Nieuwsbrief 7/8 (vakantie editie) -2012

W.Bosgra Taakaccenthouder digitale criminaliteit

Digitale nieuwsbrief verzorgd door Secure Computing.

Doel is bewustwording van wat u doet met de computer en kennis opdoen voor de opsporing van strafbare feiten gepleegd middels de computer. U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Deze nieuwsbrief zal met enige regelmaat in uw mailbox verschijnen.

Middels deze nieuwsbrief houden wij u op de hoogte van:

- Onderwerpen die betrekking hebben op het veilig gebruik van de computer en het internet
- Nieuws uit de media
- Juridische vragen
- Nieuwe technieken
- Vele andere wetenswaardigheden

Deze editie wijkt wat af van de overige. Dit keer is gekozen voor interessant leesvoer, voornamelijk omtrent social media. Lokfiets, lokauto, …lokpuber?! Facebookgebruiker? Chat u ook via Facebook? Heeft u een smartphone? Wilt u van uw Facebook-, Twitter- of Linkedinaccount af? Lees dan zeker verder.

Gaat u op vakantie? Print 'm uit en neem 'm mee.

Facebook : nieuwe tactiek om een verblijfsvergunning te krijgen

Volgens Noyan Sahami, freelance tolk/vertaler bij de IND, heb je voor een verblijfsvergunning in Nederland niet meer nodig dan een facebookpagina, een willekeurige imam en een journalist die graag eens over Iran wil schrijven. Sahami zegt in zijn werk vele Iraanse asielzoekers te zien die op een regulier visum naar Nederland komen maar niet meer terug willen. Probleempje: geen vluchtelingenstatus. Maar dat is te regelen, schrijft Sahami. Je opent een facebookpagina, je kiest een heilige imam, je plaatst wat beledigende teksten, paar foto's erbij. Je zorgt dat veel mensen je pagina 'liken' en je zoekt publiciteit, liefst een journalist die over je schrijft en een foto van je plaatst. Omdat het Vluchtelingengedrag in dit soort gevallen bescherming biedt, heb je een 'aantoonbare vervolgingsgrond' gecreëerd voor het bemachtingen van een vluchtelingenstatus. Sahami reageert op een artikel over een in Nederland woonachtige Iraniër wiens vader in Iran gearresteerd zou zijn wegens een door zoonlief aangemaakte Facebookpagina. Volgens Sahami wordt op deze manier het Nederlandse vluchtelingenbeleid doorkruist en het Vluchtelingenverdrag misbruikt. 'Er is geen enkel verifieerbaar bewijs van een onafhankelijke bron dat de vader van de betrokken persoon vanwege de door hem aangemaakte Facebookpagina in Iran is aangehouden.' En dus kan iedereen 'met een vestigingsambitie in Nederland' op deze manier een verblijfsvergunning 'afdwingen'.

Facebook scant chatconversaties van gebruikers

Het moet niet gekker worden, met dat facebook. Na de ophef over gebruikersnamen is nu bekend geworden dat facebook chatgesprekken geautomatiseerd afluistert en scant op 'criminele inhoud'. De reden? Bescherming van minderjarigen, zegt de chef beveiliging van facebook, Joe Sullivan. Volgens hem kijkt de afluistersoftware onder meer naar de relatie tussen twee facebookers die berichten met elkaar uitwisselen. Daarbij worden conversaties vergeleken met echte chats van veroordeelde seksdelinquenten en wordt speciaal gekeken naar chats tussen mensen die geen duidelijke relatie met elkaar hebben of die nauwelijks gezamenlijke vrienden hebben. Personeel van facebook zou de chats niet actief bekijken, zegt Sullivan, maar alleen als de scanner aanslaat. Onlangs werd zo een chat tussen een 13-jarig meisje uit California en een man van begin dertig gemonitord. De twee hadden een afspraakje gemaakt maar de politie was al gealarmeerd en de man werd aangehouden. Het maar de vraag of het echt zo werkt: opsporingsambtenaren hebben al aangegeven dat op elke betrapte er tien doorheen glippen.

Lokpuber ontmaskert pedofiel in chatbox

Er loopt een rechtszaak tegen een man (37, uit Leiden) die via internet een minderjarige had benaderd voor seks. De man, organisator van jazzevenementen, werd begin 2012 opgepakt nadat hij op Gaychat.nl en MSN contact had gezocht met een 13-jarige jongen. De jongen bleek echter een politie-infiltrant, een zedenrechercheur uit Hollands-Midden die werd ingezet als 'lokpuber'. De zaak is juridisch interessant. Volgens de officier zoekt de politie naar opsporingsmiddelen om misbruik via internet aan te pakken. 'Heel veel kinderen zitten achter de computer en hebben bescherming nodig'. Het dossier is daarom overgedragen aan het landelijk parket in Rotterdam dat moet oordelen over de inzet van lokpubers als opsporingsmiddel. Een woordvoerder van het landelijk parket ziet geen belemmeringen. De verdachte staat ook terecht voor het bezit van 33 kinderpornofilmpjes en 149 afbeeldingen

Uw smartphone virusvrij!

Bankieren, mailen, internetten, whatsappen… onze mobieltje heeft tegenwoordig meer weg van een zakcomputer dan van een belapparaat. Handig voor de gebruiker, maar al die nieuwe toepassingen hebben het mobieltje ook een stuk interessanter gemaakt voor cybercriminelen. Hoe veilig is uw mobieltje eigenlijk voor virussen? En belangrijker nog: wat kunt u eraan doen?

Vroeger, toen mobieltjes nog eenvoudige apparaten waren, leek het ondenkbaar dat er ooit computervirussen voor mobiele telefoons zouden komen. Dat is een illusie gebleken. In 2004 werden de mobiele bellers voor het eerst opgeschrikt door het Cabir-virus. Cabir was een programmaatje dat zich ongemerkt nestelde op de mobiele telefoon en via bluetooth een kopie doorzond naar andere telefoons. Het was een betrekkelijk onschuldig virus: op het toestelscherm verscheen het woord 'Caribe' en de batterij van het toestel werd extra snel uitgeput.

Enige hulp van de gebruiker was hierbij wel nodig, want die moest zijn toestel open hebben staan voor ontvangst van bluetoothberichten en het berichtje accepteren om het virus binnen te halen. Desalniettemin veroorzaakte Cabir een wereldwijde epidemie en werden een jaar na de eerste melding nog steeds telefoons met het virus aangetroffen. Sindsdien duiken er steeds meer nieuwe mobiele virussen op die zich op verschillende manieren verspreiden. In 2005 verschenen de eerste mobiele virussen die via mms-berichten telefoons infecteren, waardoor virussen niet enkel telefoons konden infecteren die zich op maximaal tien meter afstand bevonden. Eind 2008 werd het eerste virus voor de iPhone gevonden, dat zich voordeed als een systeemupdate. En nu, in 2011, verschenen er meer mobiele virussen dan ooit tevoren en veiligheidsbedrijven als G Data, McAfee en Kaspersky verwachten dan ook dat het aantal Trojaanse paarden , virussen en wormen voor mobiele telefoons komende jaren zal blijven toenemen.

Schade

Het is vooralsnog lastig voor cybercriminelen om geld te verdienen met malware voor mobiele telefoons. De zwaktes van Windows-ps's zijn al grotendeels bekend, terwijl die voor mobiele telefoons nog uitgezocht moeten worden. Daarbij worden programma's, en dus ook malware, ontworpen voor een bepaald besturingssysteem. Het overgrote deel van de vaste computers gebruikt Windows en de meeste virussen zijn voor dat systeem actief. Voor smartphones is er niet één dominant besturingssysteem dat alle telefoons ondersteunt. Dit gegeven maakt dat smartphones nog altijd stukken veiliger zijn dan pc's. Waarom zou een hacker immers de aandacht richten op mobiele toestellen, wanneer hij gemakkelijk geld kan verdienen met malware voor de dektop? Momenteel maken de meeste mobiele virussen gebruik van sms-diensten om de gebruiker geld afhandig te maken. Het virus verstuurt automatisch sms-berichten naar een peperduur telefoonnummer en het slachtoffer vindt deze terug op de telefoonrekening.

Ontvangstbevestigingen worden door sommige van die virussen in de inbox onderschept, zodat de gebruiker niets merkt. Jmsonez A voor Android is zo'n virus. Het virus werd aangetroffen vermomd als een onschuldig ogende kalender-applicatie. Na installatie geeft de kalender altijd een datum in januari 2011 aan. Wanneer de gebruiker vervolgens de datum verandert, begint het programma sms-berichten te verzenden naar een premium-telefoonnummer. Ook richten de cybercriminelen zich op mobiel internetbankieren. Gebruikers kunnen door malware bijvoorbeeld worden omgeleid naar phishingsites – webpagina's die er precies zo uitzien als die van uw bank – om zo wachtwoorden te stelen. Daarnaast is er ook malware gevonden die zich bezighoudt met het onderscheppen van tan-codes.

Zo werd dit jaar het Trojaanse paard ZITMO (Zeus in the mobile) gevonden. ZITMO werkt samen met malware die is binnengedrongen op de pc. De gebruiker krijgt tijdens de banksessie een door het virus gegenereerde melding, waarbij gevraagd wordt om in verband met veiligheid een app te installeren op de telefoon. Eenmaal geïnstalleerd op de telefoon onderschept de app de tan-codes en stuurt deze ongemerkt door naar de server van de hackers. Het oorspronkelijke idee van de tan-code, waarbij er gebruikgemaakt wordt van twee gescheiden werelden, is dus niet meer waterdicht.

Verspreiding

Bluetooth en mms worden nog steeds gebruikt om virussen te verspreiden, maar tegenwoordig worden vooral applicaties gebruikt om malware als een Trojaans paard op de telefoon te laten binnenkomen. De meeste malwareapps bevinden zich buiten de officiële kanalen. Gebruikers zoeken daar nog wel eens naar gekraakte of goedkopere versies van applicaties die in de officiële applicatiewinkels beschikbaar zijn. Maar ook apps in de officiële winkels worden niet allemaal even goed gescreend. Zo werden er afgelopen jaar regelmatig apps aangetroffen in

de Android Marketplace die geïnfecteerd waren met het DroidDreamvirus.

Google moest een aantal keer de Marketplace doorlichten om malafide apps te verwijderen. Google hanteert, in tegenstelling tot bijvoorbeeld Apple en BlackBerry, een open systeem. Dat betekent dat

iedere ontwikkelaar applicaties mag toevoegen en er geen strenge controles worden uitgevoerd om te kijken wat een app precies doet op een toestel. Daarbij werkt het besturingssysteem met veel verschillende toestellen en vaak door de operator of telefoonfabrikant aangepaste versies van de software. Kwaliteitscontrole is hierdoor lastig. Bovendien kunnen updates niet voor alle klanten even snel worden gerealiseerd.

Momenteel zijn de meeste virussen nog actief op het Symbian-platform, maar mede door de zwaktes van het open systeem van Google is het aantal virussen voor Android in 2011 fors toegenomen. Die trend zal waarschijnlijk doorzetten, want Android verwerft een steeds dominantere positie op de mobiele markt. iPhone-en BlackBerry-bezitters lijken veiliger te zijn voor mobiele virussen, maar ook voor deze toestellen zijn virussen actief. Zo was het enige tijd geleden mogelijk voor hackers om via het berichtenscherm van de Skype-applicatie van de iPhone malware te versturen. In juli 2009 ontdekten Californische onderzoekers hoe ze via sms-berichten het geheugen van de iPhone konden vernielen. In datzelfde jaar maakte beveiligingsbedrijf Intego melding van malware onder de naam Privacy A, die misbruik maakt van het standaardwachtwoord ‘alpine’ op gekraakte iPhones.

Antivirus

En wat nu te doen tegen al dat virusgeweld? Die oude telefoon uit de la halen maar weer? Nee, dat ook weer niet. Mobiele virussen zijn lang niet zo talrijk als voor de pc en u surft met uw mobieltje online nog altijd een stuk veiliger dan met uw thuiscomputer. Bovendien kunt u vergelijkbare maatregelen nemen als voor uw pc door de telefoon uit te rusten met een antivirusprogramma. Softwarebedrijven als Kaspersky, F-Secure en Bullguard hebben afgelopen jaren allerlei antivirusvarianten gelanceerd die geschikt zijn voor smartphones.

Symbian- en Androidgebruikers hebben daarbij een stuk meer keus, omdat deze platformen nu eenmaal het vaakst getroffen worden door virussen en er dus ook meer antivirusprogramma’s voor zijn gelanceerd. Antivirusprogramma’s voor mobiele telefoons kunnen doorgaans meer dan de varianten voor de pc. In beginsel kunnen de apps de mobiele telefoon scannen op bekende virussen. Ook blokkeren ze gevaarlijke websites wanneer die worden benaderd. Daarnaast zijn er nog allerlei extra mogelijkheden. Zo kunt u de telefoon op afstand lokaliseren en vergrendelen wanneer u ‘m verloren hebt. Het ene pakket kan net weer wat meer dan het andere en het is daarom goed om te bedenken wat u precies wilt alvorens u een bepaald pakket neemt. U kunt antivirusprogramma’s vinden op de website van de antivirusmaker.

Daarnaast kunt u in een officiële applicatiewinkel antivirusapps vinden. Soms zijn die nog goedkoper dan op de website. Zo kost de Kaspersky mobile applicatie op de website 24,95 euro per jaar, terwijl hij in de Android Marketplace 6,95 euro kost voor een onbeperkte licentie. Let wel: ga niet zoeken op alternatieve sites! Sommige malware vermomt zich als een antivirusprogramma. Om dezelfde reden raden we dan ook aan om antivirussoftware te installeren van een bekende maker. Mocht u toch een

alternatief willen gebruiken, zoek dan wel op fora uit wat de ervaringen van anderen zijn met dit programma.

Een mobiel antiviruspakket hoeft niet veel te kosten. De goedkoopste abonnementen van F-Secure en Bullguard (voor Android, Symbian en Windows mobile) kosten op hun website 24,95 euro per jaar, zo'n 2,08 euro per maand. Daarbij zijn er allerlei gratis pakketten beschikbaar, zoals Netqin, Lookout en AVG die net zo goed virussen detecteren. Dergelijke apps hebben vaak wel minder mogelijkheden en kunnen opgewaardeerd worden met betaalde apps. De gratis app van AVG kan bijvoorbeeld wel de telefoon lokaliseren en op afstand leeghalen, maar niet een backup maken van bestanden. Daarvoor moet u dan de AVG pro-app aanschaffen. Zo kunt u de Netqin-app in eerste instantie gratis downloaden, maar u moet wél betalen om de virusdatabase te updaten.

Uiteraard: gewoon goed uitkijken!

Los van het feit dat uw telefoon wellicht veiliger is gemaakt met een antivirus-app, hebben dergelijke programma's ook nadelen. Ze kosten het apparaat werkgeheugen en stroom. Bovendien worden soms apps als gevaarlijk bestempeld terwijl ze dit niet zijn en wordt er op fora nog wel eens geklaagd dat antivirus-apps niet, of in ieder geval moeilijk, zijn te verwijderen. Verder kunnen er vraagtekens gezet worden bij de kwaliteit. Zo bleek uit een test van het Duitse AV-Test.org dat een groot aantal gratis antivirus-apps voor Android nauwelijks virussen detecteert. Ze onderzochten daarbij wel relatief onbekende merken als Bluepoint, Kinetoo en Privateer Lite. Uit de testresultaten bleek dat van de tien aanwezige virussen er door sommige scanners maar één werd herkend. Ook waren er die helemaal geen virus herkenden.

Kaspersky mobile en F-Secure kwamen als beste uit de bus. Lookout, AVG en Netqin werden niet getest. Het belangrijkste wat u tegen verspreiding van malware op uw mobieltje kunt doen, is gewoon goed uitkijken. Het heeft geen enkele zin om het mobieltje dicht te timmeren en vervolgens roekeloos apps binnen te halen. Probeer uw enthousiasme dus wat te temperen vlak na aanschaf van de smartphone en download niet zomaar allerlei apps. Wees daar ook extra voorzichtig mee wanneer u een applicatie downloadt van een onbekende bron. Houd rare e-mails en berichten in de gaten. Zet uw bluetooth of wifi-verbinding niet onnodig aan en laat deze alleen berichten ontvangen bij het verzenden. En bekijk natuurlijk uw telefoonrekening geregeld...

Uiteraard kan het zo zijn dat u toch een virus op uw mobiel binnen hebt gekregen. De oude virussen van het eerste uur waren betrekkelijk eenvoudig te verwijderen. Cabir kon verwijderd worden door enkel de telefoon terug te zetten naar de fabrieksinstellingen. Tegenwoordig kunnen virussen echter een stuk hardnekkiger zijn. Zoek op de eerste plaats uit wat voor virus uw telefoon precies te pakken heeft. Dat kunt u doen door een scan te draaien met een antivirus-app of door u online te oriënteren. Wanneer u erachter bent wat er mis is, kunt u de schuldige app verwijderen. Daarnaast zijn er ook applicaties beschikbaar tegen bepaalde virussen. Lookout heeft bijvoorbeeld een speciale verwijdertool voor Droid-Dream-virussen. Vindt u dat

allemaal te ingewikkeld, dan kunt u ook langslopen bij de winkel waar u de telefoon hebt aangeschaft. Een winkel als The Phone House neemt dan bijvoorbeeld de telefoon in en zet er de officiële software weer op. Een nadeel is dat u uw telefoon dan wel enige tijd kwijt bent en hem zonder applicaties terugkrijgt.

Facebook, Hyves en Twitter: Zo komt u van uw accounts op internet af!

Voor vrijwel alle sociale netwerken en andere online diensten bent u verplicht een account aan te maken. Maar hoe lastig is het om zo'n account op een later moment weer op te heffen?

Het Oudhollandse gezegde 'bezint eer u begint' is anno 2011 nog steeds actueel. Afmelden voor diensten als Skype, Twitter, Google, World of Warcraft, Flickr en You-Tube blijkt namelijk nog niet zo eenvoudig. Bij sommige online diensten moet u allerlei capriolen uithalen om er vanaf te komen. En als het u wel lukt, blijken uw gegevens niet te worden verwijderd of gebeurt dit pas na een bepaalde periode. Wij laten zien hoe u bij een aantal populaire diensten uw account kunt stopzetten.

Deactiveren of opheffen?

Wist u dat er een aantal online diensten zijn waar u helemaal nooit meer vanaf kunt komen? Je zou denken dat het anno 2011 goed geregeld is wat betreft uw privacy, maar niets is minder waar. Op AccountKiller.com een site waar van veel diensten is te zien of en hoe u er vanaf kunt komen is een zwarte lijst opgesteld van diensten waarbij afmelden niet of nauwelijks mogelijk is. Uw Skype-account kunt u bijvoorbeeld niet verwijderen, u kunt hooguit uw gegevens wissen zodat u niet langer vindbaar bent. Dit geldt ook voor het onder jongeren populaire Habbo, de banensite Nationale Vacaturebank en de online gamedienst Steam.

Argumenten die aangevoerd worden is dat men spijtoptanten de mogelijkheid wil bieden om op een later tijdstip het account te kunnen reactiveren. Ook zou het voor hackers anders makkelijker worden accounts over te nemen wanneer accounts kunnen worden opgezegd. Dat uw privacy hier vervolgens onder lijdt, is blijkbaar van ondergeschikt belang.

Bij een aantal andere diensten gaat afmelden lastig. Om van muziekdienst Spotify af te komen, moet u bijvoorbeeld zelf een mailtje sturen naar support@spotify.com en dan pas zullen ze uw account verwijderen. Hoe lang dit duurt is echter niet duidelijk. Ook Marktplaats moet u zelf een bericht sturen. Bij een dienst als iTunes wordt het de gebruiker ook flink lastig gemaakt. Men raadt aan om het account te deactiveren. Verwijderen is mogelijk, maar kan als gevolg hebben dat uw gekochte muziek niet meer op bepaalde apparaten kan worden afgespeeld of dat uw apps niet langer worden bijgewerkt.

Tips om af te melden

Bij een aantal sites en sociale netwerken gaat afmelden vrij eenvoudig, bijvoorbeeld via een knop die te vinden is onder Account-instellingen. Bij andere ontbreekt een duidelijke functie en is het zoeken. De volgende tips helpen u op weg:

- Weet u zeker dat u een account wilt stopzetten? Verwijder eerst zoveel mogelijk content die u geplaatst hebt of zorg ervoor dat dit niet langer zichtbaar is voor andere gebruikers.

- Gebruik de zoekfunctie van de aanbieder of kijk in de Terms of Service of Privacy Policy hoe u zich kunt afmelden. Goede zoekwoorden zijn: ‘delete’, ‘terminate’, ‘cancel’, etc. Zoek ook op het forum als dit er is.

- Nog steeds niets gevonden? Zoek dan op Google of kijk op AccountKiller.com waar voor veel diensten informatie is te vinden over hoe er vanaf komt.

- Stuur de dienst een e-mail of gebruik het webformulier voor support om aan te geven dat u wilt dat uw account verwijderd wordt. Bellen en faxen kan eventueel ook, maar dat is kostbaar wanneer een dienst in het buitenland is gevestigd.

Lukt het nog niet of was het lastig? Geef dit dan door aan AccountKiller.com en deel uw ervaringen met andere gebruikers. Diensten die geen gebruiksvriendelijke methode bieden om af te melden, komen op de zwarte lijst terecht.

Let op: sommige diensten reactiveren automatisch uw account wanneer u na het afmelden of deactiveren probeert in te loggen. Dat maakt het lastig om te checken of uw account inactief of verwijderd is. Vraag in zo’n geval aan een vriend of familielid dat nog wel een account heeft om te checken of u nog ‘gevonden’ wordt.

Flickr

Via de link www.flickr.com/profile_delete.gne kunt u heel eenvoudig afscheid nemen van uw account bij Flickr. Wel is het zo dat uw foto’s na beëindiging nog zo’n 90 dagen in het systeem blijven staan. Ze zijn dan niet langer zichtbaar voor andere gebruikers. Mocht u binnen deze periode niet uw account reactiveren, dan wordt het materiaal alsnog verwijderd.

Hyves

Wilt u uw Hyves-account verwijderen, ga dan naar Instellingen, Profielbeheer, Account opzeggen. Klik als u zeker bent op de knop Ik neem afscheid. Daarna ontvangt u via de e-mail een bericht met een link waarop u moet klikken om te bevestigen dat u inderdaad uw Hyves-account wilt verwijderen.

Let op: het is in veel gevallen mogelijk dat u na het verwijderen nog steeds kunt inloggen omdat het zo'n 24 uur kan uren voordat uw account daadwerkelijk is verwijderd.

LinkedIn

Klik wanneer u bent aangemeld bij LinkedIn rechtsboven op uw naam en kies voor Settings. Klik op het tabblad Account en daarna op Close your account. Geef eventueel een reden in en klik op de knop Continue.

YouTube

Wanneer u uw account bij YouTube wilt stoppen, raden we u aan om eerst uw video's te verwijderen. Sommige gebruikers die dit niet hebben gedaan beweren dat hun video's gewoon nog online staan, ondanks het feit dat YouTube zegt dat alles wordt verwijderd. Ga daarna naar Accountinstellingen, Account beheren en klik op de knop Account sluiten. Wanneer u een Google account gebruikt, blijft dit account gewoon beschikbaar voor andere diensten die u daar gebruikt.

Google

Uw Google-account gebruikt u waarschijnlijk voor meer diensten dan u denkt. Daarom krijgt u wanneer u naar www.google.com/accounts/DeleteAccount gaat een overzicht van alle diensten waarvoor u dit account gebruikt. U dient deze allemaal aan te vinken om te bevestigen dat u echt wilt stoppen. Voer daarna uw wachtwoord in en vink nog tweemaal 'Yes' aan om te bevestigen dat u uw account echt wilt verwijderen. Klik daarna op Delete Google Account.

Wikipedia

Hebt u een account bij online encyclopedie Wikipedia, bijvoorbeeld omdat u daar in het verleden een bijdrage aan hebt geleverd? Helaas is het niet mogelijk om uw account hier te verwijderen. Wikipedia heeft deze informatie nodig om te achterhalen wie welke bijdrage heeft gemaakt. Gelukkig bewaart Wikipedia nauwelijks persoonlijke informatie. Het is eventueel wel mogelijk om uw gebruikersnaam te laten veranderen.

Twitter

Stoppen met Twitteren doet u door in te loggen en te kiezen voor Settings, Account. Scroll vervolgens helemaal naar het einde van de pagina en klik op Deactivate my account. U kunt ook rechtstreeks naar twitter.com/settings/accounts/confirm_deactivation gaan. Na het stopzetten bewaart Twitter 30 dagen al uw tweets en andere gegevens voordat deze worden verwijderd. Gedurende deze periode kunt u uw account reactiveren.

Facebook

Via www.facebook.com/deactivate.php kunt u uw Facebook-account deactiveren. Echter, uw gegevens worden bewaard en het op het moment dat u zich in de toekomst aanmeldt, wordt uw account automatisch gereactiveerd. Als u uw account permanent wilt verwijderen, moet u hiervoor een verzoek indienen. Dat doet u via www.facebook.com/help/contact.php?show_form=delete_account of door in het Facebook Helpcentrum te zoeken naar ‘Hoe verwijder ik mijn account permanent?’.

MySpace

Om van het sociale netwerk My-Space af te komen gaat u naar My Stuff, Account Settings en klikt u in de linker kolom op Cancel Account. Klik daarna op de knop Cancel account. Nadat u de reden hebt opgegeven waarom u wilt opzeggen, ontvangt u een e-mail met een link waarop u moet klikken. U moet daarna wederom uw e-mailadres ingeven en op de knop Cancel Account klikken. Het kan vervolgens nog zo'n 48 uur duren voordat uw account daadwerkelijk is verwijderd.

Foursquare

Een sociaal netwerk dat intensief gebruikt maakt van locatiegegevens en dat steeds populairder wordt is Foursquare. Afmelden is zo gebeurd via de link foursquare.com/delete_me. Nog even uw wachtwoord in-voeren en zoals de mensen achter Foursquare aangeven: "U komt terecht op de homepage van Four-square en zult zich afvragen... was het allemaal een droom?"

Tot slot

Is het afmelden gelukt? Uw account werkt dan misschien niet langer, maar of uw data wordt verwijderd is maar helemaal de vraag. In de voorwaarden van veel diensten staat expliciet vermeld dat zij van alles met uw gegevens mogen doen, ook nadat u bent vertrokken. Veel diensten zijn – onder druk van consumentenorganisaties – zo fatsoenlijk om uw gegevens inderdaad te wissen, maar toch is het belangrijk om de voorwaarden eens te lezen.

U krijgt dan ook een indruk wat er allemaal met uw gegevens kan worden gedaan. Daarnaast is het opvallend dat vrijwel alle aanbieders in het reglement een clausule hebben opgenomen waarin staat dat ze de voorwaarden zonder vooraankondiging mogen wijzigen. Kortom: een minder sociale kant van sociale netwerken en iets om over na te denken wanneer u zich een volgende keer voor zo'n dienst aanmeldt.

Koppelingen met andere diensten

Veel online diensten zoals Facebook en LinkedIn bieden ontwikkelaars een zogeheten 'Application programming interface' (API) aan. Hiermee wordt het bijvoorbeeld mogelijk dat diensten achter de schermen gegevens met elkaar uitwisselen. Op die manier kunt u de locatie-informatie van bijvoorbeeld FourSquare automatisch publiceren op Facebook, en kunnen andere

Facebookgebruikers zien welke route u tijdens het sporten hebt gelopen nadat u deze op uw

mobieltje geregistreerd hebt, bijvoorbeeld met Endomondo of Nike+GPS. Handig? Dat wel. Maar het maakt het verwijderen van accounts en de bij-behorende gegevens nog een stuk ingewikkelder. Want als u een account opheft bij één dienst, worden de gegevens die deze dienst in het ver-leden heeft doorgegeven aan andere diensten daar nog wel gewoon getoond. Dat is dus iets om rekening mee te houden.

Welke externe toepassingen toegang hebben tot bijvoorbeeld uw Facebook-account, vindt u bij Facebook onder Accountinstellingen, Toepassingen. U kunt hier ook de toestemming weer intrekken. Andere online diensten beschikken over een soortgelijk dashboard waarin te zien is met wie er gegevens worden uitgewisseld.

Hoe hackers hacken


Hackers hit

Terroristen, activisten, criminelen, nieuwsgierige jongeren, soldaten, digitale huurlingen en idealisten; hackers zijn er in alle soorten en maten. Maar wat drijft hen en hoe werken ze? Is er zoiets als 'onhackbaar'? Een kijkje in de wereld van valse beschuldigingen, hoge idealen en hightech oorlogsvoering.

We gaan ervan uit dat een hacker iemand is die voor zijn gewin illegaal inbreekt op computer- of communicatiesystemen of die op een andere illegale manier een digitale beveiligingsmaatregel omzeilt. Deze digitale inbrekers worden black hats genoemd. White hats zijn beveiligingsexperts die met hun hacks geen schade willen toebrengen, maar aantonen dat een bepaald systeem onveilig is. Omdat er niet echt wordt ingebroken is er in onze context geen sprake van een echte hack. Tenslotte zijn er de grey hats, die geen geld verdienen aan hun illegale activiteiten.

Hacktivist
Sinds de sterke groei van het publieke internet midden jaren 90 is de term hacktivist populair geworden. De meeste grey hats zijn hacktivisten. Zo'n hacktivist breekt illegaal in op systemen – meestal publieke websites – om deze offl ine te dwingen, of om een boodschap te planten. Zo werd de website van Geert Wilders op 23 september door de Turkse hacker SEPTEMB0X gehackt en aangepast, waarna de site onder andere een Korantekst vertoonde. Het op die manier aanpassen van een website wordt 'defacen' genoemd. Omdat de hacker geen geld verdiende aan zijn actie, maar slechts zijn morele ongenoegen toonde over de uitspraken van Wilders, is er sprake van hacktivisme. Veel andere hacktivisten zijn voor vrijheid van meningsuiting en hacken organisaties en overheden die naar hun mening de vrijheid inperken.

Skillz
Doordat de privacy van miljoenen mensen op het spel staat en online bankieren enorm populair is geworden, zijn er steeds meer professionals die werken om de digitale veiligheid te garanderen. Zodra er een lek in een programma, besturingssysteem, communicatie-protocol of apparaat wordt gevonden gaan de pro's direct op zoek naar een 'patch' om te voorkomen dat hackers dit lek kunnen uitbuiten. Zolang een lek niet bekend is bij de fabrikant of leverancier heet het een zero day exploit. De term 'exploit' geeft al aan dat hackers het lek al exploiteren om te kunnen inbreken. Het zelf vinden van een zero day exploit is een van de vaardigheden (in het Engels: skills) van een hacker. Andere vaardigheden, zoals het succesvol uitbuiten van zwakheden in systemen, het achterhalen van wachtwoorden en het bespelen van gebruikers vormen samen de 'skillz' waarop de hackers trots zijn.

Onhackbaar?
Is er een systeem dat niet te hacken is? Nee. Zelfs al zou de technologie 100 procent onkraakbaar zijn, dan is er altijd nog de gebruiker als zwakke plek. Het veiligst zijn zogenaamde standalone-systemen, die geen enkele verbinding met internet of een ander netwerk hebben. Maar die – zeldzame – systemen zijn vaak juist zeer interessant als doelwit, waardoor er heuse spionnen met usb-sticks en speciale cd-roms op af komen om fysiek de machine aan te vallen of een gebruiker om te kopen. Het MKB is steeds vaker slachtoffer. Zo kan een gehackte telefooncentrale een bedrijf meer dan tienduizend euro kosten.

Frappant is dat zelfs 'air gaps' (fysiek volledig op zichzelf staande netwerken) de zwaarbewaakte Predator drone-basis niet konden beschermen. De topgeheime machines waarmee op afstand onbemande vliegtuigjes kunnen worden bestuurd, en waarmee ook raketten kunnen worden afgeschoten blijken besmet met een 'weerbarstig' virus. Eerder hadden Iraakse en Afghaanse militanten al de – onversleutelde! – videobeelden die de drones verzonden met gemak afgeluisterd. Het leger van de VS wist al dat de vijand dit kon sinds 1999, maar het versleutelen van de speciale verbindingen is 'duur'. Het Pentagon zelf is al drie jaar zonder succes bezig om de evoluerende worm Agent.btz van zijn computers af te krijgen.

Opvallend is dat de VS momenteel geld uitlooft voor de bedenker van een systeem dat kan controleren of microchips (waaronder computerprocessors en onderdelen van routers en moederborden) niet stiekem geprogrammeerd zijn met malware of kill-switches door China. De oorlogsmachine van de VS is zeer afhankelijk van microchips en aangezien die bijna allemaal in China worden gemaakt is men kennelijk bang voor sabotage van de cruciale hardware.

Scripted?
In eerste instantie zal de hacker een reeks commando's naar een systeem hacken of programma zenden, ondertussen peilend of zijn acties succes hebben. Als de hack gelukt is, heeft de hacker een reeks commando's tot zijn beschikking die hij verzamelt in een tekstbestand, een zogenoemd script. Bij een volgende aanval kan hij het script in één keer afdraaien en zonder moeite vanzelf een

kwetsbaar systeem verschalken. Iemand zonder hack-ervaring kan zo'n script ook gebruiken, aangezien het praktisch automatisch werkt. Een onkundig persoon die zo'n script gebruikt wordt met enig dedain een scriptkiddie genoemd. Meestal gaat het namelijk om tieners, die uiteindelijk vaak opgepakt worden. Een deur openen met een loper is tenslotte één ding, na afloop wegkomen zonder

bewijsmateriaal achter te laten een ander. Soms is hacken wel erg makkelijk. Zo maakt het programma ERD Commander – van Microsoft – het mogelijk om met een paar muisklikken de wachtwoorden op elke Windows-pc te veranderen.

Tor

Een groot probleem voor hackers is het voorkomen van opsporing door de autoriteiten. The Second-Generation Onion Router oftewel Tor is een initiatief dat hackers flink helpt op vrije voeten te blijven. Het internet bestaat in de basis uit computers die – via via – contact met elkaar kunnen opnemen. Elk apparaat heeft een uniek ip-adres, waarmee uw internet service provider activiteiten aan uw identiteit kan linken. Tijdens het browsen laat u het adres overal achter, want zo werkt internet; alle datapakketjes van en naar uw pc bevatten uw ip-adres en worden door spionerende partijen opgeslagen in logbestanden. Bovendien is wereldwijd bekend welke provider de beschikking heeft over elk ipadres, zodat meteen duidelijk is dat u uit Nederland komt en bij welke provider u klant bent. Het ip-adres vormt ook nog eens een goede basis voor allerlei digitale aanvallen, bijvoorbeeld om een stiekeme keylogger op uw systeem te planten.
Hoe Tor dit oplost? Door een virtueel, gedistribueerd, anoniem netwerk boven op bestaande internetverbindingen te bouwen. Niet alleen is het met Tor mogelijk om anoniem te surfen, te chatten of te e-mailen, zelfs diensten aanbieden (websites, chatservers, bestanden) is geen probleem. Het Tor-netwerk verstuurt datapakketjes met een drievoudige, sterke versleuteling. En elke zender/ontvanger krijgt een willekeurig Onion-adres dat in de plaats komt van het ip-adres. Pakketjes worden willekeurig van het ene naar het andere Tor-knooppunt gestuurd totdat ze de ontvanger hebben bereikt. Door het Onionadres te gebruiken bij het doorsturen van de pakketjes blijven de onderliggende ip-adressen geheim voor iedereen behalve de toevallig gekozen laatste in de keten van doorzendende computers. Omdat elk pakketje volstrekt willekeurig van de ene naar de andere 'Onion' gaat zal zelfs een spion die álle 3000 knooppunten in het Tor-netwerk constant volgt specifi eke communicatie niet kunnen afl uisteren. Onversleuteld gebruik van Tor kan trouwens wél tot ontdekking leiden.
Voordat Tor bestond konden hackers een groot aantal gehackte pc's gebruiken als willekeurige doorgeefluiken om hun verblijfplaats zoveel mogelijk te beschermen, maar Tor is beter doordat het een legitieme dienst is. De hackers staan anoniem tussen 450.000 overheidsdiensten, soldaten, terroristen, argeloze thuisgebruikers en journalisten. Het staat buiten kijf dat de beste hackers praktisch onvindbaar zijn. Ruziënde hackers proberen elkaars identiteit vaak openbaar te maken, het zogenoemde doxen.

Anatomie van een hack

In maart werd beveiligingsreus RSA gehackt. RSA houdt zich bezig met het versleutelen van informatie en geavanceerde gebruikersauthenticatie. Elke hack begint met een vector, een succesvolle aanval op een zwakke plek in de beveiliging. Steeds vaker is dit geen systeem, maar een gebruiker. In dit geval stuurden de hackers vier medewerkers een e-mailtje met een Excelbestand. Het mailtje leek van een bekend adres te komen, maar door het vervalsen van de

afzender werd verhuld dat het eigenlijk van de hackers afkomstig was. Tenminste één argeloze ontvanger opende het Excel bestand, waarin zich een Flash-component bevond. De Flash-component startte zelf een script dat de Poison Ivy-backdoor downloadde. Dit onzichtbare programmaatje nam vervolgens contact op met een door de hackers opgezette machine, waarna de hackers commando's naar de besmette pc konden sturen.
Poison Ivy had onopgemerkt de deur wijd open gezet voor de hackers, vandaar de term backdoor. Met deze vrij beperkte voet tussen de deur is het tijd om te zorgen voor toegang tot relevante systemen als de beheerder. Want de gebruiker die de e-mail opent heeft normaliter maar zeer beperkt rechten om diensten, systemen en programma's te starten of te beïnvloedden. Een systeembeheerder kan in principe wél alles. Het toe-eigenen van hogere rechten wordt elevation genoemd en kan door misbruik te maken van een bug, of – in dit geval – door het stelen van accountinformatie worden gerealiseerd. Als de hackers eenmaal kunnen inloggen als systeem- of netwerkbeheerders zijn ze oppermachtig en kunnen ze interessante informatie uit databases, e-mailsystemen en bestanden gaan verzamelen. De laatste stap is het verzenden van die informatie naar een machine buiten het gehackte bedrijfsnetwerk. In het geval van RSA verpakten de hackers de informatie in versleutelde rararchiefbestanden en verzonden deze naar een gehackte machine van een internetprovider.

Vakantie? Smartphone mee!

Reisgidsen en routekaarten meesjouwen tijdens de vakantie hoeft anno 2011 niet meer: een smartphone, mobiel internet en de nodige apps zijn genoeg om de reis vlekkeloos te laten verlopen. Of u nu de weg zoekt, een hotelletje wilt boeken of de leukste beziens-waardigheden wilt ontdekken: zolang u uw smartphone mee hebt, bent u onder de pannen!

Elke vakantie begint uiteraard met een goede voorbereiding. Voor wie een smartphone meeneemt op reis, bestaat die voorbereiding uit een aantal zaken. Zo is het verstandig om na te gaan of de kosten voor internationaal dataverbruik betaalbaar zijn, zodat er bij thuiskomst geen gepeperde rekening op de deurmat ligt. Als u regelmatig op reis gaat, neem dan een speciale databundel voor het buitenland. U bent dan namelijk goedkoper uit. De meeste telecomproviders bieden dergelijke abonnementen aan.

De capaciteit van de accu is een ander aspect om rekening mee te houden. Controleer vooraf hoe lang de accu meegaat. Zorg zo nodig voor een reserve-exemplaar of schaf een autolader aan.

Op reis

Om te illustreren welke apps u in bepaalde situaties kunt gebruiken, nemen we u mee op reis naar enkele landen in Europa. Stelt u zich het volgende eens voor. U vertrekt met de auto vanuit Nederland richting Frankrijk en overnacht een paar dagen in Parijs. Vervolgens reist u verder naar het zuiden, waarbij u een tentje neerzet aan de voet van de alpenreus Mont Blanc. Na een week rijdt u

richting een klein dorpje in Italië waar u het comfort van een hotel opzoekt. Ten slotte keert u via Zwitserland en Duitsland weer terug naar Nederland. Onderweg overnacht u nog bij verschillende campings.

Zodra u de smartphone als navigatiemiddel wilt inzetten, is Google Maps onmisbaar. U gebruikt deze app direct na vertrek. Een voordeel is dat u geen duur navigatieapparaat hoeft aan te schaffen. U vraagt een routebeschrijving op door een eindpunt in te stellen. Via gps is uw huidige locatie al bij Google Maps bekend. Geef daarnaast ook aan dat u per auto reist. U ontvangt gedetailleerde instructies over hoe u moet rijden, hoe ver het is en hoe lang u erover doet. De route bekijkt u eventueel ook op een geografisch kaartje of in de straatweergave (Street View). Bezitters van een Android-toestel hebben geluk, omdat er voor dit platform ook gesproken route-instructies beschikbaar zijn. U activeert daarnaast verschillende bruikbare lagen op de kaart, zoals benzinestations, restaurants en parkeerplaatsen. Als u een andere smartphone gebruikt, laat u door een medepassagier de route voorlezen.

Overnachtingen

Zodra u in Parijs bent aangekomen, gaat u op zoek naar een mooie overnachtingplaats. Gebruik hiervoor de Nederlandstalige app van Hotels.com. Hiermee zoekt u in een database van 135.000 hotels, die zich overal op de wereld bevinden. U bekijkt aanbiedingen en het is zelfs mogelijk om direct een kamer te boeken. In dat laatste geval moet u wel een account aanmaken. Prettig is dat u beoordelingen van andere gebruikers leest, zodat u snel ziet welke adressen kwaliteit bieden. De foto's geven u een indruk van het interieur en ook de faciliteiten worden uitgebreid omschreven. U rekent af met een creditcard, waarna Hotels.com boekingsgegevens per e-mail naar u verzendt.

Een alternatieve app is Hotels near me. Dit hulpmiddel is vooral handig voor als u op de bonnefooi naar een stad vertrekt en pas op het laatste moment een hotel wilt boeken. Op basis van uw gps-locatie ziet u precies welke adressen er in de buurt zijn. Een derde mogelijkheid om vlot een kamer te boeken, is via de app van Booking.com.

Stad verkennen

Wanneer u met meerdere personen reist, bestaat de kans dat u in aparte groepen Parijs gaat verkennen. In dat geval komt Google Latitude goed van pas. Met dit onderdeel van Google Maps ziet

u op een kaartje waar iedereen zich bevindt – mits uw mede-vakantiegangers Latitude ingeschakeld hebben uiteraard. Wie een iPhone heeft, dient deze app apart te downloaden. Via chat kletst u rechtstreeks met bekenden, zodat u op ieder willekeurig punt kunt afspreken.

Wilt u graag meer weten over bijvoorbeeld de historische gebouwen die u onderweg tegenkomt? Download dan de Wikitude World Browser. De werking van deze app is erg slim bedacht. Richt de camera van uw smartphone op een bekend bouwwerk, bijvoorbeeld de Eiffel-toren. Wikitude zorgt er vervolgens voor dat er, als u tenminste de gps-functie ingeschakeld hebt, relevante informatie op uw beeldscherm verschijnt, afkomstig van onder meer Wikipedia. U kunt WWB ook gebruiken voor meer praktische doeleinden: zo leest u bijvoorbeeld beoordelingen van restaurants en ziet u welke winkels er in de omgeving zijn.

Als u een stad niet goed kent, is het lastig om te achterhalen waar er wat vertier te vinden is. In dat geval gebruikt u het sociale netwerk Foursquare. Hiermee checkt u virtueel in bij openbare locaties, zoals winkels en stadsparken. U vraagt eenvoudig een overzicht op van de populairste plekken in uw omgeving. Wellicht ontdekt u op deze manier een goed restaurant of leuke kroeg. Verder leest u gebruikerservaringen van diverse uitgaansgelegenheden. Wanneer u ondanks alle moderne hulpmiddelen evengoed de behoefte voelt om een reisgids op zak te hebben, installeert u de app van 100% stedengids. Die is tenslotte veel handzamer dan een echt boekje! Een belangrijk pluspunt is dat de informatie ook offline beschikbaar is. Het is zelfs mogelijk om zonder internettoegang te navigeren. Ideaal voor diegenen die de datakosten in bedwang willen houden. U betaalt voor deze app 6,99 euro.

Campings

Het is tijd om te vertrekken uit Parijs. U verruilt de luxe van een hotel voor de eenvoud van een camping in de Alpen. Misschien wilt u onderweg nog een kort uitstapje maken naar een mooi kasteel of museum. Bijzondere bezienswaardigheden zijn verzameld in de app Mijn Frankrijk Gids. Verder vindt u met deze tool leuke campings in de omgeving. U gebruikt voor dit doel eventueel ook de ANWB Campinggids. U moet hiervoor wel een bedrag van 3,99 euro neerleggen, maar dan kunt u ook bijna achtduizend campings uit verschillende Europese landen moeiteloos vinden.

In berggebieden kan het weer snel omslaan. Om te voorkomen dat uw tent wegspoelt, is het verstandig om de weersverwachting in de gaten te houden. Er bestaan honderden goede apps op dit gebied.

Met WeatherBug vraagt u van iedere gemeente een weersverwachting op. Mocht er noodweer op komst zijn, kunt u daarop inspelen door vroegtijdig uw biezen te pakken.

Vreemde talen

Na een week pakt u de tent weer in en vertrekt u naar Italië, waar u een klein dorpje net over de grens opzoekt. U kunt de eerder besproken hotel-apps uitproberen om een geschikte slaapplaats te boeken. Verwacht hier overigens niet teveel van, want het zijn vooral hotels in grotere steden die u in deze apps vindt.

Op afgelegen plekken is lang niet iedereen de Engelse taal machtig. Zeker in kleinschalige hotels is communicatie weleens lastig. Toch is het voor praktische zaken wel handig als u zich verstaanbaar kunt maken. Hoe legt u bijvoorbeeld uit dat de airco het niet doet, of dat u geld wilt opnemen?

U vindt in Google Vertalen de oplossing. Met deze dienst zet u tekstdelen om naar een vreemde taal. Overigens is de vertaling letterlijk, dus de woordvolgorde is soms niet helemaal correct. Dat maakt natuurlijk niet zoveel uit, als ze u maar begrijpen! In het grensgebied van Italië spreekt de bevolking Frans of Italiaans. U selecteert één van deze talen en typt vervolgens een Nederlandse zin. De vertaling verschijnt op uw scherm. Alleen voor iPhone en Android is er een app beschikbaar. Op overige smartphones surft u naar www.translate.google.nl.

Met de app spreekt u eventueel ook zinnen in en zet u ze om naar de gewenste taal. Als u niet weet hoe u een zin moet uitspreken, laat u Google simpelweg de tekst voorlezen. Het voorkomt dat u bij de hotelreceptie zelf zit te stuntelen.

TIP: Handig is dat de vertaalgeschiedenis wordt bewaard. Als u geen mobiel internet in het buitenland wilt gebruiken, slaat u thuis praktische zinnen alvast op in de app van Google Vertalen.

Internetloos

De dekking van mobiel internet is binnen Europa over het algemeen goed. Toch hebt u in bepaalde gebieden geen internetbereik, bijvoorbeeld in de Alpen. Zonder internet hebt u niets aan Google Maps, om die reden is het slim om een landkaart lokaal op te slaan. Aan de hand van gps ziet u dan evengoed waar u bent, waardoor u probleemloos restaurants en supermarkten in de buurt opspoort.

Met City Maps 2Go voor de iPhone kunt u voor 1,59 euro meer dan drieduizend plattegronden downloaden en opslaan. De nieuwste versie van deze dienst heeft honderd procent dekking in Italië, Frankrijk en Duitsland.

Wifi vinden

Over offline gesproken; het is bijzonder irritant als er geen mobiel internetbereik is terwijl u op dat moment iets wilt opzoeken. Gebruik in deze situatie Wi-Fi Finder om draadloze hotspots in de omgeving te vinden. Via uw gps-locatie geeft deze dienst aan welke gratis en betaalde wifi-toegangspunten er in de buurt zijn. Als alternatief downloadt u de volledige database naar uw smartphone, zodat u geen gps nodig hebt.

De vakantie zit er bijna op. U gaat via Zwitserland en Duitsland naar huis. Onderweg maakt u tussenstops bij verschillende campings.

U gebruikt de ANWB Campinggids om goede overnachtingplaatsen op de route te selecteren. Als u bijna thuis bent, is het vervelend om nog kilometers lang in de file te staan.


In Nederland is die kans nogal groot. Installeer daarom de app File-Flits, zodat u zo nodig een alternatieve route uitstippelt.

Beelden bewakingscamera's sneller online

Beelden van bewakingscamera's komen binnenkort sneller beschikbaar voor internet. De ministerraad heeft ingestemd met een wetsvoorstel van staatssecretaris Teeven (VenJ) dat regelt dat burgers en bedrijven zelf beelden van bewakingscamera's mogen verspreiden als ze aangifte hebben gedaan. Toestemming van justitie blijft vereist. Wie daar niet op wachtte, was een hotelbaas in Harlingen. Die zette vorige week een filmpje online van een man die een iPhone steelt. De politie Fryslan zegt niet blij te zijn met de actie: publicatie op internet kan het onderzoek belemmeren en mag bovendien niet volgens privacywetgeving. De politie zegt ook te weten wie de dief is. Hij zal spoedig worden aangehouden, aldus een woordvoerder.

Nederland mist urgentie in aanpak cyberdreiging

Onlangs verscheen het tweede Cybersecuritybeeld. Daarin schrijft het Nationaal Cyber Security Center (NCSC) dat Nederland nog steeds 'een gevoel van urgentie mist' en 'bekende basismaatregelen' bij cyberbedreigingen niet neemt. In een begeleidende brief schrijft minister Opstelten aan de Kamer dat 'de handelingen van de hacktivisten, beroepscriminelen en cyberonderzoekers de afgelopen periode zichtbaarder' waren maar dat er 'geen grote verschuivingen' in de dreigingen te zien waren. Zichtbaarder betekent vooral dat zaken vaker het nieuws halen; ook blijken hackers 'redelijk vaste patronen' te volgen en zijn hun acties makkelijk te traceren. Incidenten leiden echter niet altijd tot de juiste acties, schrijft de general manager van het NCSC, Elly van den Heuvel. Volgens het rapport zijn cyberspionage en cybercrime de grootste digitale dreigingen waar Nederland mee wordt geconfronteerd. Overheid, bedrijfsleven en burgers blijven een gewild doelwit. Maar een aantal incidenten was voorkomen als 'de bekende basismaatregelen' genomen waren. Omdat 'bepaald' geen lering is getrokken uit eerdere incidenten, geeft het NCSC dezelfde waarschuwingen als in het eerste Cybersecuritybeeld. Verder ontbreekt het doorsnee internetgebruikers maar ook veel organisaties aan voldoende kennis en kunde om zich goed te beschermen tegen digitale risico'.

Anti-virusbedrijf AVG lanceert social media beheertool

Het Tsjechische anti-virusbedrijf AVG heeft een programma gelanceerd waarmee gebruikers meer sociale netwerksites, media en diensten kunnen beheren. MultiMi, zoals de tool heet, integreert Facebook, Gmail, Twitter en andere platformen. Het programma is voorzien van een ingebouwde Chromium browser en ondersteunt allerlei diensten, zoals Gmail, Yahoo, Hotmail, POP3 en IMAP, Facebook, Twitter, LinkedIn, Facebook en Google kalenders, RSS-lezers, fotosites zoals Picasa en Flickr, YouTube, Google Docs en Gtalk.

Verder is MultiMi voorzien van de Linkscanner technologie van AVG, die voor kwaadaardige websites waarschuwt.

Prettige vakantie!