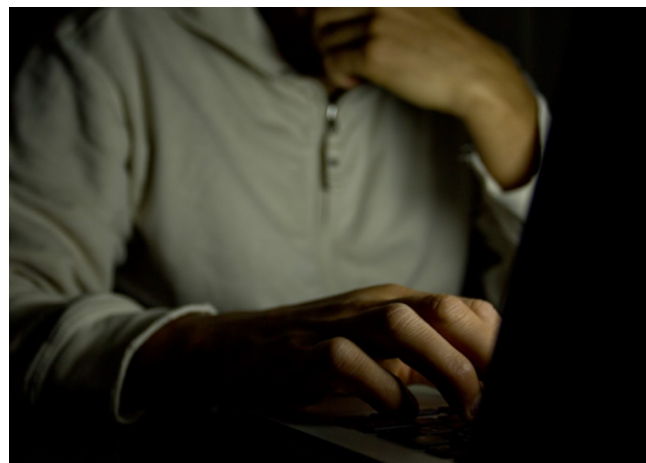
Gretige gebruiker gekiekt

Het dreigement van zogenaamde illegale activiteit en de losgeldeis van 500 dollar wordt kracht bijgezet met een foto van het slachtoffer. De ransomware legt de pornoliefhebbende gebruiker namelijk vast met de frontcamera van diens eigen Android-toestel. Porndroid houdt nu flink huis in de Verenigde Staten, maar ook Nederlandse gebruikers met een zwak voor 'natuurvideo's' kunnen risico lopen. De malware wordt aangeboden via porno-advertentienetwerken als ExoClick, EroAdvertising en Plugrush die zo'n 500.000 gebruikers per dag doorsturen naar de zogenaamde pornosite met de gratis 'videoplayer'.

Tot en met december zijn er zo'n 180.000 tot wel 240.000 slachtoffers gemaakt, aldus de onafhankelijke Franse security-onderzoeker Kafeine. Per dag worden er gemiddeld 7000 toestellen gegijzeld. Ondanks dat grote aantal infecties is er tot op heden nog weinig ruchtbaarheid geweest over Porndroid. Kafeine blogt dat schaamte van de slachtoffers de voornaamste oorzaak is van dit stil houden.

Opgerolde illegale marktplaats Silk Road weer online

Silk Road is terug onder de naam Silk Road Reloaded. De verborgen marktplaats bevindt zich niet langer op het Tor-netwerk maar is verplaatst naar een minder bekend anoniem netwerk, I2p.



Afgelopen november rolden autoriteiten Silk Road 2 op, waarbij er meer online zwarte markten het schip ingingen. Silk Road Reloaded biedt veelal dezelfde illegale handel aan: drugs, vervalst geld, nep ID-bewijzen en hacksoftware.

Er wordt nog niet gehandeld in wapens en gestolen creditcardinformatie, meldt Motherboard. Betalingen zijn mogelijk in verschillende vormen van cryptovaluta, waaronder Darkcoin, Anoncoin en Dogecoin. Silk Road en zijn opvolger handelden voornamelijk in Bitcoin.

Verhuizing

Inmiddels is twee maal gebleken dat Silk Road niet veilig is op het Tor-netwerk. Nu is de opvolger te vinden door de I2p-software te installeren en op die manier naar de site te surfen, die eindigt op de .i2p-extentie.

Onderzoekers claimden al meerdere keren methodes te hebben gevonden Tor-gebruikers uit de anonimiteit te halen en de beheerders van het Tor-netwerk waarschuwden gebruikers ervan vooreventuele aanvallen.

Kwetsbaar

Het is de keerzijde van de medaille: door de onthullingen van Snowden is het anonieme netwerk populairder dan ooit, maar ook kwetsbaarder. Criminelen lijken hun heil daardoor nu ergens anders te zoeken.

[I2P](#), of voluit Invisible Internet Project (onzichtbaar internetproject), is een gedecentraliseerd, Peer-to-peer, anoniem communicatienetwerk dat bovenop het gewone internet werkt (een zogenaamd 'overlay netwerk'). Programma's kunnen bovenop I2P met elkaar communiceren door berichten uit te wisselen. Zo kan men anoniem browsen, bestanden delen, bloggen, chatten en dergelijke. Het is vergelijkbaar met Tor en Freenet, hoewel er grote verschillen zitten tussen I2P, Tor en Freenet. I2P is open source vrije software, en is gratis te gebruiken.



Selfies gelinkt aan psychopathie en narcisme

Amerikaans onderzoek stelt een link vast tussen mannen die vaak selfies posten en psychopatische en narcistische trekjes. Ook bij vrouwen zou een dergelijke link aanwezig zijn.



De selfie: een mooie illustratie van de tijdsgeest. Het feit dat een selfiecamera vandaag een must is op iedere smartphone, en dat hij maar al te vaak vergezeld wordt van digitale make-upsoftware, vertelt ongetwijfeld iets over het tijdperk waarin we leven. Onderzoekers aan de Ohio State University ontdekten nu dat het posten van selfies ook iets vertelt over jezelf. Professor Jesse Fox onderzoekt het selfiestgedrag van mannen en linkte het aan narcisme en psychopathie. 800 mannen tussen de 18 en de 40 jaar oud werden ondervraagd over hun selfiegewoontes. Onderzoekers wilden onder andere te weten komen hoe vaak ze foto's van zichzelf online zetten, en of ze die afbeeldingen dan ook eerst bewerken.

Narcissus

Vervolgens moesten de mannen standaard vragenlijsten invullen die gebruikt worden om narcistische en psychopathische eigenschappen te detecteren. De eerste vaststelling van het onderzoek valt moeilijk verrassend te noemen. Mannen die geregeld foto's van zichzelf op Facebook of Instagram zetten en die ook bewerken, blijken significant narcistischer dan hun geslachtsgenoten die dat niet doen. Wij hadden reeds een donkerbruin vermoeden dat een dergelijke correlatie ging opduiken maar bij deze wordt dat vermoeden dus wetenschappelijk bevestigd.

De tweede vaststelling was opvallender. Mannen die zich geroepen voelen veel selfies van zichzelf met de wereld te delen, hebben meer psychopathische eigenschappen dan mannen die dat niet doen. Bij de psychopaten gaat het in contrast tot de narcisten vooral om de kwantiteit van de selfies. Fotobewerking zoals het toevoegen van flatterende sepiafilters of het uitsnijden van een strakke biceps laten zij dus achterwege.

Gebrek aan empathie.

Fox is niet verrast door dat onderscheid. Psychopathie wordt

gekenmerkt door een gebrek aan empathie, interesse in anderen en een neiging om impulsief te werk te gaan. Dat achteloos online gooien van foto's van jezelf past perfect in dat plaatje. Het moet snel en impulsief gebeuren, en dat het beeld misschien niemand anders interesseert, vermoedt onze selfiefanaat niet.

Het onderzoek linkte het bewerken van foto's dan weer succesvol aan zelf-objectificatie. Dat is het idee dat je uiterlijk je belangrijkste kenmerk is. Iemand die aan zelf-objectificatie doet, plaatst zijn uiterlijk boven andere positieve kenmerken, wat de kans op aandoeningen zoals een depressie verhoogt. Bij vrouwen komt het fenomeen geregeld voor terwijl het bij mannen nauwelijks onderzocht wordt. Sociale media dragen er echter toe bij dat uiterlijk voor velen belangrijker wordt, ongeacht het geslacht.

Geen echte psychopaten

Professor Fox benadrukt wel dat meer psychopathische kenmerken niet impliceren dat iedere selfietrekker een psychopaat of narcist is. Volgens Fox waren de antisociale kenmerken van mannen die veelvuldig selfies trekken wel degelijk bovengemiddeld, maar vielen alle resultaten nog binnen de marge van wat als normaal bestempeld wordt.

Voor dit onderzoek spitste de onderzoeker zich toe op mannen, maar gezien de interessante correlatie werkt hij momenteel aan een gelijkaardige studie bij vrouwen. De eerste resultaten lijken in de lijn van de mannenstudie te liggen. Fox besluit dat we allemaal bezig zijn met onze online aanwezigheid, maar dat hoe we dat doen wel eens meer over onze persoonlijkheid kan verklappen dan we aannemen. Over de link tussen duckface en het IQ deed Fox geen uitspraken.

Geavanceerde malware is haast niet tegen te houden

Malware is stukken lastiger tegen te houden en te verwijderen en richt veel meer schade aan dan de meeste mensen denken, zo stelt een rapport van de beveiligingsspecialist FireEye.



Of je nu voor een overheidsinstelling werkt of voor een bekend advocatenkantoor, er is een behoorlijke kans dat je computers geïnfecteerd zijn met malware. Dat is de conclusie van een rapport van FireEye over hoe de meeste bedrijven een stuk kwetsbaarder zijn voor kwaadaardige software dan ze zelf inschatten.

In mei was er al een eerste, gelijkaardig onderzoek van FireEye, dus Dave Merkel, de Technology Chief van het bedrijf is niet geheel geschokt door de resultaten. De moderne hackers zijn enorm gesofisticeerd en steeds op zoek naar de laatste manieren om digitaal in te breken.

“We hebben meer en meer te maken met professionele aanvallers”, aldus Merkel, “of dat nu georganiseerde criminelen zijn, dan wel overheden.”

Meer malware dan gedacht

Voor zijn studie gebruikte FireEye zijn cybersecuritysoftware om aanvallen te loggen bij meer dan 1.200 bedrijven in 20 sectoren. Malware, zo bleek, is veel meer aanwezig en richt veel meer schade aan dan de meeste mensen denken.

Elk onderzocht bedrijf uit de retail-, landbouw-, onderwijs-, gezondheids- en transportsector werd met succes aangevallen, zegt FireEye. Ook 91 procent van de entertainment- en mediabedrijven werden geïnfecteerd. Andere instellingen deden niet veel beter: liefst 76 procent van de ruimtevaart- en defensiebedrijven, sectoren die regelmatig het doelwit zijn van overheden, hadden krakemikkige IT-systemen. De studie duurde van januari tot juni 2014.

Dat is slecht nieuws voor de sector van de cyberbeveiliging: zij proberen de bedrijven al jarenlang te overtuigen dat hun software het enige is wat ze nodig hebben om zich te beschermen tegen hackers. De investeringen in beveiligingssoftware nemen bij bedrijven dan ook alleen maar toe.

Volgens FireEye echter is dat grotendeels weggegooid geld en zijn die dure tools hoogstens maar deels effectief. De meeste aanvallen gebeuren via e-mail en websites waarlangs er nieuwere en verbeterde versies van oude malware op de pc's van de slachtoffer wordt gezet. Volgens FireEye evolueert de malware veel sneller dan de oude technologieën kunnen bijhouden en moeten er dringend nieuwe verdedigingsmanieren worden ontwikkeld.

Het probleem ligt deels bij de bedrijven zelf. Ze betrouwen nog te vaak op antivirusprogramma's (technologie die in de laatste 20 jaar niet eens zo veel geëvolueerd is), wat hen te kwetsbaar maakt.

Aanvallen zoals die gebeurden op Sony Pictures zijn dan misschien niet 100 procent te voorkomen, de schade kan wel ingeperkt worden. Een manier zou kunnen zijn door gevoelige documenten op computers te bewaren die helemaal niet met het internet verbonden zijn, zegt Tyler Shields, veiligheidsanalist bij Forrester. “Als je echt bezorgd bent dat je kopieën van films of documenten kan kwijtspelen, moet je ze op een geïsoleerd systeem zetten”, zegt hij. “En dat hebben bedrijven nog altijd niet gedaan.”

Je pc wordt vaker aangevallen dan ooit tevoren

De afgelopen twee jaar is meer kwaadaardige software ontwikkeld dan in de tien jaar daarvoor bij elkaar opgeteld.



Computerherstellers hebben de laatste paar jaar steeds meer te maken met pc's die de geest hebben gegeven vanwege kwaadaardige software. Het verhelpen van virussen en malware is bij sommige reparateurs zelfs verantwoordelijk voor ongeveer een derde van de inkomsten. Dit heeft deels te maken met de exponentiële groei van het aantal types malware.

Enorme groei

Malware-ontdekkingen door AV-Test, een bedrijf dat de effectiviteit van antivirussoftware onderzoekt, stegen in 2014 naar meer dan 143 miljoen. Dat is een groei van 72 procent ten opzichte van een jaar eerder. Om het in perspectief te plaatsen: de afgelopen twee jaar is meer kwaadaardige software gevonden dan in de tien jaar daarvoor bij elkaar opgeteld.

Andere bedrijven die zich met malware bezighouden, zoals Malwarebytes en Kaspersky, is hetzelfde opgevallen. Zo zag Kaspersky in 2014 vier keer meer mobiele malware-aanvallen dan een jaar eerder. Dat zegt Patrick Nielsen, onderzoeker bij het bedrijf.

Jarenlang blokkeerde antivirussoftware de malware op basis van de code, maar hackers hebben iets nieuws bedacht. Ze kunnen een

bestaande malwarecode kopen of ergens gratis downloaden, vervolgens vervangen ze slechts een paar onderdelen en voila: ineens is je code onzichtbaar voor antivirusprogramma's.

"Het heeft veel weg van het overschrijven van het huiswerk van een klasgenoot", zegt Timo Hirvonen, onderzoeker bij F-Secure. "Het is net zo simpel als het weghalen van een woord of het toevoegen van een letter in een Word-document." Als gevolg hiervan verandert malware zo vaak dat het bijna niet meer tegen te houden is.

Gedrag bestuderen

De veiligheidsbranche probeert een antwoord te vinden. Een van de nieuwste technieken houdt in dat het gedrag van de malware wordt bestudeerd. Zo heeft de kwaadaardige software het vaak gemunt op je inlogcode voor online bankieren. Daarom worden alle bestanden die dit doen of proberen in de gaten gehouden door deze nieuwe veiligheidsssoftware.

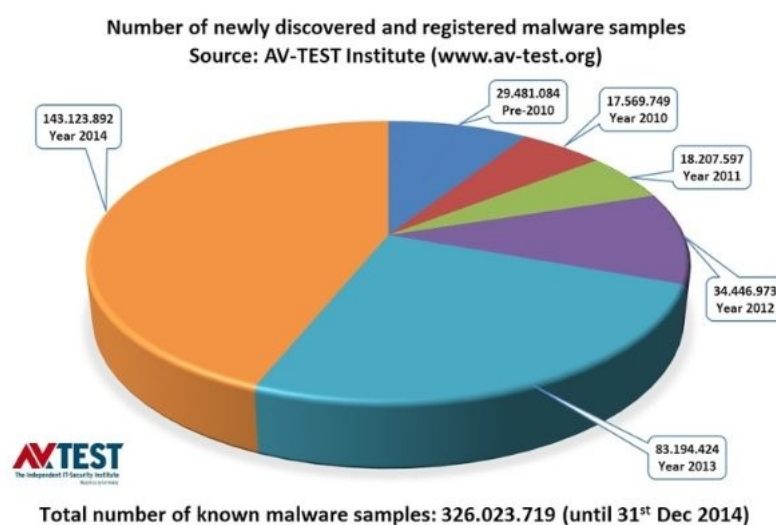
Maar zelfs op die manier is het bijna niet te doen. "Als het aan dit tempo doorgaat, dan heeft het gewoon geen zin meer om jezelf te verdedigen", vreest onderzoeker Jérôme Segura

van Malwarebytes.

Het escalerende kat-en-muisspel heeft de wereld van de cryptografie betreden. Hackers maken bewust een warboel van hun code, zodat de pakkans kleiner is. Hiervoor gebruiken ze dezelfde techniek als bedrijven die hun gevoelige informatie willen beschermen.

Voorzorgsmaatregelen

Het vermijden van 'dubieuze websites', zoals Nielsen het noemt, is al lang niet meer genoeg. We leven in een tijdperk dat kwaadaardige software ook geplaatst kan worden via advertenties op legitieme websites. Eenvoudige voorzorgsmaatregelen zoals het installeren van een goed antivirusprogramma en het up-to-date houden van alle software op je computer blijven van tel bij het beschermen van je computer tegen ongewenste software.



Spellingscontrole is gevaarlijker dan je denkt

Je spellingscontrole geeft meer informatie over je weg dan je denkt. Door spellingscontrole zijn je toetsaanslagen makkelijker af te luisteren. Zodanig zelfs dat het niet eens nodig is een keylogger te installeren.

**Spell check
your spell checker!**

Het gebruik van spellingscontrole in Word (of een ander tekstverwerkingsprogramma) maakt het mogelijk toetsaanslagen op te vangen en te herkennen. Dat zeggen wetenschappers van het Georgia Institute of Technology tegen de IDG News Service, de internationale nieuwsdienst van Webwereld-uitgever IDG.

De wetenschappers hebben een studie gedaan naar de mogelijkheden van het aftappen van zo geheten side-channel signalen (elektromagnetische pulsen vanuit pc-onderdelen, of soms gewoon geluid) en kwamen tot verrassende conclusies. Dat dergelijke signalen zijn op te vangen met antennes of microfoons was al eerder bekend. En ook dat daaruit zelfs encryptiesleutels zijn te distilleren. Maar naar nu blijkt zijn zelfs de meest onschuldige lijkende toepassingen helemaal niet zo onschuldig.

Een luid kabaal, op te vangen via radio

Het onderzoek moest oplossingen geven om aanvallen via side-channelsignalen af te slaan of moeilijker te ma-

ken. Daarbij werd duidelijk dat soms het uitschakelen van simpele toepassingen al genoeg kan zijn. Zo bleek een tekstverwerkingsprogramma vrij weinig signalen af te geven, zelfs zodanig dat het voor de af luisterende aanvaller vrijwel niet mogelijk is te identificeren welke toets op het toetsenbord werd ingedrukt.

Maar eenmaal de spellingscontrole aan gaf dat relatief gezien een enorm kabaal. Zodanig luid dat het signaal was op te vangen met een AM-radio, waardoor het zelfs hoorbaar werd voor het menselijk oor. Elke toetsaanslag zorgt ervoor dat de spellingscontrole aan de slag gaat voor controle in het woordenboek. Dat geeft enorm veel side-channelsignalen en kan dus worden afgeluisterd.

spell ✓
✓ check

Expert waarschuwt voor overdrijven van cyberterrorisme

Met de aanval op Sony is het woord "cyberterrorisme" regelmatig door media en politici genoemd, maar één expert merkt op dat het "hypen" van deze term voor angst onder de bevolking kan zorgen en uiteindelijk tot slechte wetgeving kan leiden.



[Edwin Covert](#) van het Amerikaanse [beveiligingsbedrijf Norse](#) stelt in een analyse van het concept cyberterrorisme dat er zeer weinig bewijs is dat het ook daadwerkelijk voorkomt.

Bij veel beveiligingsincidenten en aanvallen is er sprake van sabotage of spionage en niet van terrorisme. Volgens Covert is cyberterrorisme als strategie voor echte terroristen overdreven door de media. "Er is een algemeen idee in de nieuwsindustrie dat zegt, 'If it bleeds, it leads', verhalen moeten een sensationele hoek hebben om de aandacht van lezers of kijkers te trekken." Het overdrijven kan echter voor angst zorgen, waarop politici vervolgens slecht beleid voorstellen.

"Dit overdrijven heeft in meerdere gevallen tot dubieuze wetgeving geleid door mensen die niet de details van het uitvoeren van een cyberterroristische-aanval kennen. In plaats daarvan reageren ze vanuit angst en twijfel", stelt Covert. Zo zijn in meerdere landen de gevangenisstraffen voor het binnendringen van computersystemen verhoogd, ongeacht de uitgevoerde activiteiten. Een rechter, die volgens Covert vaak niet het fijne weet van cyberdreigingen en aanvallen, gaat bij iemand die wegens ongeautoriseerde toegang tot een computersysteem is opgepakt van het ergste uit en legt vervolgens een zware straf op.

Relativeren

"Door de komst van internet is het leven van mensen opmerkelijk veranderd en de snelheid van deze veranderingen zorgt voor angst", stelt Covert. De angst ontstaat dat terroristen de systemen waarvan we afhankelijk zijn tegen ons gebruiken. Toch zijn er nog altijd geen concrete aanwijzingen voor cyberterrorisme. Eerder haalde ook beveiligingsexpert Bruce Schneier uit naar het hypen van de term cyberterrorisme.

Volgens Covert moeten dan ook meer security-professionals dit soort sentimenten onder bevolking en politici tegengaan door ervoor te zorgen dat de echte dreigingen worden verholpen en dat de ongefundeerde dreigingen minder aandacht en middelen krijgen.

"Alleen dan kunnen de belangrijke dreigingen worden aangepakt", zo besluit de expert.



ENISA doet aanbevelingen voor privacy by design

Privacy is een kernwaarde voor zowel individuen als democratische samenlevingen en daarom is het belangrijk dat 'privacy by design' standaard bij het opstellen van beleid en ontwikkelen van systemen wordt meegenomen, zo stelt het Europees agentschap voor netwerk- en informatiebeveiliging (ENISA).



De organisatie schreef een nieuw rapport voor databeschermingsautoriteiten, beleidsmakers, toezichthouders, ingenieurs en onderzoekers dat naar privacy by design kijkt. Huidig beleid zou namelijk niet altijd compatibel met privacy by design zijn. Daarom moet nieuw beleid ervoor zorgen dat het toepassen van dit principe juist wordt aangemoedigd.

Standaarden

Verder wil [ENISA](#) dat nieuwe standaarden voor elektronische communicatie met privacy- en databescherming rekening houden, terwijl standaarden die dit niet doen worden uitgefaseerd. De organisatie wijst naar zogeheten Privacy-Verbeterende Technologieën (PETs). Het gaat dan bijvoorbeeld om encryptie en protocollen voor anonieme communicatie. Op een aantal uitzonderingen na, zoals encryptie dat nu veel wordt gebruikt, zijn PETs geen standaard en worden weinig gebruikt binnen sys-

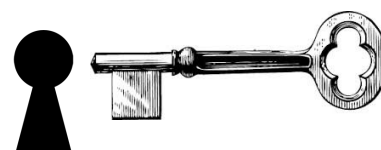
teemontwerp.

Het rapport van ENISA probeert naar eigen zeggen een brug te slaan tussen het juridische raamwerk en de beschikbare technologische oplossingen. Zo wordt een overzicht van bestaande aanpakken en privacy by design-strategieën gegeven, alsmede de "technische bouwstenen". Uiteindelijk worden verschillende onderdelen genoemd die voor de ontwikkeling van privacyvriendelijke systemen en diensten moeten zorgen.





Software schatkist



< Klik op de sleutel om de schatkist te openen >

Browser Hijack Recover

PC Transfer

Trusteer Rapport

Blackberry Desktop Software

DVD Flick

EaseUs Partition Master

EmsiSoft Emergency Kit

Any Burn

Freemake Video Converter

xPlorer2

2Doc: Puck en raadsel van de codes (video)



Keer op keer blijkt het enorm lastig om ID-fraude op sociale media te bestrijden. Een recent slachtoffer is kerkhistoricus Frank van der Pol, professor aan de Theologische Universiteit te Kampen. Van der Pol kreeg te maken met een genepte twitteraccount waarop uit naam van zijn 'tweelingbroer' Wim werd opgeroepen om mensen die Geert Wilders bedreigen, te vergassen. Bij de tweets werd een profielfoto van Frank van der Pol gebruikt. Hij schrok: 'als ik naast mijn beeltenis foto's zie van een executiepeloton en geknielde slachtoffers in combinatie met Wilders, voel ik als hoogleraar gereformeerde theologie een onmogelijke spanning'. Het account is inmiddels weer verdwenen. Van der Pol deed aangifte en hoopt dat de dader, via een ip-adres, getraceerd kan worden. En vervolgd: sinds 2014 staat er maximaal vijf jaar celstraf op het aannemen dan wel misbruiken van andermans identiteit. Van der Pol is lang niet de enige die last heeft van een id-fraudeur, hoewel exacte cijfers niet voorhanden zijn. Volgens Simone van der Hof, directeur van het Center for Law and Digital Technologies, komt het vaak voor en wordt er ook 'flink meer melding van gemaakt'. ID-fraude vindt volgens haar vooral plaats voor financieel gewin; ook geen kattenkwaad natuurlijk. Vaak zijn BN'ers de pineut. Zo bleek deze week dat ook zanger Jan Smit last heeft van een nepaccount op facebook. Daarop 'schrijft' de zanger dat een handtekening vijftien euro kost 'plus 6,95 verzendkosten', want 'voor niets gaat het Volendamse zonnetje op!' Ook deze pagina werd snel verwijderd.

In de VS is Timothy DeFoggi (56) veroordeeld voor het runnen van een kinderpornosite op het dark web. DeFoggi, voormalig chieft cybersecurity bij het ministerie van Gezondheid, kreeg 25 jaar. Hij werd aangehouden op heterdaad – toen de FBI binnenviel, was hij net aan het downloaden. Volgens de aanklager gebruikte hij dezelfde technologie als waarmee hij cybercrime oploste, voor zijn eigen zoektocht. DeFoggi was eerder al schuldig bevonden door een jury. Vier medeverdachten kregen straffen van twaalf tot twintig jaar opgelegd.

Het meeste internetverkeer naar verborgen websites in het Tor-netwerk betreft kinderpornografie, zo blijkt uit onderzoek van de universiteit van Portsmouth. Onderzoeksleider dr Gareth Owen zei dat deze uitkomst hem tot andere gedachten bracht. Vond hij het dark web aanvankelijk een goede zaak – gebruikers kunnen actief zijn op internet zonder dat overheden of inlichtingendiensten kunnen herleiden in welk land ze zich bevinden -, nu blijkt dat het vooral een plek is 'waar pedofiele daders straffeloos hun gang kunnen gaan', veranderde hij van mening. De universiteit zette veertig computers in die niks anders deden dan Tor-sites zoeken en bekijken. In zes maanden tijd werden tachtigduizend verborgen sites gevonden, waarvan het merendeel maar een paar dagen bestond. Op de meeste sites werden drugs verhandeld, circa 2% van de verborgen sites bevatte kinderporno. Die sites trokken echter wel 83% van alle verkeer in het Tor-netwerk – 'een grote schok' voor Owen en zijn onderzoekers. Het Tor-netwerk trekt twee miljoen anonieme bezoekers per dag. Daarvan zouden er, volgens berekeningen van Owen, dertigduizend op zoek zijn naar kinderpornosites. Overigens stelt Owen ook dat niet met zekerheid te zeggen is hoeveel van die bezoeken door opsporingsdiensten en/of automatische zoekmachines worden gedaan dan wel door 'echte' gebruikers – Tor-verkeer is anoniem! In een reactie stelt de hoofdontwerper van Tor, Nick Mathewson, dat de bevindingen van Owen niet kloppen. Volgens Mathewson maakt het verkeer op het dark web slechts twee procent van het totale anonieme Tor-gebruik uit en is het onderzoek niet te controleren omdat veel sites alweer verdwenen zijn.

Het OM onderzoekt de bedreigingen die op de facebookpagina 'Steun de PVV' gedaan zijn tegen moskeeën. Op de pagina wordt, naar aanleiding van brandstichtingen bij drie Zweedse moskeeën, geroepen dat zoiets hier ook maar moet gebeuren 'maar dan wel tijdens hun gebed opruimen die hap'. Anderen roepen simpelweg 'gewoon platbranden die zooi' en kondigen een 'landelijke brandbommendag tegen moskeeën' aan. De facebookpagina werd augustus 2013 ingericht, kort nadat Wilders zijn 'mars' door de Schilderswijk aankondigde. De Raad van Marokkaanse Moskeeën (RMMN) en het Contactorgaan Moslims en Overheid (CMO) deden aangifte. Voorzitter Yahia Bouyafa van de raad riep moskeebe-

stuurders op waakzaam te zijn. Een deel van de reacties werd weggehaald nadat opiniesite Joop.nl erover berichtte. Eerder riep ook PvdA-kamerlid AAhmed Marcouch dat het OM in actie moest komen. De reactie van Marcouch leidde op de pagina overigens tot nieuwe geweldsoproepen.

Uit onderzoek van Women's Aid blijkt dat 41% van de slachtoffers van huiselijk geweld was gevolgd of belaagd via elektronische apparatuur. Een tweede onderzoek van Digital Trust, dat slachtoffers van online stalking helpt, laat zien dat meer dan de helft van de gewelddadige partners spyware of een andere vorm van elektronische surveillance gebruikt om slachtoffers te bespioneren. Volgens Polly Neate van Women's Aid zetten daders 'alle beschikbare middelen' in om de controle op hun slachtoffers te vergroten: telefoons, computers, internet, trackingsoftware en spyware.

De rechtbank Gelderland heeft drie personen veroordeeld voor mensenhandel. Het slachtoffer was een minderjarig meisje. De jongste man (21) kreeg drie jaar celstraf, waarvan een jaar voorwaardelijk. Hij werd ook veroordeeld voor mishandeling, bedreiging en wederrechtelijke vrijheidsbeneming. De oudste man (32) kreeg een jaar celstraf (de helft voorwaardelijk); de vrouw (24) kreeg 240 uur werkstraf en zes maanden voorwaardelijk. De oudste man en de vrouw maakten en verspreidden kinderporno, ze hadden onder meer foto's en een profiel van het meisje gemaakt voor een internetadvertentie waarin ze haar als prostitute aanboden. De jongste man werd ook veroordeeld voor loverboy praktijken. De twee mannen maakten afspraken met klanten, reden het meisje naar die klanten en verdeelden de opbrengst.



De 'waakdienst' voor cyberbedreigingen van het Nationaal Cyber Security Center (NCSC) is nu 24/7 beschikbaar. Het 'Nationaal Cyber Security Operations Center' (NCSOC) kan zo sneller opschalen en een gezamenlijke analyse en incidentenaanpak maken. De bredere openstelling is een gevolg van de toegenomen digitale dienstverlening van de overheid. Systemen moeten daarvoor altijd beschikbaar zijn, kwetsbaarheden moeten dan zo snel mogelijk worden ontdekt. Uiteindelijk moet een integrale aanpak van cyberdreigingen mogelijk worden. Daartoe zijn in 2014 al het Nationaal Respons Netwerk en het Nationaal Detectie Netwerk gelanceerd en nu dus het NCSOC. 'Aangevuld met specifieke cyberexpertise zijn we gezamenlijk in staat om, daar waar dat nodig is, gepast en tijdig respons te leveren bij cyberincidenten', aldus het NCSC.

In 2013 en 2014 werden 1,1 miljoen Nederlanders slachtoffer van internetoplichting. Zij gingen in totaal voor 5,3 miljard euro het schip in, gemiddeld 4900 euro per persoon. De Fraudehulpdeskondervroeg de afgelopen weken duizend mensen en daarvan zegt 9% slachtoffer te zijn geworden. De meeste mensen raken bedragen tot 500 euro kwijt, 12% van de slachtoffers verliest tussen de 1000 en 10.000 euro; 3% raakt meer dan 20 mille kwijt. Opvallend is wellicht dat het vooral dertigers en hoogopgeleiden zijn die in de val liepen. Ook opvallend is dat minder dan de helft aangifte deed. Volgens de Fraudehulpdesk is dat uit schaamte of omdat de politie die aangifte weigert op te nemen. Met tweederde van de aangiftes 'is niets gedaan'.

Jongeren sturen steeds vaker naaktfoto's en -filmpjes van zichzelf rond, berichtte Nieuwsuur deze week. Uit een peiling van bureau Sense en Rutgers WPF onder duizend scholieren bleek dat zeker zeshonderd van hen wel eens zo'n filmpje of foto ontvangen. Dat zoiets strafbaar is, beseffen jongeren zich niet of nauwelijks. En dat ze hierdoor zelfs een strafblad kunnen krijgen, al helemaal niet. De gemeente Amsterdam en de politie organiseren daarom in 2015 voorlichtingsbijeenkomsten voor ouders en docenten. In Kampen, een kleine honderd kilometer oostwaarts, sprak wijkagent Jean Louis Becker de afgelopen weken regelmatig met jongeren en welzijnswerkers over sexting. Het versturen van naaktfoto's blijkt voor scholieren een manier om je status in de klas te verhogen. Hoe seksueler of explicieter de foto's die je verstuurt, hoe populairder je bent. Becker zegt te zijn geschrokken. 'In mijn tijd was je blij met een kus in het fietsenhok, nu wordt je status bepaald door seksvideos'. Becker wil dat ouders hun rol pakken.

Waar het in deze kolommen regelmatig over Engeland, de VS, Canada, Spanje en België gaat, komt Duitsland relatief weinig aan bod. De politie in Duitsland doet, zeker in verhouding tot omliggende landen, ook maar weinig aan internetrecherche. Ze laat 'veel kansen op sociale media liggen', schreef Die Welt vorige week in een lang artikel. In het blad stelt politievakbondsbaas Andy Neumann dat de Polizei 'in der digitalen Steinzeit' is blijven steken waardoor bronnen als twitter, Youtube en facebook maar weinig gebruikt worden. De belangrijkste reden om die bronnen niet te gebruiken, is behalve een generatiekloof – we hebben het

toch ook jarenlang zonder sociale media gedaan – vooral een juridische. Experts wijzen op het zogeheten Legalitätsprinzip, dat bepaalt dat een Duitse agent ieder strafbaar feit waarvan hij kennis draagt, moet onderzoeken. Een kwestie van 'wat niet tweet, wat niet deert'? Tja, daar lijkt het wel op, aldus Neumann. Want op die sociale media gebeurt zo veel, dat alles aanpakken toch niet mogelijk is, met de toch al overbelaste korpsen. Ach, allemaal problemen die opgelost kunnen worden, stelt echter criminoloog Rudiger die de Duitse politie al eens adviseerde om vaker sociale media in te zetten.

De politierechter heeft een man (55, uit Woerden) veroordeeld tot dertig uur werkstraf omdat hij een wijkagent had bedreigd. De verdachte had naar eigen zeggen een slechte relatie met de wijkagent in Oudewater. Op Politie.nl stuurde de verdachte de agent, van Surinaamse komaf, een mail. 'Wat ben jij toch een zielig ventje op je mountainbike; ga terug maar je apenland om ploppers lastig te vallen'. Hoewel wijkagenten volgens de officier van justitie echt wel tegen een stootje kunnen, was de verdachte, die de agent ook nog een tekening van zijn piemel stuurde, veel te ver gegaan. Dat vond de rechter dus ook.

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](#)

[DeltaLloyd Bank](#)

[Staal Bankiers](#)

[DHB Bank](#)

[Triodos Bank](#)

[Friesland Bank](#)

[Van Lanschot Bank](#)

[ING Bank](#)

[ASN Bank](#)



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

Antwoord

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

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

Wij adviseren u om het formulier zo accuraat en volledig mogelijk in te vullen.

Zorg dat u, wanneer u aangifte gaat doen, alle relevante gegevens bij de hand heeft zoals:

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

Meld oplichting ook altijd aan Marktplaats. Wij nemen dergelijke meldingen zeer serieus en nemen waar mogelijk gerichte maatregelen. Indien u aangifte doet via het formulier Melding Internetoplichting op www.mijnpolitie.nl wordt direct



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

Cybercrime wetsartikelen

Wetsartikelen voor computercriminaliteit in enge zin

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

Voor cybercrime in enge zin zijn de volgende wetsartikelen beschikbaar:

. [Artikel 138a WvSr](#): het binnendringen in een geautomatiseerd werk.

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

. [Artikel 161 septies WvSr](#): stoornis in de gang of in de werking in een geautomatiseerd werk of werk voor telecommunicatie door schuld.

. [Artikel 350a WvSr](#): het opzettelijk onbruikbaar maken en veranderen van gegevens.

. [Artikel 350b WvSr](#): het onbruikbaar maken en veranderen van gegevens door schuld,

. [Artikel 139c WvSr](#): het aftappen en/of opnemen van gegevens en

[Artikel 139d WvSr](#): het plaatsen van opname-, aftap- c.q. af luisterapparatuur.

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

Haatzaaien.

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

[Haatzaaien](#) staat niet als zodanig in het wetboek.

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

- [Artikel 147 WvSr](#): godslastering
- [Artikel 90quater WvSr](#): discriminatie.
- [Artikel 137d WvSr](#): aanzetting tot discriminatie van een bevolkingsgroep.

- [Artikel 137e WvSr](#): openbaarmaking discriminerende uitspraken.
- [Artikel 137f WvSr](#): deelname of steunen van discriminatie.
- [Artikel 137g WvSr](#): discriminatie in ambt, beroep of bedrijf.
- [Artikel 131 WvSr](#): opruiing.

Cyberstalking.

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

Relevante wetsartikelen zijn:

[Artikel 285b WvSr](#): belaging.

[Artikel 138a WvSr](#): computervredebreuk.

[Artikel 266 WvSr](#): belediging.

Grooming.

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

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

meeting').

Handel in mensen of foute goederen.

Verschijningsvormen:

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

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

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

Relevante artikelen zijn:

[Artikel 273a WvSr](#) mensenhandel.

[Artikel 416 WvSr](#) opzetheling.

[Artikel 417 WvSr](#) opzetheling (gewoonte).

[Artikel 274 WvSr](#) slavenhandel.

[Artikel 2 Wwm](#): wet wapens en munitie

[Artikel 31 Wwm](#): overdragen van wapens of munitie

[Artikel 2 Ow](#): opiumwet

[Artikel 3 Ow](#): opiumwet

[Artikel 3b Ow](#): opiumwet



Cybercrime wetsartikelen (2)

Bij **piraterij** gaat het feitelijk om illegale handel van allerhande 'cd's, dvd's, films, software en andere producten waarvoor auteursrechten gelden'. De nadruk ligt volgens het [KLPD](#) veelal bij eindgebruikers, internetpiraten en vervalzers, 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 groeiindustriën

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 310 WvSr](#): diefstal.

[Artikel 321 WvSr](#): verduistering.

[Artikel 416 WvSr](#): heling.

