Secure Computing

07-2014

W.Bosgra taakaccenthouder Digitale Criminaliteit

"Als je bij de balie komt om aangifte te doen van een poging tot hacken, moet er wel iemand zitten die begrijpt waar het over gaat"

"Dat betekent dat de anonimiteit van de melder niet voldoende gegarandeerd kan worden. Daarnaast zal een gemiddelde gebruiker ongewild sporen achterlaten, en is ook de vernietiging van gegevens aan de kant van het meldpunt een punt van zorg"

"Gebruikers dachten dat ze hun toestel volledig schoonveegden en de fabrieksinstellingen herstelden"

Hoge Raad geeft zegen aan IMSI-catcher en stealth-sms

Het gebruik van een IMSI-catcher of stealth-sms om verdachten te lokaliseren is een 'beperkte inbreuk op de privacy', oordeelt de Hoge Raad. Toestemming van de Officier van Justitie is afdoende.

Er is geen aparte wettelijke regeling nodig voor de inzet van IMSI-catcher en stealth-sms, mits gebruikt voor het traceren van een verdachte en met toestemming van de Officier van Justitie. Dat oordeelt de Hoge Raad in drie verschillende zaken van verdachten die de legitimiteit van deze opsporingsmethoden bestreden.

Locatie verdachte achterhalen

Daarmee haalt de Hoge Raad een streep door het vonnis van het Hof, dat eerder oordeelde dat het gebruik van stille sms'jes door politie onwettig was. Een overwinning voor Justitie, die volhield dat een wetswijziging niet noodzakelijk was.

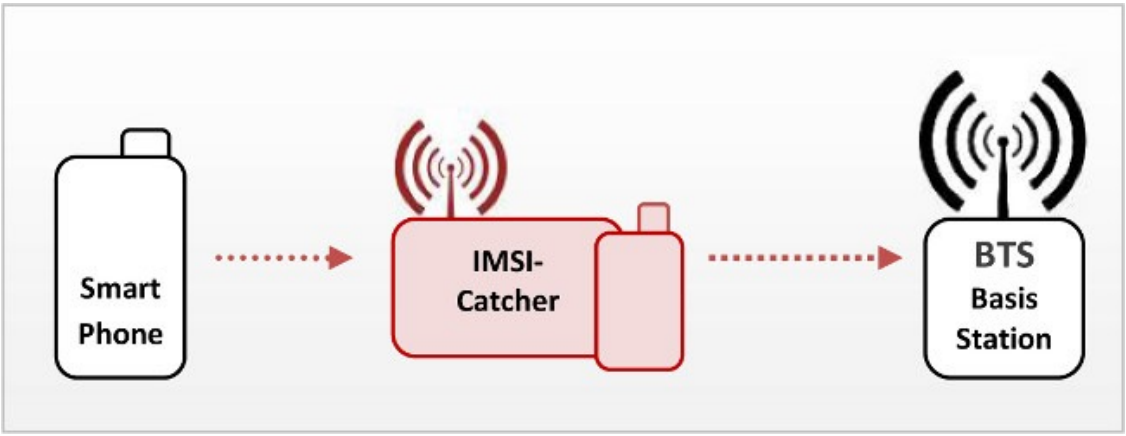
Bij het inzetten van stealth-sms stuurt de politie een leeg sms-bericht naar het mobiele nummer van de verdachte. Diens toestel straalt daardoor de dichtstbijzijnde gsm-antenne aan voor de ontvangst van dit onzichtbare bericht. Op basis van zendmastdata van de mobiele provider kan de politie de locatie van de verdachte op dat moment achterhalen.

IMSI-catcher kan ook tappen

Een IMSI-catcher is een apparaat dat zich voordoet als basestation van een mobiel netwerk. In het onderhavige geval is het alleen gebruikt voor lokalisatie van een verdachte, maar in principe is ongemerkt aftappen van mobiele gesprekken en data ook mogelijk met een IMSI-catcher.

Maar als beide opsporingsmiddelen alleen dienen om een verdachte te traceren, kortstondig worden gebruikt en met toestemming van de Officier, is er niets mis mee, oordelen 's lands hoogste magistraten.

Stealth-sms'jes worden gebruikt om mensen met zelfmoordneigingen op te sporen. Dat kan ook makkelijk want de telefoontap die nodig is voor die stealth-sms'jes is "binnen een half uur geregeld".



Juridische vraag:
mogen de buren mijn huis fotograferen?

Vraag: Mijn buren fotograferen mijn tuin/huis/erf. Ze doen dit zogenaamd om bewijs te verzamelen omdat ik ruzie met ze heb. Maar ze doen het wel op rare momenten dus het voelt als pesten. Kan ik hier wat tegen doen? Is dit niet in strijd met de wet op de privacy?

Antwoord: Op zich is het legaal om huizen of erven te fotografe-ren, zolang je dat maar vanaf de openbare weg doet of vanaf een erf waar je met toestemming mag zijn. Er is geen portretrecht voor gebouwen.

Als je ménsen op de foto zet in huin huis of tuin, dan schend je mogelijk hun privacy. Zeker als je gaat publiceren moet je reke-ning houden met portretrecht. Dit recht zegt dat als mensen een redelijk belang kunnen aanvoeren tegen publicatie (bijvoorbeeld omdat het een evidente privésituatie was) je de foto niet mag publiceren.

Gebruik als bewijs, bijvoorbeeld bij de rechter of gemeente in een bezwaarprocedure, is eigenlijk altijd toegestaan. Je moet bewijs kunnen verzamelen van waar je klacht (of verweer tegen een klacht) over gaat. Natuurlijk mag zulk verzamelen van bewijs mensen niet hinderen, dus kies bij voorkeur een rustig moment en vermijd mensen op de foto tenzij dát essentieel is voor het bewijs.

Als je foto’s of films maakt als bewijs, is het natuurlijk niet de bedoeling dat dat vervolgens op Youtube verschijnt om je stand-punt nog eens kracht bij te zetten. Ook niet als je de procedure verliest en tóch vindt dat je gelijk hebt.

Recherche richt pijlen op cybercrime

De Landelijke Recherche concentreert zich op cybercrime, nu die vorm van misdaad 'zich snel ontwikkelt'.


INTERVIEW PAULISSEN

'Aanhoudingen zijn mooi, maar het aantal pogingen verminderen nog beter'

'Dader en slachtoffer zijn bij cybercrime nooit netjes op één plek bij elkaar'

'Het betalingsverkeer is verstoord geweest, maar niet in gevaar gekomen'

'De samenleving moet aan cybercrime wennen, net als aan fietsendiefstal'

Wilbert Paulissen vraagt om enig geduld bij het opsporen van internetcriminelen

CV

1962 Geboren te Eindhoven

1979-1983 Nederlandse politieacademie

1983-1994 Diverse functies bij de gemeentepolitie Eindhoven, waaronder hoofd centrale

Rob de Lange
Driebergen

In een kamer achteraf op het terrein van de KLPD in Driebergen huist de Electronic Crimes Taskforce (ECTF), ook wel het Bankenteam genaamd. Zo'n tien veiligheidsexperts van de grote Nederlandse banken, het OM en politie werken hier sinds 2011 eendrachtig samen in een verwoede poging het betalingsverkeer veilig te houden. Daar is alle reden voor, gezien het grote aantal storingen en digitale aanvallen die de financiële instellingen te verduren krijgen.

Het team is uiteindelijk de verant-

Ddos-aanvallen geen afleidingsmanoeuvre waren om op een andere plek in de bank toe te slaan, maar daar hebben we geen aanwijzingen voor gevonden. Het is vooral lastig. Consumenten kunnen een tijdje niet betalen.'

V Is dat niet te makkelijk? Stel ik ga tanken en van de tien keer doet de pomp het drie keer niet. Dat zouden we niet normaal vinden.

'Zo kijk ik er niet naar. Ik ben tevreden over de manier waarop de banken hun eigen betalingsverkeer monitoren. Ook weten ze steeds meer pogingen tot diefstal te onderscheppen, waardoor de schade niet toeneemt. Ze hebben natuurlijk ook een enorm belang om met ons samen te werken. Het gaat om grote bedragen.'

V Wat heeft het bankenteam de politie tot nu toe opgeleverd?

'Het schadebedrag is gedaald en het aantal onderzoeken is gestegen. Dankzij de samenwerking hebben we vijfduizend "geldezels" in beeld gekregen. Over het

"Als je bij de balie komt om aangifte te doen van een poging tot hacken, moet er wel iemand zitten die begrijpt waar het over gaat"

Cybercriminaliteit is "een zeer zorgelijke trend die zich snel aan het ontwikkelen is", zegt Wilbert Paulissen, hoofd Landelijke Recherche, in het FD. Tot een paar jaar geleden was cybercrime volgens hem alleen weggelegd voor mensen met veel technische kennis. Tegenwoordig zijn er ook veel leken die zich ermee bezighouden, doordat de benodigde software makkelijk verkrijgbaar is. Bovendien huren criminelen vaker professionele hulp in.

Bedrijfsproces

"Er zijn al jongeren die vaker het slachtoffer zijn geweest van cyber- dan van traditionele criminaliteit. Die verandering betekent voor de politie dat we ons echt op alle lagen van de organisatie moeten herorganiseren. Het moet onderdeel van ons bedrijfsproces worden. Als je bij de balie komt om aangifte te doen van een poging tot hacken, moet er wel iemand zitten die begrijpt waar het over gaat", aldus Paulissen in het FD.

Geldezels

Paulissen is tevreden over de samenwerking met de Nederlandse banken waardoor vijfduizend 'geldezels' in kaart zijn gebracht. "Kwetsbare jongeren, maar wel degelijk met verwijtbaar gedrag, die geronseld worden, soms gewoon op straat. Ze denken snel geld te kunnen verdienen door een korte tijd hun bankpas af te staan. Er wordt een paar keer een bepaald bedrag op die rekening overgemaakt en vervolgens contant gemaakt bij de pinautomaat."

Wetsvoorstel terughacken

Net als Paulissen zegt ook Nationaal coördinator Terrorisme en Veiligheid Dick Schoof in de krant te hopen dat de Tweede Kamer instemt met het wetsvoorstel waardoor de politie eenvoudiger computers mag binnendringen. "Het is de enige manier om bij de dader te komen. We hebben zulke opsporingsmethoden echt nodig." Hij signaleert ook een groei in het aantal bedrijven dat zich in Nederland toelegt op cybercrime, maar moeilijk is te traceren.

Grote obstakels voor anoniem internetmeldpunt

Het is een zeer lastige opgave om een anoniem internetmeldpunt te starten waarbij de anonimiteit van de melders wordt gegarandeerd. Dat laten onderzoekers van het Privacy & Identity Lab weten. Ze onderzochten de technische, juridische en organisatorische mogelijkheden van een anoniem meldpunt.

De onafhankelijke Stichting M. exploiteert sinds 2002 de meldlijn 'Meld Misdaad Anoniem', waar mensen anoniem via de telefoon informatie over misdrijven kunnen geven. De onderzoekers wilden kijken of een dergelijk meldpunt ook op internet is te realiseren. Daarnaast werd onderzocht wat de mogelijke voor- en nadelen van melden via internet zijn voor de hoeveelheid en kwaliteit van de meldingen.

Anonimiteit

Volgens de onderzoekers is er vanuit een technisch perspectief een duidelijk verschil tussen een internetmeldpunt en een telefonisch meldpunt. Ze merken op dat het vanwege het open karakter van het internet lastig is om de communicatie tussen melder en meldpunt anoniem te maken. Anonimimiseringssoftware zoals Tor kan hier in theorie tegen beschermen maar zou in de praktijk te complex zijn om voor de gemiddelde gebruiker te adviseren.

"Dat betekent dat de anonimiteit van de melder niet voldoende gegarandeerd kan worden. Daarnaast zal een gemiddelde gebruiker ongewild sporen achterlaten, en is ook de vernietiging van gegevens aan de kant van het meldpunt een punt van zorg", zo staat in het onderzoeksrapport. Van de verschillende oplossingsrichtingen waar de onderzoekers aan dachten zou een web-gebaseerde chat-toepassing of een smartphone-app nog het meest aan de gestelde eisen voldoen.

"Maar ook hier is de technische complexiteit hoog en is, zoals hierboven al gezegd, de garantie van anonimiteit sub-optimaal." De onderzoekers concluderen dat gezien de combinatie van technische, juridische en organisatorische mogelijkheden en obstakels voor de anonimiteit van meldingen via internet vooral de technische inrichting van een meldpunt dat de anonimiteit van de melder afdoende kan beschermen een uitdaging is.

Europol traint tientallen cybercops voor bestrijding cybercrime

In de maand juli zullen bijna 40 politieagenten uit 22 verschillende landen door Europol worden getraind in het voorkomen, detecteren en verstoren van cybercrime, waar zowel individuen en bedrijven als overheden en academici het doelwit van zijn.

De praktijktraining van de 'cybercops' volgt op een negen weken durend online lesprogramma. In totaal doen 37 agenten aan de training mee. "We hebben echte experts nodig om cybercriminelen te vinden, te identificeren en op te sporen", zegt Troels Oerting, hoofd van het Europees Cybercrime Centrum (EC3) van Europol. "We zijn misschien wat laat begonnen, maar leren snel en zullen hierin blijven investeren om ons deel te doen om het internet open en transparant maar ook veilig te houden."

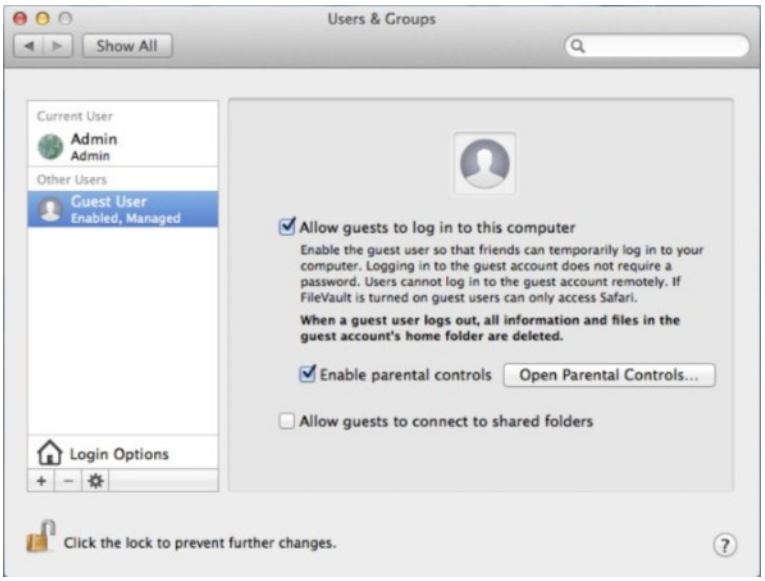
Zijn Macs altijd virusvrij?

Het antwoord op die vraag is niet zo eenduidig. Macs hebben inderdaad een sterke reputatie als het aankomt op virusveiligheid, daar valt niets tegenin te brengen. Een onbeveiligde Windowsmachine heeft een veel grotere kans om geïnfecteerd te raken dan een onbeschermde Mac.

Dat komt gedeeltelijk door het feit dat er simpelweg minder Macs op deze planeet staan dan Windowscomputers, waardoor criminelen meer geneigd zijn om malware te schrijven voor Windows. Het is namelijk zo dat een virus voor Windows geen enkel effect sorteert in OS X en omgekeerd, omdat de onderliggende structuur van beide besturingssystemen helemaal anders opgebouwd is. OS X is, net als Linux, gebaseerd op de Unix-architectuur, die met meer sandboxed compartimenten en gelaagde toestemmingen werkt dan Windows. Het is dus moeilijker voor malware om zich doorheen je volledige systeem te verspreiden. Al deze factoren maken van OS X een veiligere omgeving dan Windows – maar het is natuurlijk niet omdat je in een goede buurt woont, dat je je voordeur niet meer op slot hoeft te doen.

Ingebakken bescherming

Malware voor OS X is dan wel relatief zeldzaam, het bestaat wel degelijk. Gelukkig weet Apple dat ook en hebben ze de recentste iteraties van hun besturingssysteem uitgerust met een aantal nuttige beveiligingsfeatures.

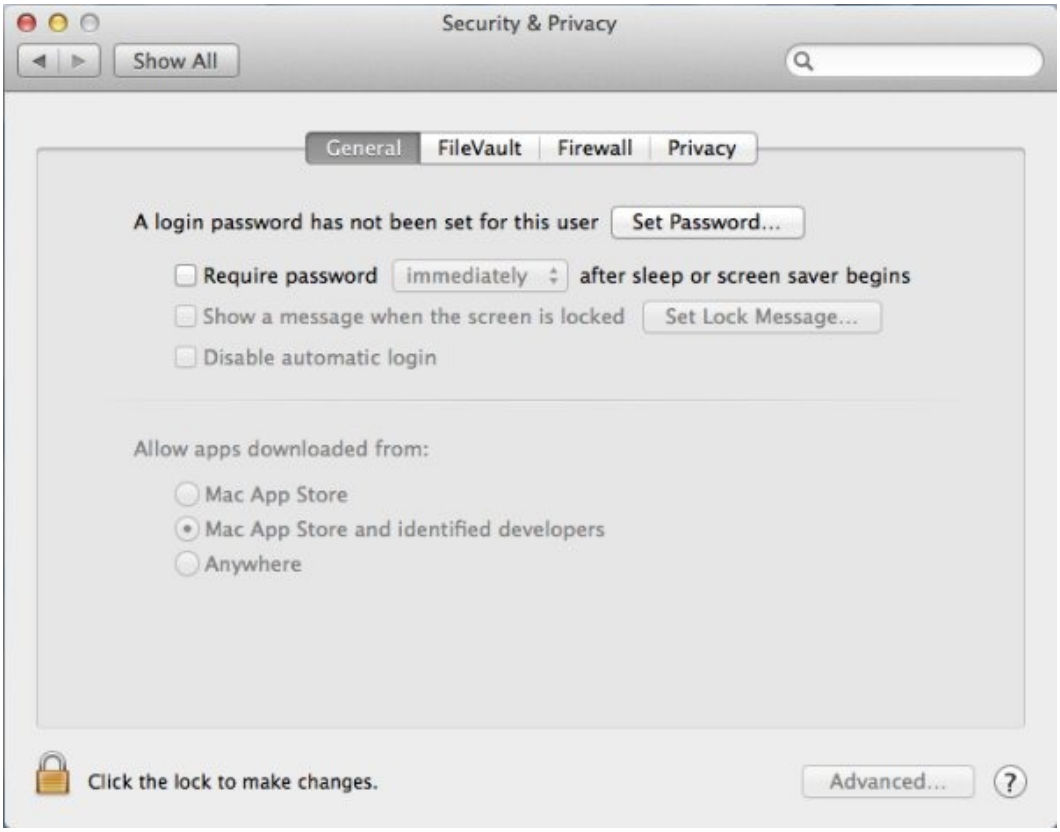


Zo heeft elke Mac sinds OS X 10.6 (Snow Leopard) een ingebouwde antivirus: File Quarantine. Die draait automatisch in de achtergrond en geeft je een waarschuwing als je een bestand downloadt dat geïnfecteerd is met een gekend stukje malware. File Quarantine is erg basic, maar het is wel efficiënt. De software werkt volledig automatisch, maar er zijn ook een aantal opties om je computer veiliger te maken die je zelf moet instellen.

Allereerst is het belangrijk dat je ervoor zorgt dat je apps, software en firmware up-to-date zijn. Sinds OS X 10.8 (Mountain Lion) vind je die updates in de Mac App Store; werk je nog met een oudere versie, dan vind je ze onder 'Software Update' in 'System Preferences' of in het Apple-menu. Denk er ook aan dat bepaalde externe software niet in deze lijst terechtkomt – zorg ervoor dat je ook die regelmatig updatet.

Een ander feature waar je gebruik van kan maken zijn de verschillende soorten gebruikers. In 'System Preferences' vind je een tabje 'Users & Groups', waar je bijvoorbeeld een aparte account met 'Parental Controls' kan aanmaken voor kinderen, zodat zij geen ongewenste bestanden kunnen downloaden. Als je je computer even door iemand anders wil laten gebruiken, kan je hen dat laten doen onder een 'Guest Account': alle bestanden en informatie die zij tijdens hun sessie aangemaakt hebben wordt dan verwijderd als ze weer uitloggen. Zo kan je in elk geval al niet besmet worden door derden.

De meeste veiligheidsopties vind je natuurlijk onder de categorie 'Security & Privacy'. Onder 'General' vind je de zogenaamde Gatekeeper: daarmee kan je aanduiden welke applicaties je wil toelaten. Standaard zal daar 'Mac App Store and identified developers' aangevinkt staan. Als je dan software downloadt van een niet door Apple erkende ontwikkelaar, zal je een waarschuwing krijgen. Die waarschuwing wil niet per definitie zeggen dat de software onbetrouwbaar is; het is echter wel een goede aanleiding om even na te kijken of je écht geen rommel binnenhaalt. Je kan de waarschuwing negeren door te control-klikken op de app en vervolgens 'Open' te kiezen. Je vindt hier ook de ingebouwde Firewall; die is ook eenvoudig en basic, maar net als de ingebouwde antivirusoplossing houdt hij de belangrijkste boosdoeners wel buiten. FileVault, tenslotte, laat je toe om je volledige interne (of externe) harde schijf te versleutelen. Dit maakt het uiteraard moeilijker voor eventuele malware en spyware – of dieven die je fysieke toestel in handen krijgen – om je data te lezen. FileVault heeft daarenboven geen of nauwelijks merkbare invloed op de prestaties van je systeem.



Een toevoeging in OS X 10.9 (Mavericks) is ook dat de ingebouwde wachtwoordmanager, Keychain, nu werkt via iCloud. Als je al een wachtwoordenoplossing van een derde partij gebruikt, kan je dit negeren, maar als je daar niet in wil investeren, moet je Keychain zeker bekijken. Met Keychain kan je je wachtwoorden en andere inloggegevens versleuteld bewaren en synchroniseren tussen je verschillende toestellen. Om Keychain in je iCloud te gebruiken, ga je in 'System Preferences' naar 'iCloud' en vink je daar 'Keychain' aan. Er verschijnt dan een wizard die je door het proces leidt.

Ook de ingebouwde browser, Safari, heeft een aantal nuttige features als je malware buiten de deur wil houden. Open via de menubalk de 'Settings' in Safari en navigeer naar 'Security'. Daar kan je kiezen of je gewaarschuwd wil worden als je een riskante website bezoekt en kan je pop-ups blokkeren. Als je zelf geen enkele plug-in gebruikt voor Safari, vink 'Allow Plug-ins' dan niet aan; dat zorgt ervoor dat websites of software geen ongewenste extraatjes kunnen installeren. Je hebt hier tenslotte ook nog de mogelijkheid om JavaScript te blokkeren; één van de manieren waarop Macs geïnfecteerd kunnen worden is namelijk via valse, besmette versies van Java of Flash. Je zal bij een nieuwe Mac ook merken dat Flash automatisch niet geïnstalleerd staat; als je beide plug-ins liefst volledig schuwt, dan kan dat.

Zo kies je een goede antivirus voor OS X

Als je besloten hebt dat je wel een antiviruspakket wil draaien op je Mac, dan zal je al snel vinden dat je meer dan genoeg keuze hebt – ondanks jaren geruchten dat Macs virusvrij zouden zijn, zijn de meeste gekende merken al een hele tijd geleden op de kar gesprongen. Net zoals bij Windows heb je de keuze tussen een aantal gratis en betalende pakketten, die allemaal hun eigen sterktes en zwaktes hebben.

Waar moet je specifiek op letten? De beste antiviruspakketten geven je de optie om zowel ondemand als gepland te scannen en om zowel het volledige systeem als specifieke bestanden te controleren. Je wil ook liefst een antivirus kiezen die je systeem zo min mogelijk belast terwijl hij draait in de achtergrond. Ook scannen de betere pakketten niet enkel je bestanden, maar ook websites en je mail. Ten slotte is het verstandig om voor een pakket te gaan dat zowel Windows- als Mac-gerichte malware tegenhoudt. Je Mac kan dan wel niet besmet worden door een Windows-virus, maar je kan het besmette bestand wel doorgeven aan een Windows-gebruiker. Twee van de meest populaire opties zijn Avast! Free Antivirus for Mac en het eveneens gratis Sophos Antivirus for Mac. Avast! biedt je een erg uitgebreid pakket features, terwijl Sophos dan weer een van de lichtste belastingen op je systeem oplevert.

Conclusie: moet je een antivirus installeren?

Het antwoord op die vraag is voor het grootste deel afhankelijk van de manier waarop jij jouw Mac gebruikt. Is het een privémachine, die je nooit of zelden voor je werk gebruikt, dan kom je er naar alle waarschijnlijkheid mee weg om geen antivirussoftware te installeren. Volg de tips die ik hierboven uiteenzette, gebruik je gezond verstand als het op verdachte e-mails en dergelijke aankomt, neem backups, en de kans dat je Apple-toestel geïnfecteerd raakt is minuscuul. Een aantal antivirusfirma's stellen dat ze elke dag grofweg 65.000 nieuwe virusvarianten tegenkomen voor Windows; voor OS X zijn dat er een handvol per jaar. Is het een risico? Uiteraard – maar in het geval van virussen voor Mac is het, mijns inziens, een aanvaardbaar klein risico.

Als je Mac echter je werkcomputer is of als er op jouw kantoor gewerkt wordt met een gemengde vloot computers – Mac en Windows door elkaar – dan kan het verstandig zijn om toch te investeren in een goede antivirusoplossing. Hetzelfde geldt voor al wie vaak omgaat met gevoelige of waardevolle data. Ook hier zijn de cijfers nog steeds in jouw voordeel, maar als je veel te verliezen hebt is het motto 'better safe than sorry' altijd van toepassing.

Hoe veilig is de cloud?

Wie heeft toegang tot de servers waarop uw gegevens staan? En hoe kiest u een 'veilige' cloudprovider?

De dagen dat je al je foto's, documenten, muziek en filmpjes op je eigen harde schijf bewaarde, liggen stilaan achter ons. Heel veel pc-gebruikers hebben tegenwoordig een (al dan niet betalend) abonnement op clouddiensten als Dropbox, Google Drive of iCloud. En waarom ook niet? Het is gemakkelijk, je kan overal aan je bestanden en je hoeft je geen zorgen te maken dat je harde schijf vol loopt. Als je meer plaats nodig hebt, neem je gewoon een duurder abonnement.

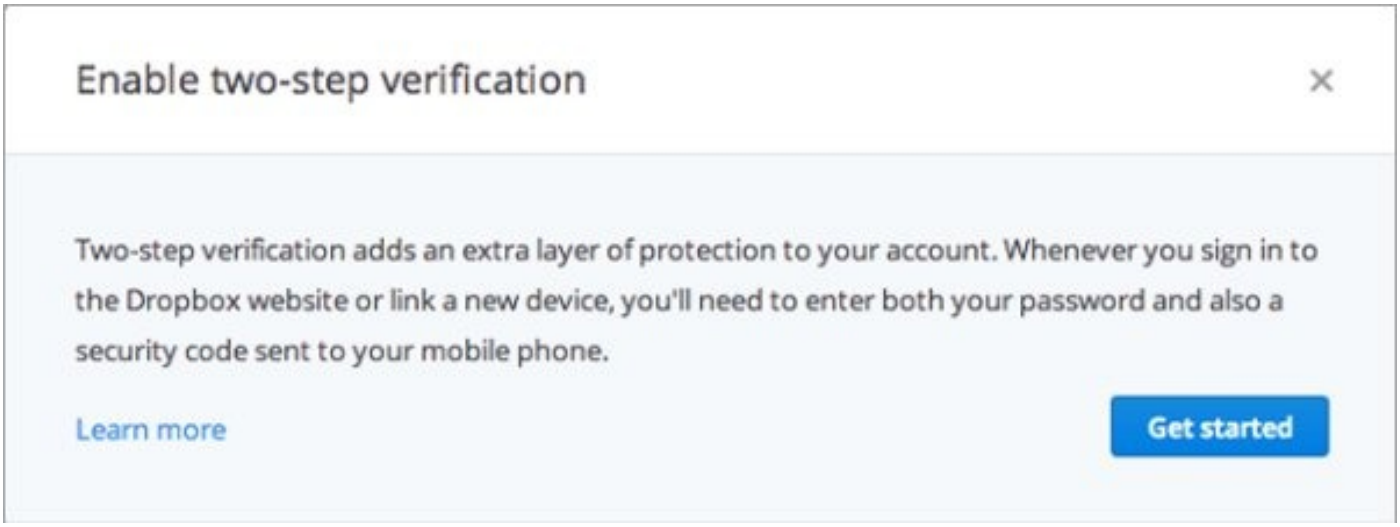
In de keuze voor een cloudprovider geven zaken als het aantal megabyte dat je gratis krijgt, de prijs voor een betalend abonnement en het aantal apps dat beschikbaar is voor mobiele apparaten meestal nog de doorslag. De veiligheid van de bestanden wordt veel minder vaak in overweging genomen. En dat is jammer. Want hoe je het ook draait of keert, als je data naar de cloud stuurt, geef je al je gegevens in handen van iemand anders. Hoe en waar ze opgeslagen en beveiligd worden of wat er daarna mee gebeurt, daar heb jij niets meer over te beslissen en dat is toch een serieuze sprong in het donker.

Fysieke toegang

Uiteraard beweren alle cloudproviders bij hoog en bij laag dat je data bij hen in veilige handen is. Vaak is dat ook wel zo, maar "veiligheid" is een heel veelzijdig begrip. Wie dus echt heel gevoelige of bedrijfskritieke data naar de cloud stuurt en absoluut zeker wil zijn dat niemand daar aan kan, moet dan ook heel wat zaken in overweging nemen bij zijn keuze voor een provider.

Zo is er de fysieke toegang tot de datacenters. Amazon bijvoorbeeld (dat onder andere een groot deel van de infrastructuur levert voor Dropbox) gaat er prat op dat zijn datacenters op haast militaire wijze beveiligd worden. De centers zelf huizen in anonieme gebouwen zonder enige verwijzing naar Amazon en hangen tjokvol camera's. Externe bewakingsfirma's controleren verschillende malen alle personeelsleden alvorens ze toegang krijgen tot de werkvloer. Alle toegang wordt ook uitvoerig gelogd en regelmatig nagekeken. Dat klinkt allemaal prima, maar als individuele gebruiker is dit natuurlijk haast onmogelijk te controleren. Hier komt dus, alweer, een stuk vertrouwen bij kijken.

Daarnaast is het natuurlijk ook belangrijk om te weten hoe goed je data geback-upt wordt. Van een serieuze cloudprovider mag je verwachten dat hij verschillende, redundante kopieën van je data op verschillende fysieke locaties bewaart. Als alles op dezelfde plaats staat en de boel brandt af of loopt onder water, dan sta je immers net even ver als wanneer er helemaal geen back-up was.



Veilig, veiliger, veiligst

De manier waarop je data naar je provider stuurt, moet uiteraard ook beveiligd worden, zo niet is er een kans dat hackers je gegevens onderweg onderscheppen. Let er dus op dat je webverbinding versleuteld is. Dat kan je zien door de https voor het webadres, de "s" duidt er op dat je een beveiligde http-verbinding hebt. Als je een apart programma gebruikt om met je cloudprovider te communiceren, kijk je best even na of deze ook een versleuteling gebruikt; bij de meeste cloudproviders is dat zo.

Wil je nog meer veiligheid, ga dan in zee met een provider die voorziet in tweestapsverificatie. Daarbij moet je niet alleen je gebruikersnaam en je wachtwoord intikken, maar ook een steeds wisselende code die bijvoorbeeld via sms naar je gsm gestuurd wordt of die gegenereerd wordt met een speciale app. Zelfs als je wachtwoord dan op straat ligt, kan er nog niet ingelogd worden zonder de code in te geven.

Natuurlijk gelden in dit geval ook alle regels wat betreft het kiezen van een goed wachtwoord. Gebruik geen wachtwoord dat gemakkelijk te raden valt zoals de naam van je hond, je geboortedatum of, nog erger, 1 2 3 4. Zelfs een echt woord ("taartbeslag", "kanonskogel" of "landbouwmachine") is geen goed idee. Hackers gebruiken immers alfabetische lijsten met woorden die stuk voor stuk ingetikt worden tot ze beet hebben. Beter is om een willekeurige reeks van letters, cijfers en leestekens te gebruiken die geen enkele betekenis heeft, zoiets als "Ki5ps4!X0&$" dus. Ja, deze zijn inderdaad een stuk moeilijker te memoriseren, maar wel veel veiliger.

I know nothing...

Het probleem met wachtwoorden is dat de meeste cloudproviders deze lokaal opslaan en lokaal versleutelen. Dat wil zeggen dat de sleutels om de wachtwoorden terug tevoorschijn te halen, in het bezit zijn van de provider. Werknemers die het niet goed menen of slimme hackers zouden in theorie dus die sleutels kunnen aanwenden om je data in te kijken.

Enkele cloudproviders zijn daarom beginnen te werken via het zogenaamde "zero knowledge"-principe. Hierbij gebeurt de volledige versleuteling van de data die je doorstuurt op je eigen computer. De cloudprovider ziet enkel een hoop nullen en enen in zijn datacenter verschijnen die hij niet kan uitlezen. Hij weet zelfs niet over welke bestandstypen het gaat of hoe de bestanden heten. Providers die deze dienst aanbieden, zijn onder meer Wuala en SpiderOak. Let wel: als je bij hen je wachtwoord vergeet, is er geen enkele manier om je data weer op te vissen…

Uncle Sam leest mee (maar Europa doet niet veel beter)

Toen George W. Bush in oktober 2001 de zogenaamde Patriot Act invoerde, had hij waarschijnlijk geen idee dat deze wet meer dan tien jaar later nog een serieuze invloed zou hebben op de wereld van de datacenters en cloud computing. De wet werd meteen ingevoerd na de aanval op de Twin Towers in New York en moest een krachtig wapen worden in Bush's War on Terrorism. Om helemaal de puntjes op de i te zetten: de Patriot Act was eigenlijk zelfs geen echte wet op zich, maar versterkte en breidde bestaande wetten uit die al jarenlang in voege waren in de V.S.

Het eindresultaat is echter ontegensprekelijk dat de Amerikaanse overheid verregaande bevoegdheden heeft om informatie te verzamelen over iedereen die zij verdacht vindt, inclusief informatie die op servers en netwerken staat. De Amerikaanse bedrijven die deze netwerken beheren, moeten aan deze onderzoeken meewerken en zijn dus, op eenvoudig verzoek, verplicht om bijvoorbeeld opgeslagen data over te dragen aan Justitie. Het opmerkelijke is dat deze wet hoegenaamd geen rekening houdt met landsgrenzen. Ze geldt voor buitenlandse bedrijven in Amerika, maar ook voor Amerikaanse dochterbedrijven in andere landen. Een Iers, Japans of Braziliaans filiaal van Google of Microsoft valt evenzeer onder de Patriot Act als het lokale Google-filiaal in San Francisco of New York.

Voor veel Aziatische en Europese ondernemingen die gevoelige informatie willen opslaan, is dit een brug te ver. De roep om een "pure" Europese cloud wordt dan ook steeds luider. Sommige bedrijven proberen uit die onvrede ook al commerciële garen te spinnen. Een bedrijf als Belgacom bijvoorbeeld laat het niet na om expliciet te vermelden dat de dataservers van haar clouddiensten in Europa staan en niet in de Verenigde Staten.

Dit kan echter een vals gevoel van veiligheid geven: ook Europese landen als het Verenigd Koninkrijk, Frankrijk en Spanje beschikken immers, naast strenge privacywetten, over een uitgebreide antiterrorismewetgeving met bevoegdheden die echt niet zo ver van die van Uncle Sam liggen. Het Duitse BKA (het BundesKriminalAmt, zeg maar het "Duitse FBI") heeft bijvoorbeeld het recht om in bepaalde gevallen virussen op de servers van cloudproviders los te laten om bepaalde klanten in de gaten te houden. De zogenaamde G-10-wet laat de Duitse veiligheidsdiensten dan weer toe om zonder gerechtelijk bevel alle telecommunicatie van bepaalde personen af te luisteren wanneer deze verdacht worden van bijvoorbeeld terrorisme.

Copy: Het veilige alternatief voor Dropbox en OneDrive

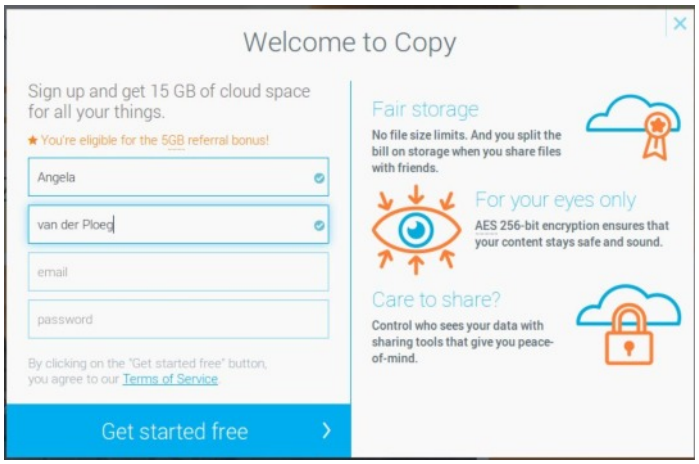
Copy is net zo'n clouddienst als Dropbox en OneDrive. Niets nieuws onder de zon, of toch wel? Copy heeft samenwerken en veiligheid als speerpunten. Ook de gratis 15 GB opslagruimte maakt Copy bijzonder interessant. Via de website kun je met elke computer (Windows, Mac en Linux) bij je bestanden komen. Gewoon inloggen en je kunt er bij.

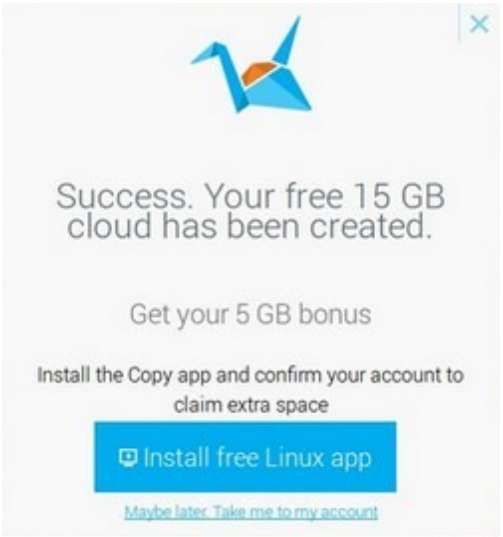
Er zijn ook apps voor smartphones en tablets. Delen is eenvoudig. Je hebt twee keuzes. 'Public' waarbij je een linkje verstuurd dat door iedereen geopend kan worden. En 'Secure' waarbij je bestand alleen geopend kan worden indien de ander ook inlogt op zijn/haar Copy.com-account.

Zijn je bestanden veilig bij Copy.com? Je wil natuurlijk niet dat andere mensen ongevraagd jouw bestanden inzien. Copy.com versleuteld je bestanden (o.a. AES 256 encryptie). Normaal gesproken is dat meer dan voldoende. Natuurlijk weet je dat de overheid wel je bestanden zou kunnen inzien als men dat echt zou willen, maar dat is eigenlijk bij elke online opslagdienst het geval.

Stap 1: Copy registreren

Copy is er voor Windows, Mac, Linux en alle bekende smartphone- platformen. Surf naar http://www.copy.com en download het programma. Met Create maak je de eerste keer een nieuw account/registratie aan.





Is alles goed ingevuld en het account is aan gemaakt, krijg je daarna het volgende te zien (zie plaatje links). Let wel, je krijgt via de mail nog wel eerst een link die je moet gebruiken om je account te verifiëren. Wanneer je de Copy app installeert krijg je 5 GB extra ruimte. Je kan anderen ook via e-mail uitnodigen om Copy te gaan gebruiken; je krijgt dan allebei 5 GB extra wanneer men jouw link gebruikt om zich te registreren.

Copy maakt net als Dropbox en OneDrive een aparte map aan op je computer. In dit geval heet de map Copy. Je vindt het onder Favorieten in de Windows Verkenner (Dit betreft Windowsgebruikers. Bij punt 5 kan je lezen hoe je Copy op een Linux computer kunt installeren). Je kunt de map ook openen door te dubbelklikken op het Copy-icoontje in je systeemvak.

Stap 2: Delen

Alles wat je in de map Copy bewaart is automatisch beschikbaar op alle apparaten en computers waarop je Copy geïnstalleerd hebt. Heb je geen eigen computer of smartphone bij de hand? Ook via de website van de dienst kun je bij je bestanden.

Surf naar http://www.copy.com, meld je aan en je kunt zo door je bestanden bladeren. Copy biedt meerdere manieren om bestanden te delen. Open de map Copy in de Windows Verkenner. Klik met de rechtermuisknop op een bestand of map die je wil delen en kijk in het menu Copy actions. Met Send public link kun je een link versturen. Iedereen met deze link kan het bestand (of de map) downloaden. Hiermee gebruik je Copy als een vervanger van online bestandskoeriers als WeTransfer.

Stap 3: Samenwerken en geschiedenis

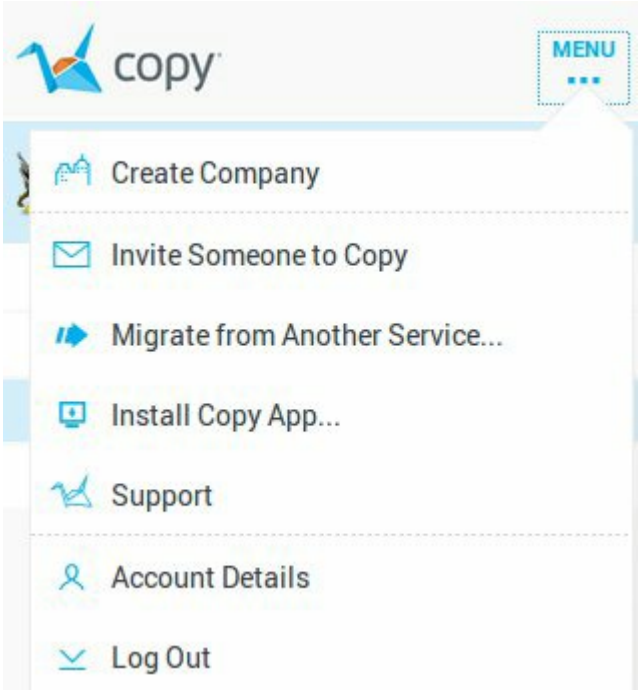
Als je in het menu Copy actions kiest voor Share, kun je de map of het bestand delen met andere gebruikers van de Copy-dienst. Op deze manier kun je bijvoorbeeld echt samenwerken aan bestanden. Alle gebruikers beschikken altijd over de meest recente versie van bestanden in de gedeelde map.

Copy heeft een professioneel karakter en is een goed alternatief voor Dropbox en OneDrive.

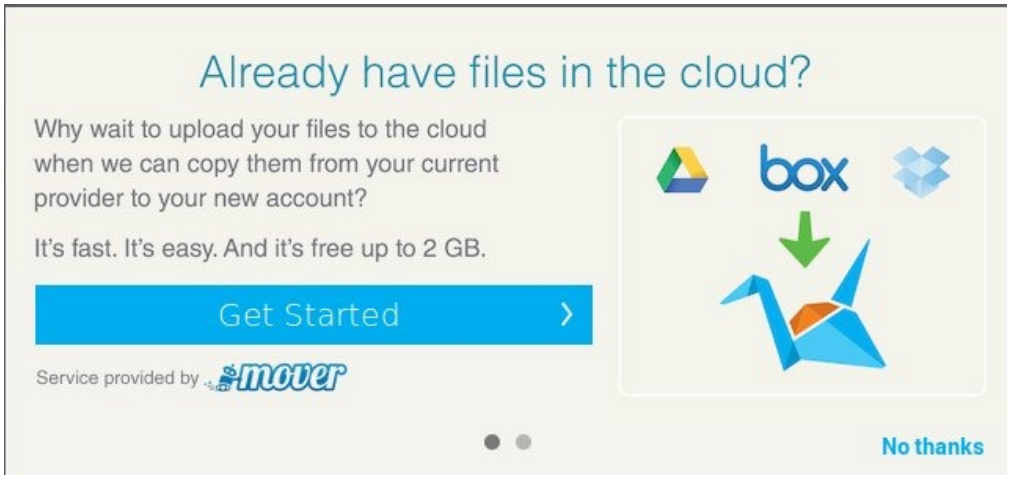
Het menu Copy actions biedt naast de opties om bestanden of mappen te delen, nog een andere interessante optie: bestandsgeschiedenis. Het menu toont de meest recente versies van een bestand. Zo zie je precies wie er aan een bestand heeft gewerkt. Dit is handig wanneer je samenwerkt aan een project, maar ook wanneer je een bestand alleen zelf gebruikt. Dankzij deze optie behoort het per ongeluk overschrijven van een document tot de het verleden. Je kunt namelijk oudere versies bekijken en herstellen via Copy actions / History.

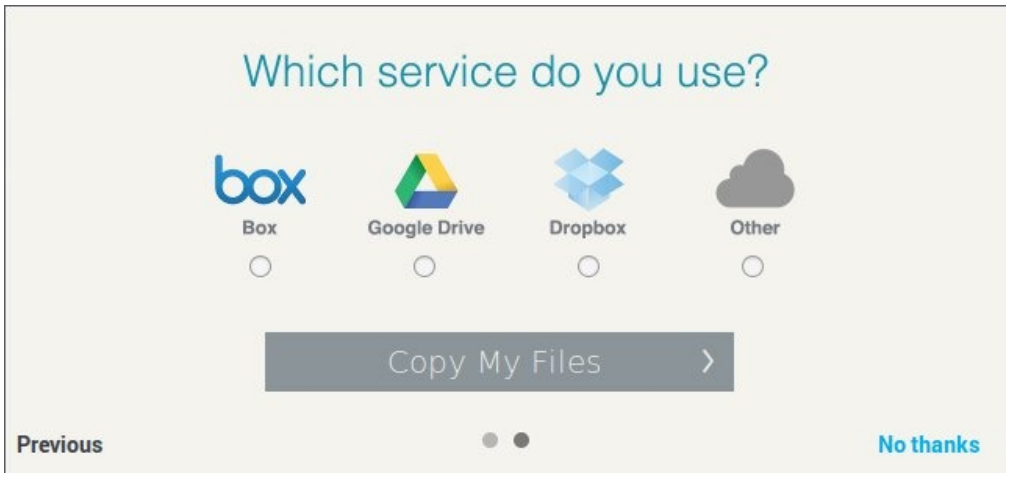
Stap 4: Importeren vanaf een andere cloud

Wanneer je al een andere cloud in gebruik hebt waar files op staan, kan je deze via het menu Migrate naar Copy importeren.



Klik dus op Migrate from Another Service...en doorloop de procedure.





Het menu heeft verder nog andere zaken, waaronder uitnodigen van anderen om Copy te gaan gebruiken, je accountgegevens, support en je kan hier de Copy App installeren.

Dreiging jihadisten door sociale media groter dan ooit

Volgens een nieuw rapport van de AIVD is de potentiële dreiging van jihadisten tegen de Nederlandse democratische rechtsorde en samenleving, 'groter dan ooit tevoren'.

De slagkracht van jihadi's is groot en de aanzuigende werking, vooral dankzij internet, zo extreem groot dat 'vele moslimjongeren in korte tijd van meelopende sympathisanten uitgroeien tot keiharde strijders'.

De AIVD vreest voor aanslagen en noemt het tekenend dat moslims in Nederland die zich openlijk verzetten tegen jihadisme 'steeds vaker virtueel en fysiek worden geïntimideerd'.

Tegen de jihadistische beweging valt ook nauwelijks op te treden, aldus het rapport, omdat het 'amper sprake is van centrale leiders'. De radicalisering is vooral door sociale media 'tot hoog tempo opgestuwd' – helemaal 2.0, iedereen is met iedereen in contact maar ook verstopt in the crowd.

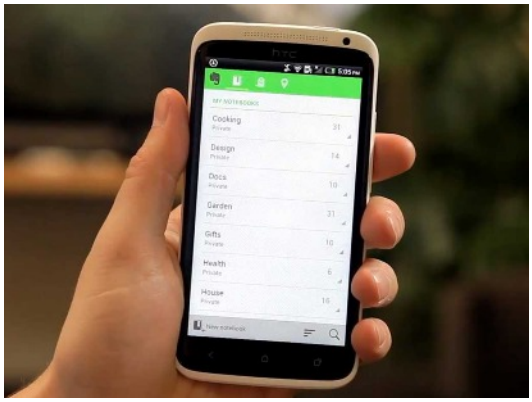
Het rapport noemt het misbruik van sociale media de voornaamste succesfactor in de groei van het aantal jihadi's. Jihadpropaganda is 'in elke vorm en elke taal' te vinden. 'Het is steeds professioneler en daardoor aantrekkelijker vormgegeven'.

Zo heeft het 'groepje jihadisten achter website De Ware Religie inmiddels meerdere jihadistische websites, Twitter- en Facebookaccounts opgericht'. Deze 'regisseurs op de achtergrond' zijn 24/7 online actief. Ze wanen zich onaantastbaar, gezien de vele vrijspraken in rechtszaken. Een uitgereisde jihadist twitterde de AIVD 'de groeten uit Syrië'. Hij schreef 'jarenlang intensief gemonitord, 4x teruggestuurd en nu pepsi drinkend in Syrië?

Wat is er misgegaan?' De AIVD stelt een 'deltaplan tegen jihadisme' voor, met nieuwe preventieve en repressieve maatregelen die de diverse overheidspartners 'in samenhang en onderlinge coördinatie moeten ontwikkelen en doorvoeren'.

Android-telefoon wissen verwijdert persoonlijke data niet

Verkoop of doneer je een oudere Android-telefoon? Let dan op: de standaardtools doen je persoonlijke data en gênante selfies niet onherroepelijk verdwijnen.



Een recente studie van beveiligingssoftwarebouwer Avast trekt de efficiëntie van Androids factory reset-functie in twijfel. Juist, de functie waar de meeste gebruikers op vertrouwen om hun persoonlijke data te verwijderen voor ze een telefoon verkopen of weggeven.

Avast kocht voor het onderzoek twintig Android-smartphones via eBay, waar je op elk moment zo'n tachtigduizend tweedehands smartphones te koop vindt.

Wat vonden de medewerkers op die toestellen? Onder andere zo'n veertigduizend foto's – inclusief 250 naakt-selfies van mannen – 750 e-mails en sms-berichten, 250 contacten, de identiteit van vier van de ex-telefooneigenaars, en één ingevulde aanvraag voor een lening.

Jude McColgan van Avasts mobiele divisie is ervan overtuigd dat mensen nog steeds niet gewend zijn aan de mogelijke implicaties van alle persoonlijke data die we op onze smartphones bewaren.

"Gebruikers dachten dat ze hun toestel volledig schoonveegden en de fabrieksinstellingen herstelden", zei hij, maar die factory reinstall wist je toestel "alleen op het niveau van de applicaties".

Avast hoefde bovendien geen al te gekke kunstjes uithalen om de data terug te vinden, zegt McColgan. Zijn team gebruikte generische, publiek te verkrijgen software voor digitale forensics, zoals FTK Imager.

"Op het eerste gezicht zien de telefoons er dan wel grondig gewist uit, maar we haalden al snel een berg privégegevens boven. In de meeste gevallen konden we ook sms'en en chatberichten terughalen", schrijven Avast-onderzoekers Jaromir Horejsi en David Fiser in het rapport.

Avast legt er natuurlijk graag de nadruk op dat zijn eigen beveiligings-app voor Android een verwijdertool aan boord heeft die zijn werk beter doet dan de ingebouwde reset.

Snapshots:

Publieke computers gebruiken voor werk, mail en financiën is buitengewoon riskant. Ook hotel-pc's liggen in de hinderlaag, waarschuwt de geheime dienst.

Publieke wifi zonder VPN is onverstandig, maar zomaar een publieke computer gebruiken voor meer dan alleen surfen is echt vragen om problemen. Dat blijkt eens te meer uit verschillende incidenten waarbij hotel-pc's door criminelen waren voorzien van malware, zoals keyloggers. Hierdoor kregen ze de logins, wachtwoorden, bank- en creditcardgegevens van talloze (zakelijke) reizigers te pakken.

Alleen met 'draagbaar' OS

De cybercrimetak van de Secret Service waarschuwt nu in een uitgelekte memo aan de hotelbranche om alle pc's die ze beschikbaar stellen aan gasten grondig te controleren op malware, meldt Krebs on Security.

Daarnaast volgt basaal beheeradvies zodat gasten geen adminrechten kunnen krijgen, maar dat zal cybercriminelen niet stoppen, constateert Krebs. Het advies is dan ook: blijf weg van publieke pc's, tenzij je als gast een eigen, tijdelijk en schoon besturingssysteem kunt draaien met een usb-stick of cd-rom.

—----------

Na de drugs- en de bomhond is er nu de gadgethond, door de politie ingezet om verborgen kinderpornobestanden te vinden.

In de strijd tegen makers en verspreiders van kinderporno worden nu speurhonden ingezet. Zo vind de labrador Thoreau feilloos uiteenlopende digitale dragers, ook al zijn deze in plastic verpakt ergens diep in een verborgen la of in het plafond, meldt The Providence uit de Amerikaanse staat Rhode Island.

De hond heeft 22 weken training gehad, en pikt harddisks, usb-sticks en andere geheugenkaarten en gadgets er zo uit. Hij wordt beloont met voer. "Zo krijgt hij elke dag z'n eten," aldus zijn baasje Adam Houston. Het is niet duidelijk of Thoreau ook gebrande cd's en dvd's kan opsporen.

Vaak zijn kinderpornobestanden goed versleuteld, daar kan de hond geen uitkomst bieden. In sommige landen kunnen verdachten worden gedwongen om hun wachtwoord voor dergelijke encryptie af te geven. Die decryptieplicht wil Justitie in Nederland ook invoeren, ondanks veel kritiek, onder meer van rechters.

—----------

Op 1 september start in Den Haag een nieuwe Europese cybercrime taskforce die zich met de bestrijding van cybercriminelen gaat bezighouden. De Joint Cybercrime Action Taskforce (J-CAT) zal zich voornamelijk op botnets, banking Trojans en het 'darknet' gaan richten.

Andy Archibald van de Britse National Cyber Crime Unit (NCCU) zal de nieuwe taksforce leiden, aangevuld met personeel van het Europese Cybercrime Centrum (EC3), de FBI, het Britse National Crime Agency en het Duitse Bundeskriminalamt (BKA). Politieonderzoekers uit verschillende Europese landen zullen permanent in het centrum verblijven en zich met onderzoeken bezighouden.

Het gaat vooralsnog om een pilot die zes maanden duurt en door de European Cybercrime Task Force (EUCTF) van de Europese Unie zal worden gemonitord. De EUCTF bestaat uit de hoofden van verschillende cybercrime-eenheden van de EU-lidstaten, alsmede Europol, Eurojust en de Europese Commissie.

Volgens Paul Gillen, hoofd operaties bij het EC3, is het vooral als oefening bedoeld. "Hoe vaker je iets oefent, des te beter, en gelukkiger, je erin wordt", zo laat hij tegenover SC Magazine weten. Als de pilot succesvol is zullen uiteindelijk onderzoekers van alle 28 lidstaten een plek bij de taskforce kunnen krijgen. "We hebben op het moment niet teveel regels, problemen die we tegenkomen zullen we onderweg oplossen", besluit Gillen.

Cops in Cyberspace blog

Per deze maandis in Nederland de Joint Sigint Cyber Unit (JSCU) operationeel. Dit samenwerkingsverband tussen AIVD en MIVD gaat aan de slag met 'signals intelligence': in het digitale domein inlichtingen vergaren, aanvallen uitvoeren en cybercrime bestrijden. Concreet: de JSCU richt zich op hacken, data-analyse, het inzetten van malware en onderscheppen van digitale gegevens bij digitale aanvallen en het uitschakelen van vijandige militaire doelen.

Anoniem iets melden op internet? Kan niet, stellen onderzoekers van het Privacy & Identity Lab en de Radboud Universiteit. Technisch is die anonimiteit niet te waarborgen: het is 'technisch moeilijk uitvoerbaar, organisatorisch een uitdaging en er zijn mogelijke schadelijke neveneffecten'. De onderzoekers deden een quickscan in opdracht van het ministerie van VenJ en keken naar de haalbaarheid van een anoniem internetmeldpunt. Dat blijkt dus niet zo simpel, 'in een klimaat waarin politiebestanden op tamelijk intransparante wijze ook voor andere doeleinden dan opsporing worden ingezet'. Dan zeker moet je terughoudend zijn 'met het voeden van dergelijke databanken met ongecontroleerde informatie' en voorzichtig met het faciliteren van anonieme meldingen.

De rechtbank in Assen heeft Frank R. (49, uit Cuijk) veroordeeld tot zes jaar celstraf plus tbs. R. stond terecht voor 21 zedendelicten, waaronder grooming, verkrachting, ontucht en het maken/bezitten van kinderporno. De verdachte deed zich voor als 18-jarige, en wist zo, 'willens en wetens', vermoedelijk honderden minderjarige meisjes voor de webcam te verleiden tot het plegen van seksuele handelingen. Deze handelingen waren in de helft van het totale aantal tenlasteleggingen in 'aard en omvang niet passend' bij de leeftijden van de meisjes. In enkele gevallen kwam het ook tot fysieke ontmoetingen, waarbij de seks 'extreem was en steeds extremer werd'. Volgens onderzoekers was de verdachte 'sociaal incompetent' en ontwikkelde hij een steeds sterkere voorkeur voor extreme en dominante seks met jonge meisjes van 12 of 13. Tegen hem was tien jaar geëist maar de rechtbank vond niet alle aanklachten bewezen. Waar het OM aanvankelijk sprak over 'mogelijk honderden slachtoffers' waren slechts 21 zaken in de dagvaarding vermeld. De rechter heeft veel slachtoffers verder een schadevergoeding toegewezen.

Een telefoon is een telefoon, maar een smartphone? Da's veel meer dan een telefoon. De PvdA wil dat de politie voortaan alleen na toestemming van de rechter-commissaris onderzoek doet naar bestanden op de smartphone van een verdachte. Kamerlid Jeroen Recourt ziet de mobiel als een huis – alleen te doorzoeken met een huiszoekingsbevel. Recourt wil het wetboek van strafvordering 'bij de tijd brengen'. Hij verwijst naar de VS waar het Hooggerechtshof onlangs unaniem oordeelde dat een telefoon tegenwoordig meer is dan een communicatiemiddel. Dat daarom dus beter beschermd moet worden.

Een foto online zetten? Prima, maar niet een foto van je rijbewijs of id-kaart, waarschuwt de politie. Steeds vaker blijken mensen een fotootje te maken van hun pasgehaalde rijbewijs en dat op facebook of twitter te zetten. En dat lokt identiteitsfraudeurs, die de gegevens op de foto perfect kunnen gebruiken voor nepdocumenten. 'Meestal is het zo dat je er pas veel later achter komt dat je slachtoffer bent van identiteitsfraude, omdat de rekeningen pas later binnenkomen.'

Op internet is een Nederlandstalige jihadistische video opgedoken. In de film Oh Oh Aleppo – De Spookstad, die een half uur duurt, komen naar verluidt 'Nederlandse mujahideen' aan het woord. Ze vertellen hoe het is om in Syrië te strijden. De film werd bekend toen de website De Ware Religie ernaar verwees op haar facebookpagina. Volgens NCTV Dick Schoof wordt op De Ware Religie het jihadistisch gedachtegoed gepromoot en steunt de site de soennitische jihadisten van ISIS. Schoof heeft de provider waar De Ware Religie gehost gevraagd de site te verwijderen. Hij gaf echter ook aan strafrechtelijk niets te kunnen ondernemen, dat is een taak van het OM.