SECURE COMPUTING

DIGITAAL COMPUTER MAGAZINE

Oktober 2012

W.Bosgra Taakaccenthouder digitale criminaliteit

INHOUD

In deze editie oa:

De Russen komen

Verslaafd aan Apps

Nieuwe Nigerian scams

Studeren met YouTube

PC hulpprogramma's

Transfer Big files

Hack preventie

Wapen uit 3D printer

@securecomputing

Bronnen: De Waarschuwingsdienst, Nederland veilig, Meldpunt Cybercrime, Digibewusr & Digivaardig, Webwereld, Security.nl, Zdnet, Veilig bankieren, You Tube, Internetsporen, Voelspriet

Amerikaanse generaal hackte Afghaanse vijand

Het Amerikaanse leger heeft in Afghanistan cyberaanvallen tegen de vijand uitgevoerd, zo heeft een luitenant-generaal laten weten. "Als commandant in Afghanistan in 2010, kon in mijn cyberoperaties met groot effect tegen mijn vijand inzetten", aldus Richard P. Mills. "Ik wist zijn netwerken binnen te dringen, zijn command en control te infecteren en mezelf te beschermen tegen zijn continue aanvallen om mijn netwerk binnen te komen en mijn operaties te ontregelen", aldus de bevelhebber tijdens een conferentie.

Aanvallen
Details over de omvang en aard van de aanvallen wilde Mills niet delen, maar het feit dat hij toegeeft dat de aanvallen plaatsvinden wordt door sommige experts als opmerkelijk beschouwd. "Dit is nieuws", stelt James Lewis Center for Strategic and International Studies.

Het was binnen defensiekringen algemeen bekend dat het Amerikaanse leger ook cyberaanvallen in Afghanistan uitvoerde, maar niet eerder sprak een legerfunctionaris zich hier openlijk over uit. Het Pentagon wilde niet op de uitspraken van Mills reageren.

Juridische vraag: is spyware illegaal?

Vraag: Onlangs installeerde ik een gratis stuk software, en elke keer als ik dat gebruikte, merkte ik dat mijn modem actief werd. Ik heb toen een netwerksniffer geïnstalleerd en ik zag dat de software op de achtergrond allerlei gegevens verstuurde.

Ik heb de leverancier hierop aangesproken, want dat is dus spyware. Maar zij zeggen dat het legaal is omdat ik in de gebruiksvoorwaarden toestemming heb gegeven hiervoor.

Er staat "The software contains an internet-enabled module that may collect and transmit aggregated data to improve the workings of our software. By using the software, you consent to this collection and transmission."

Mag dat zomaar?

Antwoord: Dat mag wel, maar niet zomaar.

Software zoals deze wordt inderdaad spyware genoemd. Spyware geeft stiekem gegevens over de gebruiker of diens PC door aan derden. Zo zijn er programma's die het surfgedrag van gebruikers bijhouden en dat doorgeven naar een centrale site, die zo passende advertenties kan aanleveren.

Spyware ligt juridisch in een grijs gebied. Het mag, maar de software moet voorafgaand aan installeren wel duidelijk melden wat er precies gaat gebeuren. En het is niet genoeg om dat alleen in de algemene voorwaarden (EULA) te doen. Hoewel EULA's juridisch bindend zijn, eist de wet meer dan alleen een contract: het moet "duidelijk en nauwkeurig" gemeld worden op "voldoende kenbare wijze". Oftewel het moet als bulletpoint in de installatieprocedure naar voren komen, en je moet dan nog de gelegenheid krijgen om "nee" te zeggen en de installatie te annuleren.

DICHTBIJ
I-Phone app

Bij het opstarten van de app bepaal je eerst hoe je locatie wordt bepaald: per gps of door zelf te zoeken op regio, plaats of postcode. Daarna kun je ervoor kiezen om in te loggen zodat je ook zelf kunt bijdragen aan Dichtbij. Onder het kopje nieuws vind je vanzelfsprekend alle recente nieuwsberichten terug op chronologische volgorde. Je krijgt de kop te zien en de eerste twee regels; wil je meer lezen dan kan dat met een simpele tik.

Foto's van recente evenementen bekijken? Dat doe je onder het kopje foto's. Door op Doe mee te tikken kun je zelf een artikel of foto aan Dichtbij toevoegen of de redactie tippen. Dichtbij voert geen voorafgaande redactionele of inhoudelijke controle uit op de door gebruikers geüploade content, dus dit heeft vaak niet bijster goed geschreven stukjes vol met spelfouten tot gevolg, waarvan je je afvraagt wat ze nu eigenlijk bijdragen...

Juridische vraag: wanneer valt site onder cookiewet?

Vraag: Ik vroeg me af wanneer een website nu wel of niet onder de cookiewet valt. Wat is beslissend: de extensie (.nl of .com), de taal, waar de server staat of iets anders?

Antwoord: Sinds enige tijd geldt de zogeheten cookiewet. Een ietwat misleidende naam, want het gaat niet alleen over cookies in die wet. Elk lezen of schrijven van data op randapparatuur van eindgebruikers is verboden, tenzij daar toestemming voor is gegeven of dit noodzakelijk is voor een door de gebruiker gewenste dienst.
De cookiewet komt uit Europa maar is omgezet in een Nederlandse wet. En daar is ook nog eens een Nederlands sausje overheen gedaan om het privacytechnisch net wat strenger te krijgen. Zo is het bij ons verplicht om expliciet toestemming te vragen, terwijl je in Engeland mag volstaan met "hoi wij zetten cookies, wilt u dat niet dan moet u dat even uitzetten".

Je valt onder de Nederlandse wet wanneer je je met je website "richt op Nederland". Daar is niet één criterium voor. Je moet de gehele website en alle bijkomstige omstandigheden bekijken en dan een inschatting maken. De Nederlandse taal is niet genoeg (want België), maar onze taal plus iDeal-betalingen plus de tekst "gratis levering in heel Nederland" zou ik wel genoeg vinden.

Ook als de extensie .com was en de servers in zeg Duitsland staan. Niemand kan met droge ogen beweren dat Bol.com een buitenlandse website is. En voor Facebook durf ik die discussie ook wel aan, met hun Nederlandstalige interface en marketing alhier.

Wapen uit de 3D-printer

Het machinegeweer dat een wapensmid fabriceerde met een 3D-printer, is nu een open source-project. Defense Distributed wil met 'Wiki-Wapens' vuurwapens in de handen van iedereen stoppen.

WikiWeps is een project waarmee een werkend wapen wordt gemaakt dat door 3D-printers wordt geproduceerd. Oprichter Defense Distributed zamelt de komende tijd geld in voor dit streven.

Ondertussen proberen de initiatiefnemers een community op te zetten van enthousiaste hobbyisten die bijdragen aan een vuurwapen dat uit de printer komt rollen.

Het is al bewezen dat het goed mogelijk is om een 3D-printer te gebruiken voor huis, tuin, keuken en munitieloods-doeleinden toen een uitvinder vorige maand een systeemkast printte. Dit is de primaire behuizing van een vuurwapen waar alle onderdelen in verwerkt worden, zoals het trekkermechanisme en wapenmagazijn.

Wapensmid Michael Guslick dupliceerde de metalen systeemkast van een M16 naar een variant van duroplast. De uitvinder vuurde naar eigen zeggen tweehonderd schoten af zonder dat dit hoofdonderdeel beschadigingen opliep. Al meteen na de succesvolle test, publiceerde de wapensmid uitgebreide CAD-tekeningen online zodat hobbyisten er zelf mee aan de slag kunnen. Dit ontwerp wordt nu gebruikt voor de Wiki-Wapens.

Geen vergunning nodig

Amerikanen mogen zonder vergunning wapenonderdelen aanschaffen en zelf assembleren. De kunst is dan ook om naast de systeemkast ook al die andere wapenonderdelen te produceren. Zo zijn de loop en het wapenmagazijn in het eerste ontwerp nog van metaal. De wikipagina is helder over het einddoel: "Een volledig functionerend vuurwapen van thermoharder printen."

Omdat de systeemkast de feitelijke behuizing is van vuurwapens, is deze specifiek genoemd als een onderdeel van de Amerikaanse wapenwet. Daarom wordt dit onderdeel speciaal samen met geluidsdempers en explosieven gereguleerd. Het idee dat mensen nu een wapen in elkaar zouden kunnen zetten zonder vergunning, is angstaanjagend te noemen.

Iedereen aan de wapens

Het doel van de wiki is om het iedereen mogelijk te maken zelf een wapen te printen. De makers hebben het niet zo op overheidsbemoeienis die het Tweede Amendement in de weg staan. Op het blog van Defense Distributed stelt oprichter Sean Kubin bijvoorbeeld dat de bioscoopschietpartij in Colorado vorige maand voorkomen had kunnen worden als iedereen wapens bij zich droeg.

De weg naar een gecrowdsourcet vuurwapen is niet zonder tegenslagen. Crowdfunder Indiegogo sloot de publieke inzamelingsactie van Defense Distributed omdat critici het project markeerden als ongepast. De oprichters hebben al 2000 van de beoogde 20.000 dollar ingezameld en zijn nu in gesprek met Indiegogo om dit geld vrij te krijgen.

Hoe werkt een 3D printer?
Er zijn verschillende soorten 3D printers op de markt. Ze verschillen allemaal in de manier waarop ze 3D printen. Hieronder worden de twee meest gebruikte toegelicht.

Verlijmen van fijne poeder of het opspuiten van een latexachtige substantie. Deze type machines verlijmen telkens een laagje poeder (of latex) op het 3D model waardoor het zijn hardheid krijgt. De printer kan heel secuur bepalen waar wel en geen poeder/latex en lijm komt. En ook bijvoorbeeld welke kleur poeder, zodat gekleurde vlakken kunnen worden gecreëerd.

Andere types werken met een hoofd- en vulpoeder. De 3D printer smelt of plakt zowel het hoofdpoeder als het vulpoeder in het 3D model. De onderdelen van het uiteindelijke fysieke 3D model worden met het hoofdpoeder gedaan. Openingen en holle ruimtes worden door het vulpoeder opgevuld.

Bijvoorbeeld een muur met een raam erin. De muur wordt opgebouwd met het hoofdpoeder, en het raam waar je dus geen plastic wenst, wordt gevuld/gelijmt met het tijdelijke vulpoeder. Als men klaar is met het opbouwen van het 3D model wordt deze verwarmd en dit zorgt ervoor dat het vulmiddel wegsmelt en uit het 3D model loopt. Wat men vervolgens overhoudt is het 3D model.

Bekijk hier de video

Plug-in beschermt Facebook foto's tegen pottenkijkers

Anti-virusbedrijf McAfee heeft een gratis bètaversie gelanceerd van een programma dat foto's op Facebook tegen ongeautoriseerd gebruik moet beschermen, zoals delen, bekijken of downloaden. McAfee Social Protection bestaat uit een Facebook-app en een browser plug-in, waarmee gebruikers precies kunnen bepalen wie van hun Facebook-vrienden welke foto's kunnen zien.

Voor alle andere gebruikers worden de foto's onscherp gemaakt. Vrienden die toestemming hebben gekregen, kunnen de foto's pas zien wanneer ze de Facebook-app installeren.

"Naarmate consumenten steeds meer van hun leven online delen met anderen via foto's op Facebook, worden ze ook steeds kwetsbaarder doordat ze niet kunnen controleren waar die foto's uiteindelijk terechtkomen", zegt senior vice president Brian Foster.

Downloaden
Het programma zou ook voorkomen dat er screenshots van foto's gemaakt worden. In plaats daarvan verschijnt alleen een blanco plaatje. De app schakelt tevens de optie uit om foto's te bewaren of te downloaden via de browser. Er wordt een icoon van een hangslot over de foto getoond zodra een gebruiker er met de muis overheen gaat.

Dit is mogelijk doordat de foto's die gebruikers met deze app beschermen, niet op de Facebook-servers terecht komen, maar bij McAfee. Het programma werkt alleen op computers met Internet Explorer en Firefox.

Facebook sollicitant bekijken maakt bedrijven ongeliefd

Bedrijven die sollicitanten screenen door hun profiel op Facebook of andere sociale netwerksites te bekijken maken zich zowel bij huidige als toekomstige werknemers ongeliefd. Dat blijkt uit onderzoek waar 175 proefpersonen aan deelnamen. De deelnemers solliciteerden naar een fictieve baan waarvan ze dachten dat die echt was. Nadat de sollicitanten hoorden dat ze gescreend waren, waren ze minder geneigd om de baan te nemen.

Volgens de proefpersonen straalde de screening af op de eerlijkheid van de organisatie en de manier waarop het met werknemers omgaat. Ook vonden ze dat hun privacy was geschonden. Uit eerder onderzoek blijkt dat 65% van de organisaties sociale media gebruikt om sollicitanten te screenen. Op deze manier hopen de organisaties het kaf van het koren te scheiden.

"Door dit te doen ga je ervan uit dat de sollicitanten die bedrijven kiezen bewuster zijn, maar er is geen onderzoek dat aantoont dat deze individuen beter zijn", zegt Will Stoughton van de North Carolina State University. "Het kan dat ze zelfs de betere sollicitanten laten liggen."

Het screenen zou niet alleen effect op sollicitanten hebben, ook huidige werknemers zouden hierdoor de organisatie kunnen verlaten.

"Facebook-weigeraars bij voorbaat verdacht"

Mensen die geen Facebookprofiel hebben zijn bij voorbaat verdacht en lopen kans om bij bedrijven niet te worden aangenomen, zo meldt het Duitse Tagesspiegel. Het magazine wijst naar psychopaten als Anders Breivik en James Holmes, die niet op de sociale netwerksite actief waren. Inmiddels zouden ook HR-managers sollicitanten die geen Facebook-profiel hebben afwijzen omdat ze iets te verbergen hebben. Geen Facebook is geen baan.

Wie zich niet op sociale media begeeft is nu bij voorbaat verdacht. "Het internet is onderdeel van het dagelijks leven", zegt psycholoog Christoph Möller. Hij merkt op dat gebruikers van Facebook en andere netwerken hier "positieve feedback" kunnen vinden, maar er niet verslaafd aan moeten worden.

In het geval van de Noor Breivik was die goed als onzichtbaar op internet en alleen op bepaalde fora actief. Wat 'bioscoopschutter'' Holmes betreft had de man zowel op Facebook als in het echte leven geen vrienden.

Veilig Facebook voor iedereen – gratis boekje

Wil jij ook je Facebook zo instellen dat jij bepaalt wat anderen zien?

Wil jij ook controle over je privacy?

Download dan nu het gratis boekje en binnen tien minuten ben jij ook weer veilig!

Printbaar
Het boekje is zo opgezet dat je het eenvoudig kunt printen voor als je dat makkelijker vindt.

Klik hier voor de download!

Hack preventie

Misbruik van simpele Google-authenticatie

Schakel direct Googles tweestaps-verificatie in. Dat betekent dat je eerst een extra code moet invoeren die naar je mobiele telefoon wordt toegezonden, voordat je het wachtwoord van je account kunt aanpassen. Bovendien krijgt niemand vanaf dat moment meer (een deel van) het mailadres te zien dat voor die wachtwoordwijziging wordt gebruikt. En zelfs als de booswichten toch op dat mailadres zouden inbreken, dan nog zou dat niet voldoende zijn om je Google wachtwoord te veranderen en je account over te nemen. De tweestaps-authenticatie beveiligt je account sowieso beter tegen hacks: ook als ze onverhoopt je wachtwoord in handen krijgen, kunnen ze het nog niet meteen wijzigen.

Toegegeven: het is wel wat omslachtiger om eerste en extra code naar je telefoon te laten sturen, maar het is en stuk leuker dan een gehackt account.

Om tweestaps-authenticatie in te schakelen ga je naar het drop-down menu rechts bovenin naast je fototje (of klik op je naam). Klik op Accountinstellingen en kies in het linker menu de optie Beveiliging. Bij Verificatie in twee stappen klik je (mits bij Status: UIT staat natuurlijk) op de knop bewerken. Je krijgt dan aanvullende informatie en wordt vanzelf (in het Engels!) door de rest van de procedure heen geleid.

Tijd: Het inschakelen van tweestaps-authenticatie vanuit je browser kost misschien drie minuten. Als je vervolgens vanaf andere apparaten of vanuit andere browsers inlogt kost je dat pakweg twee minuten om de authenticatie via je telefoon te doorlopen.

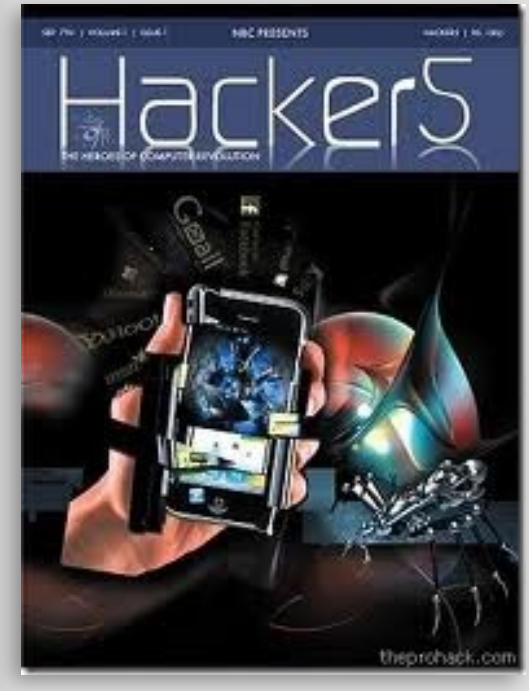
Nadeel is wel dat je dit iedere 30 dagen moet herhalen voor iedere browser waarin je je Google-account gebruikt.

Meerdere mailadressen met dezelfde gebruikersnaam

Het is niet echt hogere wiskunde om vanaf nu enige variatie aan te brengen in de gebruikersnamen die je gebruikt binnen verschillende domeinen, maar het is wel een maatregel die het weer wat lastiger maakt om via social engineering een wachtwoord-wijziging los te peuteren voor je account.

Helaas is het niet altijd wenselijk om de prefix (gebruikersnaam) aan te passen van mailadressen die je al langere tijd in gebruik hebt.

Als je alleen de prefix aanpast van een mailadres dat je toch weinig gebruikt, kost je dat vijf, hooguit tien minuten. Helaas kost het aanzienlijk meer tijd als je allerlei mensen en/of instanties op de hoogte moet brengen van je nieuwe adres.



Conclusie

Kun jij je email, sociale media en alle andere online accounts voor de volle honderd procent beveiligen tegen hackers?

Dat lijkt zeer onwaarschijnlijk. Maar als je ev wat tujd vrijmaakt om bovenstaande te regelen te nemen, kun je er in elk geval voor zorgen dat je de risico's een aanzienlijk stuk kleiner maakt.

Gevoelige gegevens opslaan op je mobiele apparaat

Hackers zitten echt niet achter een boom te wachten tot je telefoon uit je zak valt, maar aan de andere kant is je mobiele apparaat op een bepaalde manier misschien nog wel aantrekkelijker om te stelen dan je portemonnee. Bovendien blijken mensen hun telefoons opvallend vaak te verliezen of ergens te 'vergeten'. Maar stel je eens voor wat een handige hacker allemaal kan doen als hij eenmaal toegang heeft tot je apps en je email-accounts.

De oplossing: Eigenlijk is het simpel: als je telefoon je huis verlaat en je hebt er je email, je sociale media, en wie weet wat voor winkel- en thuisbankieroplossingen op draaien, dan moet je er absoluut voor zorgen dat het toestel beveiligd is met een pincode of wachtwoord. Je vindt dat soort opties onder Instellingen. Eventueel kun je de beveiliging nog uitbreiden met extra apps die het mogelijk te maken een vermiste telefoon terug te vinden of op afstand te wissen, zoals bijvoorbeeld Zoek mijn iPhone of Avast! Mobile Security voor Android.

TIPS&TRUCS

LibreOffice 3.6.1 is uit!

LibreOffice is kantoorsoftwarepakket dat u gratis kunt downloaden en installeren. Wereldwijd is er een grote groep tevreden LibreOffice-gebruikers. Het programma is verkrijgbaar in meer dan 30 talen, waaronder het Nederlands, en voor alle bekende besturingssystemen, zoals Mac OS X, Microsoft Windows, en Linux (Debian, Ubuntu, Fedora, Mandriva, ...).
U kunt LibreOffice downloaden, installeren en doorgeven zonder beperking, zonder bang te hoeven zijn voor het schenden van auteursrechten of andere licentie-bepalingen.

download

Wat biedt LibreOffice u?

Writer is de tekstverwerker binnen LibreOffice.
Te gebruiken voor alles van het vlot opstellen van een brief tot en met het produceren van een compleet boek met inhoudsopgaven, illustraties, bibliografieën en grafieken. Er zijn functies die u helpen om moeilijk werk makkelijk te maken, zoals automatische woord-aanvulling, auto-opmaak en automatische spellingscontrole maar deze functies zijn ook zeer eenvoudig uit te schakelen als u dat wenst. Writer is krachtig genoeg om desktoppublishing taken aan te kunnen, zoals het maken van nieuwsbrieven met meerdere kolommen en folders. Writer geeft volop de ruimte aan uw fantasie.

Calc temt uw getallen en helpt met moeilijke beslissingen als u de alternatieven wilt analyseren.
Analyseer uw gegevens met Calc, en gebruik het om uw uiteindelijke resultaat te presenteren.
Grafieken en analyse-gereedschappen zorgen dat u goed onderbouwde beslissingen inzichtelijk kunt tonen. Een volledige geïntegreerde assistent zorgt dat het invoeren van complexe formules eenvoudiger is. Gegevens van externe databases, zoals SQL of Oracle, kunnen worden toegevoegd gesorteerd en gefilterd voor statistische analyses. Gebruik de grafische functies voor het tonen van grote aantallen 2D en 3D grafieken uit 13 categorieën, waaronder lijn, vlak, staaf, taart X-Y, en net – met tientallen beschikbare variaties. U vindt er zeker een die geschikt is voor uw project.

Impress is de snelste en makkelijkste manier om effectieve multimedia-presentaties te maken.
Uitgebreide mogelijkheden met animaties en speciale effecten om soms net een beetje extra te geven. Maak presentaties die nog er nog professioneler uit zien dan de standaard presentaties die u gewoonlijk ziet op het werk. Krijg de aandacht van uw bazen en collega's met iets dat net even anders is.

Draw laat u uit het niets tekeningen, diagrammen en 3D beelden maken.
Een plaatje zegt meer dan duizend woorden. Dus waarom niet iets geprobeerd met eenvoudige blokken of stroomdiagrammen? Of ga een stap verder en maak op een simpele manier dynamische 3D illustraties en bijzondere effecten. Het is zo simpel en krachtig als u het wilt hebben.

Base is het database front-end van het LibreOffice pakket.
Met Base kunt u uw bestaande gegevens opslag naadloos integreren in de andere componenten van LibreOffice, of een interface maken om als standalone programma uw gegevens gebruiken en bijhouden. U kunt gebruik maken van gekoppelde tabellen en query's uit MySQL, PostgreSQL of Microsoft Access en vele andere bronnen van gegevens, of ze zelf ontwerpen in Base, om krachtige front-ends te bouwen met knappe formulieren, rapporten en views. Ondersteuning voor een groot aantal databases is ingebouwd of eenvoudig te verkrijgen.

Math is een programma voor vergelijkingen. Het laat u formules maken en tonen voor uw wiskundige, chemische, elektronische en wetenschappelijke vergelijkingen. Vlot en in de gebruikelijke notatievorm. Zelfs de ingewikkeldste berekeningen worden begrijpelijk, als ze goed worden afgebeeld.

Asus GTX 660 Ti

nVidia introduceert de GTX 660 Ti. Een erg belangrijk model, aangezien dit de sweet spot hoort te zijn van prijs en prestatie. Als we terug kijken naar de GTX 460 Ti en 560 Ti, heeft nVidia ook altijd hoge ogen gegooid in het hoge middensegment, of lage high-end segment. Gaat het ze weer lukken?

De nieuwe GTX 660 Ti is, net als de high-end GTX 680 en GTX 670 gebaseerd op de GK104 Kepler-chip. Hij heeft dan ook alle leuke features van de twee topmodellen. De GK 104 is in maart geïntroduceerd en was in eerste instantie helemaal niet bedoeld voor het high-end segement. Dat zegt de nummering ook (eindigend op een 4 is middensegment). Echter: de chip bleek zo snel – hij was sneller dan de AMD HD7970 – dat nVidia heeft besloten met deze chip verder te gaan.

De GK104 heeft – in zijn volledige vorm – 1536 shader units en een 256 bit geheugenbus. De 'beperkte' geheugenbus verraadt overigens ook zijn midrange-roots. De gpu tikt op 1006 MHz met een boost naar 1058 Mhz. De 2GB geheugen werkt op 1502 Mhz.

Concurrentie!

De GTX 660 Ti is in basis een concurrent voor de HD7870. Echter, nVidia gokt dat hij ook kan concurreren met de HD7950 die een stuk duurder is. En aangezien de Kepler-chip kleiner en goedkoper te fabriceren is, zal AMD niet zijn prijzen kunnen drukken. Vervelend. Echter AMD heeft een oplossing: een nieuw bios dat een turbofunctie toevoegt, waardoor de HD7950 zijn kloksnelheid – net als nVidia – kan verhogen. Van 800 naar 925 MHz om precies te zijn.

Benchmarks

Asus heeft ons voorzien van een GTX 660Ti DirectCU II TOP. Een overklokte versie van de GTX 660 Ti. En niet zomaar een overklok, maar een forse: 17 procent. De Top-versie draait op 1072 MHz met een boost van 1137 MHz. Lekker hoor!

We hebben de Asus GTX 660 Ti op ons X79-platfom getest waar we begin dit jaar ook de massatest op hebben uitgevoerd. Zo zijn de kaarten goed te vergelijken. Op het moederbord leggen we een Core i7 3960X processor en zetten we 16 GB ram (4 x 4 GB). De schijf is een WD Velociraptor 150 GB. Het besturingssysteem is Windows 7 X64.

Niet geheel verwonderlijk scoort de Asus bijzonder goed. We zien een 3DMark vantage-score (performance) van 32.061 punten. De 3DMark 7-score is 8917 punten, wat hoger is dan een standaard GTX 670.

We testen nu ook Battlefield 3 op Full-HD en settings op medium en Ultra (4xAA). Ook daar heeft de GTX 660 Ti Top geen moeite mee. We zien met medium-settings 108 fps en op Ultra nog steeds 54 fps. Echt een goede score.

Dirt 3 is een fluitje van een cent. Net zo snel als de GTX 670: 105,5 fps op 1920 x 1080 met alles op maximaal. Wat een beest is deze kaart zeg!

Asus GTX 660 Ti Top

nVidia heeft echt een killerkaart in het assortiment.
Voor ongeveer 300 euro (officiële prijs nog niet bekend) zet het bedrijf een videokaart in de markt die op niveau van de HD7950 kan opereren en zelfs de eigen GTX 670 end-of-life maakt.

Of dat laatste echt de bedoeling was, is nog onduidelijk. Het zegt wel hoe goed de GTX 660 Ti is. Zeker het model van Asus dat lekker gekieteld is!
Voordelen

- **Erg snel**
- **Energiezuinig**
- **Nette prijs**

Prijs

€ 300.00

Apps

Verslaafd aan apps? Vier dingen die u moet weten voordat u gaat downloaden!

Wat apps en widgets betreft, zijn de gebruikers van vandaag net kinderen in een speelgoedwinkel. In de afgelopen paar jaar is de markt overspoeld met betrouwbare apps (ruim een halfmiljoen voorde iPhone alleen al), maar zoals te verwachten valt, zijn er criminelen die hiervan misbruik willen maken.

Gelukkig kunt u door alleen al te beseffen dat deze bedreigingen bestaan, uzelf en uw Android™, iPhone® of Windows® Phone beschermen. Dus denk aan deze vier dingen voordat u nonchalant uw volgende app of widget downloadt.

1) Van wie en waar is het afkomstig?

Een van de mooie dingen van apps is dat iedereen ze kan maken, dus niet alleen grote bedrijven, maar ook die jongen van 10 jaar die nog op de basisschool zit. Het nadeel is...dat iedereen ze kan maken, dus ook een cyberdief met slechte bedoelingen.

Voordat u op die downloadknop klikt, controleert u daarom best eerst of de app afkomstig is van de officiële markt of het platform waar u op zit. Android heeft een helder contentbeleid voor hun officiële Android Market, en mocht een stukje malware de kop op steken, dan wordt dat snel door de Android-engineers van Google vernietigd. De Apple® App Store heeft soortgelijke controlerichtlijnen en regels om te zorgen dat u (en uw kinderen) geen last hebben van schadelijke of ongeschikte content.

Controleer ook of een app een goede beoordeling heeft en vaak wordt gedownload. Dit zijn twee heel duidelijke aanwijzingen van de goede bedoelingen van een app.

2) Vermijd peer-to-peer als de pest.

De kans is groot dat u er niet op uit bent gestolen apps en widgets vanaf een ondergronds peer-to-peer-netwerk te halen.
Deze websites voor het delen van bestanden zijn gevoeliger voor malware en Trojaanse paarden, zoals die ene die zorgde dat een genante sms naar het hele telefoonboek van gebruikers werd gestuurd.
Maar als u het niet kunt weerstaan om geld te besparen door een app of widget van een p2p-netwerk af te halen, wees dan heel voorzichtig. En zeg niet dat wij u niet gewaarschuwd hebben.

3) Lees de kleine lettertjes.

Wanneer u een app downloadt, wordt u vaak gevraagd de ontwikkelaar toegang te bieden tot bepaalde informatie en toestemming te geven voor bepaalde handelingen, zoals de app toestaan om te voorkomen dat uw telefoon naar de slaapstand overschakelt en om te zien wie gebruikers bellen en waar ze vandaan komen.
Vaak wil een app ook toegang tot de internetverbinding van uw telefoon. Kijk goed naar wat de ontwikkelaar vraagt, met name dingen als toestemming voor het telefoneren of sms'en vanaf uw telefoon. Dit kan door scammers worden gebru
ikt om uw telefoonrekening op te drijven.

4) Zorg voor een goede beveiliging.

In het vorige magazine heb ik u gewezen op Mobile Security en de daarbij behorende gratis beveiligingsprogramma's.

Nog niet geïnstalleerd?

DOE HET DAN NU!

Studeren doe je ~~bij~~ ~~de NCOI~~ met YouTube!

De tijd dat YouTube alleen bestemd was voor zelfgemaakte videofilmpjes en het bekijken van muziekclips, ligt inmiddels achter ons.

Misschien wist u het niet, maar YouTube is onderdeel van het Nieuwe Leren.

Zeker op gebied van PC en internet zijn er legio filmpjes te bekijken. U kunt hier uw voordeel mee doen.

Hiernaast een kleine opsomming van mijn reis door YouTube land.

Hoe herken je phishing mails?

Hack MySpace passwords

FiNBOX hoe werkt het

Hoe hack je een router password voor gratis internet (wifi)

Documentaire: Veiligheid en Privacy

Privacy - Ik heb toch niets te verbergen?

Verleiding van de Misdaad

Veilig Politiewerk

Gezag op straat...als het moeilijk wordt!

Kun jij beslissen wat de hoogste prioriteit heeft? Screen jezelf.

Mobiele Eenheid, achter de schermen

Privacyinstellingen Facebook Timeline

Opstartproces van uw pc versnellen

Recente variaties op de *Nigerian Scam*

Een dure raskitten/pup die anders geen leven heeft; de aanbieder stuurt hem gratis op, maar uiteindelijk moet men een ticket betalen, douanekosten, daarna dierenartskosten, dan inentingskosten etc. Ook wordt wel eens misbruik gemaakt van personen die een huisdier zijn kwijtgeraakt en advertenties hebben geplaatst om het dier op te sporen.

De oplichter beweert het dier gevonden te hebben en kan dit door de advertentie ook vrij nauwkeurig beschrijven. Omdat hij het dier onderweg op de snelweg zou hebben opgepikt is en verder moest, is het nu wel in een uithoek van Europa beland. De 'vinder' is bereid het dier op het vliegtuig terug naar Nederland te zetten maar wil wel de vervoerskosten vergoed zien, plus wellicht een 'vindersloon'.

Hier wordt misbruik gemaakt van de emoties van baasjes die hun huisdier zijn kwijtgeraakt.

De oplichter doet zich voor als kredietverlener en biedt leningen aan aan personen die bij reguliere banken hier niet voor in aanmerking komen (bijvoorbeeld wegens een slechte kredithistorie).

Alvorens de lening wordt uitbetaald wordt eerst betaling van transactiekosten of zelfs aflossingstermijnen verlangd. De lening wordt uiteraard nooit betaald.

Een oplichter mailt namens een (landbouw)bedrijf in Afrika. De kosten van een bepaalde grondstof zijn in Afrika hoog, en de oplichter kan deze in Europa de helft voordeliger krijgen.

Omdat de oplichter met ontslag bedreigd wordt is dit voor hem een uitgelezen kans om bij zijn baas een goede beurt te maken.
Uiteraard heeft hij te weinig contacten in Europa om zelf de grondstoffen aan te schaffen en vraagt het slachtoffer om kosten voor te schieten met uitzicht op wel 20% van de winst

Het slachtoffer wordt gevraagd mee te werken aan het wegsluizen van gelden afkomstig van de verkoop van bloeddiamanten.

Als beloning wordt het slachtoffer een deel van het geld beloofd.

Een familielid van een (ex-)dictator (Sani Abacha of Mobutu Sese Seko) wil diens fortuin via een buitenlandse rekeninghouder het land uit smokkelen.

Als beloning wordt het slachtoffer een deel van het geld beloofd.

Een rijk familielid in een ver land is overleden zonder naaste familie. Het slachtoffer is 'toevallig' een zesdegraads familielid en erft daarom de gehele nalatenschap. H

Het slachtoffer zou zich echter moeten afvragen waarom zijn broers en zussen (die even veel familie zijn) niets hebben ontvangen.

Sommige ontvangers laten zich niet beetnemen, maar doen net alsof ze dat wel doen. Ze schrijven enthousiaste berichten terug vanaf niet-traceerbare anonieme e-mailadressen, waarna er een uitgebreide correspondentie ontstaat.
Beide beloven het geld spoedig over te maken, maar steeds blijkt er iets gebeurd te zijn waardoor men die belofte voorlopig niet kan nakomen.
Naast het hiermee verspillen van hun tijd, wordt ook op verschillende manieren geprobeerd om de oplichter zelf op kosten te jagen, hetgeen af en toe lukt. Ook wordt geprobeerd de oplichter een foto van zichzelf te laten opsturen met soms een compromitterende of belachelijke tekst in zijn handen.

Veel van deze hilarische briefwisselingen en gebeurtenissen zijn op het internet terug te vinden

Bekijk hier de video

Handige hulpprogramma's voor je PC

Onmisbare gratis gereedschappen

1. AutoRuns for Windows - technet.microsoft.com/en-us/sysinternals/bb963902

Laten we beginnen bij het begin. Letterlijk dan, want AutoRuns for Windows is een programma dat onderzoekt wat er allemaal samen met Windows wordt ingeladen als je pc opstart. Het probleem zit niet zozeer bij malafide medestarters, maar wel bij legitieme toepassingen, bijvoorbeeld programma's die een scanner of printer beter doen werken.

Allemaal goed en wel, maar als er zo veel zijn duurt het opstarten eeuwig en wordt de computer traag. AutoRuns geeft niet alleen een overzicht, maar biedt ook de mogelijkheid om startprogramma's te blokkeren.

2. Recuva - www.piriform.com/recuva
http://www.piroform.com/recuva
Soms doet een mens gewoon domme dingen. Zoals per ongeluk alle vakantiefoto's van een geheugenkaart wissen zonder dat je ze eerst had gekopieerd. Wat je dan nodig hebt is Recuva.
Dit gratis programma is heel sterk in het terugvinden en terugzetten van verwijderde bestanden. Niet alleen foto's op geheugenkaartjes trouwens, maar ook andere bestanden op USB-sticks of harde schijven.

3. Audacity - audacity.sourceforge.net

Er zijn best wat programma's die geluid kunnen bewerken of die een beltoon voor je telefoon kunnen maken. De meeste kosten echter geld en hebben zelden meer te bieden dan Audacity. Behalve betere looks misschien: als dit openbronprogramma één zwak punt heeft, dan is het wel de interface. Die oogt oubollig en onaantrekkelijk.

Maar laat dat je niet afschrikken, want Audacity heeft professionele functies. Zo kun je op meerdere sporen opnemen, crossmixen en meer.

4. Moo0 Window - www.moo0.com/software/WindowMenuPlus/

WindowsMenuPlus is zo'n typisch gereedschap dat weinig doet, maar dat je na een tijd echt niet meer kan missen. Het voegt extra functies toe aan het systeemmenu dat verschijnt als je rechtsklikt op een menubalk van een programmavenster.

Dankzij Moo0 kun je vanuit dit menu een proces stoppen (handig bij vastlopende programma's), het venster transparant maken of het proces een hogere of lagere prioriteit geven.

5. VLC - www.videolan.org/vlc

Er zijn mensen die tevreden zijn met Windows Media Player, maar ik hoor daar niet bij. Geef mij maar VLC, dat alles in zich draagt om zowat elk videobestand ter wereld af te spelen. Je hoeft dus geen aparte codeccollectie te installeren.

Het standaarduiterlijk van VLC is niet echt knap, maar je kunt aparte skins downloaden en installeren. Ondersteuning is er eveneens voor ondertitels, het afspelen van dvd's en zelfs het omzetten van video.

Tips om je smartphonebatterij te sparen

Laat je batterij langer meegaan

1 – schakel bluetooth, wifi en gps uit
Bluetooth, wifi en GPS zuigen je batterij leeg. Als je niet moet weten waar je bent, of je hebt geen bluetooth carkit in de buurt, dan kan je die twee voorzieningen best uitschakelen. Ook wifi en 3G zuigen je batterij volledig leeg, dus als je niet online wil zijn kan dat ook best uitschakelen.

2 – verlaag je schermhelderheid
De schermverlichting is gemiddeld één van de grootste energieverslinders bij smartphones. Des te groter het scherm, des te meer het scherm gebruikt. Je helderheid automatisch laten verlagen en het standaard een pak lager zetten dan het maximum zal je al een eindje vooruit helpen

3 – Vliegtuigmodus
Als je geen bereik hebt of je bent in een gebied waar er enkel incompatibele netwerken zijn kan je best vliegtuigmodus aanzetten. Vliegtuigmodus stopt het constant zoeken naar beschikbare netwerken, iets waardoor je batterij opgelucht kan ademhalen.

4 – sluit apps
Apps die onnodig in de achtergrond blijven draaien kunnen een hel zijn voor je batterij. Sluit apps altijd volledig af als je ze niet meer nodig hebt

5 – fetch in plaats van push
Je emailcliënt kan vaak e-mails automatisch binnenhalen vanzodra ze op de server aanwezig zijn. In plaats van push – waarbij de server e-mails continu doorstuurt naar je smartphone kan je beter er voor kiezen om bijvoorbeeld elk uur mails op te halen, of manueel te controleren op nieuwe e-mails.

6 – enkel bellen
Gebruik, als het echt niet anders kan, je telefoon enkel als telefoon. Games en webfuncties verbruiken enorm veel energie, energie die je soms broodnodig hebt. Een smartphone is tenslotte nog altijd een phone – waarmee je belt.

Je batterij makkelijk monitoren

Android-widget om batterij in het oog te houden

Op Android zit standaard al een optie om te kijken welk deel van je smartphone het meeste energie wegzuigt uit je batterij, maar die is net iets te beperkt.

Met Battery Widget Reborn kan je in een handomdraai alle onderdelen van je batterijcapaciteit monitoren.

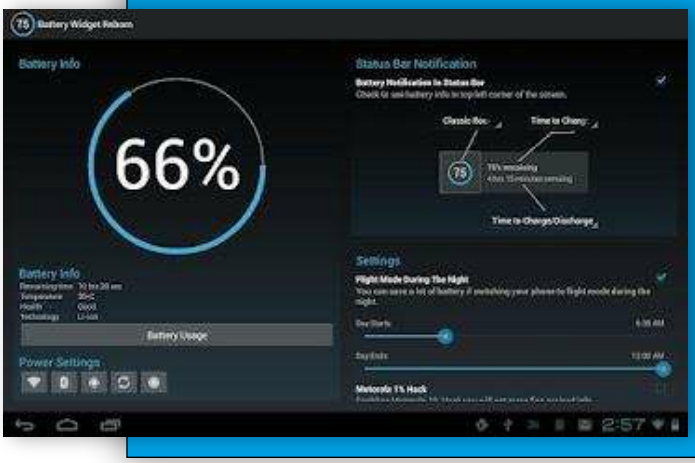
Zo heeft de app enkele handige functies, waaronder een voorspelling hoe lang je batterij nog mee zal gaan en kan de app automatisch de vliegtuigmodus inschakelen tijdens de nacht om de batterij nog meer te sparen.

De app geeft je ook uitgebreide statistieken over je batterijverbruik en kan wifi en Bluetooth uitschakelen wanneer je dat zelf wenst.

Je kan vanaf Android 4.1 Jelly Bean ook notificaties ontvangen en informatie verkrijgen over Wifi, Bluetooth en synchroniseren op de achtergrond.

Alsof dat nog niet genoeg is, ondersteunt de app ook eventuele extra batterijen zoals die bij de Asus Transformer reeks, waar het toetsenbord je batterijcapaciteit verdubbelt.

Battery Widget Reborn is beschikbaar in de Google Play Store en is vertaald naar het Nederlands.



Meeste Torrent-downloaders gemonitord

Internetgebruikers die via Torrents muziek, films en programma's downloaden worden op grote schaal gemonitord. Dat ontdekten onderzoekers van de Universiteit van Birmingham. BitTorrent downloadsites zoals The PirateBay worden zeker sinds drie jaar op grote schaal gemonitord. De onderzoekers gebruikten een honeypot server, die zich als onderdeel van 'file-sharing swarm' voordeed, een groep van internetgebruikers die bestanden uitwisselt.

Zo konden de onderzoekers de inkomende verbindingen onderzoeken en ontdekten al gauw de aanwezigheid van monitoringssystemen van copyrighthandhavingsinstanties, beveiligingsbedrijven en zelfs onderzoekslaboratoria van overheidsinstanties, zo meldt NewScientist. "We detecteerden alleen monitors in de Top 100 torrents, wat impliceert dat copyrighthandhavers alleen de populairste muziek en films op publieke trackers monitoren."

IP-adres
Het onderzoeksteam laat verder weten dat van iedereen die illegaal populaire films of muziek deelt zijn of haar IP-adres is opgeslagen. De vraag is nu wat de verschillende instanties met de verzamelde IP-adressen van plan zijn.

Volgens de onderzoekers zou het verzamelen van de IP-adressen niet voor een rechtszaak voldoende zijn. "Ze verzamelden geen van de gedeelde bestanden. Dus het is twijfelachtig of het waargenomen bewijs voor bestandsuitwisseling voor de rechter stand houdt."

Populaire vingerafdruklezer lekt Windows-wachtwoord

De vingerafdruklezer die op zeer veel laptops aanwezig is blijkt Windows-wachtwoorden niet goed af te schermen. Het gaat om de UPEK vingerafdruklezer die in op laptops van Asus Acer, ASUS, Dell, Gateway, Lenovo, MSI, NEC, Samsung, Sony en vele anderen aanwezig is. De software die ervoor zorgt dat gebruikers via hun vingerafdruk kunnen inloggen in plaats van een Windows-wachtwoord, blijkt het wachtwoord in bijna platte tekst in het register op te slaan.

Een aanvaller met fysieke toegang tot de laptop waarop de UPEK Protector Suite draait kan zo het Windows-wachtwoord achterhalen, zo ontdekte het Russisch softwarebedrijf ElcomSoft

Het bedrijf merkt op dat Windows zelf geen wachtwoorden opslaat, tenzij gebruikers voor 'automatisch inloggen' kiezen. In het geval van UPEK blijkt dat de ontwikkelaars voor de makkelijkste oplossing hebben gekozen door het originele Windows-wachtwoord op te slaan, waardoor aanvallers die kunnen bemachtigen.

Details
Inmiddels zou de UPEK Protector Suite niet meer met laptops worden geleverd, aangezien UPEK door een ander bedrijf genaamd Authentec is overgenomen. Toch is de software nog op talloze laptops te vinden. In publiek belang is ElcomSoft niet van plan om precieze details te openbaren.

Cyber security oefening Nederland en Duitsland

Nederland en Duitsland gaan samen een cyber security oefening organiseren, zo hebben beide landen gisteren in Den Haag afgesproken.

Minister Ivo Opstelten van Veiligheid en Justitie en de Duitse minister van Binnenlandse Zaken Hans-Peter Friedrich gaven aan de publiek-private samenwerking op het gebied van cyber security verder te willen versterken.

Hoe de oefeningen er precies gaan uitzien is nog niet bekend.

Nederland broeinest besmette websites

Kleine hostingproviders zijn de oorzaak dat Nederland het grootste aantal besmette websites in Europa, het Midden-Oosten en Afrika (EMEA) host.
Dat beweert McAfee in het nieuwste kwartaalrapport. 75% van alle gehackte en kwaadaardige websites die bezoekers in EMEA via drive-by downloads proberen te infecteren, staan in Nederland.

In het eerste kwartaal werd al duidelijk dat er in Nederland opmerkelijk veel besmette websites worden gehost. Deze trend heeft zich in het tweede kwartaal doorgezet.

Grote bestanden verzenden

Foto's of mp3's via e-mail versturen lukt meestal nog wel. Maar wat als je bijvoorbeeld een filmopname van 50 megabyte wilt versturen? De meeste e-mailproviders hebben een limiet aan de bestandsgrootte gesteld om te voorkomen dat je ongevraagd grote bestanden moet downloaden. Gelukkig zijn er alternatieven, waarvan wij er een aantal voor je geselecteerd hebben.

YouSendIt

Hoewel YouSendIt een betaalservice is, kun je er wel gratis bestanden versturen tot 100 mb. Het werkt als volgt: je vult het e-mailadres van de persoon aan wie je het bestand wilt sturen en je eigen e-mailadres in. Vervolgens selecteer je het bestand op je computer (maximale grootte 100 mb) en klik je op de 'send it' button. De ontvanger krijgt een e-mail met de versleutelde link naar het bestand en kan dan kiezen of hij het wil downloaden of niet.
YouSendIt

GigaSize

Is je bestand iets groter dan 100 mb en heb je geen zin om te betalen voor een 'pro-account' van YouSendIt, neem dan eens een kijkje bij GigaSize. Hoewel je je moet registreren, is een standaard account (tot 600 mb per bestand) gratis.
GigaSize

TransferBigFiles

Wil je nog grotere bestanden versturen, dan is TransferBigFiles wellicht iets voor jou. Je kunt hier tot 1 gigabyte per bestand versturen en het is wederom gratis.
TransferBigFiles

LEKKE DATABASES

DE RUSSEN KOMEN...!

Een nieuw type aanval teistert Nederland, waarbij niet alleen wordt ingebroken maar waarbij ook de beveiliging van een server wordt vernield. Is die eenmaal gehackt, dan betekent dat ook dat alle data open en bloot toegankelijk blijven. Het spoor loopt naar Rusland.

Onlangs stuitten we op een opmerkelijk artikel in het Russische tijdschrift *Hacker* [1]. In een aflevering van de rubriek EasyHack beschrijven Leonid Stroykom, Andrew Komarov en x0wl in detail wat een kwaadwillende na een inbraak kan doen om een achterdeur en extra databases aan te maken. Ze leggen uit welke zwakheden er in een systeem zitten en waarop hackers vooral moeten letten. Daarbij wordt niet alleen naar de MySQL-database gekeken, maar ook naar BIND (een DNS-server), de webserver-software op zowel Linux als Windows en hoe de kans op ontdekking wordt verkleind. Daarbij beschrijven ze ook hoe een script in een database kan worden achtergelaten. Het deed ons denken aan iets wat de laatste tijd in Nederland gaande is.

Nederland

Het is januari als duidelijk wordt dat KPN is gehackt. De zaak krijgt veel aandacht in de media, zeker als een lijst met mogelijke klantgegevens wordt gepubliceerd. Uw verslaggever toont aan dat deze van een compleet andere organisatie afkomstig is, namelijk de webwinkel Baby-Dump. De gegevens staan in een database zonder enkele beveiliging, die zonder omwegen kan worden benaderd. Wie met standaard MySQL-tools kan omgaan, heeft volledige toegang tot alle databases. Ondergetekende krijgt de data van een anonieme tipgever en daardoor is het veel werk om de bron van de informatie te herleiden.
Tegelijkertijd speelt een ander lek bij een klein reclamebureau. Deelnemers aan een wedstrijd van Bavaria staan in de database en ook dit exemplaar staat helemaal open. Een verschil is wel dat de hacker - die eveneens anoniem is - uw verslaggever vraagt om aangifte te doen. Hij of zij vermoedt misbruik en denkt dat het tijd is voor onderzoek. Het waarom van dit verzoek wordt nooit echt duidelijk. Ook is het buitengewoon lastig contact met de goedwillende hacker te onderhouden. Het reclamebureau doet aangifte, maar is niet bij machte om zelf een compleet dossier aan te leveren. De politie doet doorgaans geen forensisch onderzoek. En uiteindelijk bloedt deze zaak dood.
Wel vaker zien we volledig openstaande databases langskomen, maar een patroon van echte criminaliteit valt niet te bewijzen. Dat verandert in juli, als de internetprovider Proserve blijkt te zijn gehackt. Opnieuw staat een database volledig open en opnieuw gaat het om Baby-Dump, maar ook om de Telegraaf Media Groep, QMusic en andere organisaties. Ook ditmaal vraagt de hacker, een lid van het Nederlands Genootschap van Hackende Huisvrouwen [2], of de internetprovider aangifte doet. Want ook nu zouden er aanwijzingen voor vuil spel zijn te vinden.
Het verschil is dat deze hacker tekst en uitleg geeft. De databases waarvan de beveiliging is verwijderd, hebben een extra database met de naam *vuln*. Deze is doorgaans leeg. Toch is het een vorm van een handtekening, die door de naam - een afgeleide van *vulnerable*, kwetsbaar - lijkt te suggereren dat de machine lek is.

Test en vuln

Op basis van de beschikbare gegevens valt nog meer te ontdekken. Een hacker heeft de tijd genomen om alle bekende ip-adressen in Nederland langs te gaan op zoek naar dit soort inbraken. Daarbij valt op dat er veel databases zijn die geen wachtwoord hebben. Maar daar is het patroon anders en is er dus sprake van wanbeheer. Zeker honderd databases zijn toegankelijk met het beheerderswachtwoord admin of test. Niet echt het toonbeeld van goed beheer. In totaal zijn er honderden van zulke databases die een extra database binnen MySQL met de naam *vuln* of *test* hebben. Een ruwe schatting is dat er zeker tweehonderd databases in Nederland zijn opengezet.

Het primaire vermoeden is dat het gaat om één hacker die steeds beter in zijn vak wordt. Zo hebben eerdere *vuln*-databases geen inhoud, maar zijn er ook databases met inhoud. Daarbij gaat het dan om malware-scripts. En ook die scripts lijken, aldus het Nederlands Genootschap van Hackende Huisvrouwen, steeds beter te worden. Er is dus sprake van een progressie. En dan is er nog iets veranderd. De database *vuln* komt de laatste tijd steeds minder vaak voor. Nu verschijnt er een tabel met de naam *test*, waarin hetzelfde soort scripts staat.

Hoe groot is het probleem concreet? Om te beginnen heeft de aanvaller genoeg rechten op een systeem weten te krijgen, waardoor het mogelijk is om bij de database te komen - en mogelijk bij meer. Vervolgens kan hij meer systemen overnemen door bezoekers van de websites die bij de database horen, te infecteren met kwaadaardige software. Op dit moment is de malware nog niet slim genoeg, maar deze aanval valt verder uit te breiden naar een relatie tussen de gegevens van een bezoeker - die na inloggen duidelijk zijn - en het infecteren van een computer. Dat zou handig voor de aanvaller zijn, want dan weet hij ook precies bij wie hij de gegevens ophaalt. Tot slot wordt het wachtwoord van *root* ofwel het beheerdersaccount van de database ingesteld als niet-bestaand. Daardoor kan iedereen er opeens in.

Wat precies de bedoeling van die laatste stap is, blijft onduidelijk. Het plaatsen van een achterdeur bij hacks is op zich niet nieuw, maar dat het zo open en bloot gebeurt is wel bijzonder. Wie positief denkt, ziet een activist Anonymous-stijl voor zich, die hiermee het falen van een organisatie aantoont. Wie negatiever is, ziet een crimineel die het na de inbraak echt niets kan schelen dat hij schade achterlaat; hij heeft de buit immers al in zijn bezit.

Als meer mensen vervolgens dezelfde informatie stelen, dan maakt dat het alleen maar lastiger om de oorspronkelijke dader op te sporen. Wie bijvoorbeeld identiteitsdiefstal wil plegen, kan immers zijn gang al gaan. Aan de andere kant is het doorverkopen van informatie alleen aantrekkelijk op het moment dat de aanbieder een min of meer unieke positie heeft. Een andere mogelijkheid is dat iemand rustig bezig is een uitgebreide collectie persoonsgegevens op te bouwen die veel groter is dan je op het eerste gezicht zou zeggen.

Maar er is ook een andere optie. Het zou ook wel eens om meer individuele acties kunnen gaan en dan is het grotere verband moeilijker te vinden. Hiervoor blijken aanwijzingen te vinden in Rusland. In een aantal gevallen lijkt de aanval uit dat land afkomstig. Dat blijkt nadat een hacker bij een aantal servers diverse lekken heeft aangetroffen en zelf besloot de logboeken te analyseren. Toen bleek opeens dat sommige ip-adressen direct naar Rusland leidden. Veel criminele hackers daar nemen bij inbraken in de rest van Europa niet de moeite hun identiteit te maskeren, omdat ze in eigen land toch niet worden vervolgd voor computercriminaliteit in het buitenland.

Een extra bevestiging voor Russische betrokkenheid was het eerder genoemde artikel in het hackersblad. De daarin beschreven modus operandi was geen honderd procent match met wat in Nederland gebeurt, maar de overeenkomsten zijn verbluffend.

Een tweede groep verdachten bestaat uit 'hackers' die er geen benul van hebben waar ze precies mee bezig zijn en maar wat experimenteren. Die maken dan elementaire fouten, zoals in het wilde weg proberen te hacken en daarbij sporen achter te laten die wel erg snel naar hen terug leiden. Ook voor deze benadering zijn er aanwijzingen.

Meer problemen

Welke optie ook de waarheid zal blijken, inmiddels is wel een nieuw probleem duidelijk. Sommige zaken lopen al maanden en er zijn sporen dat een aantal inbraken al voor medio 2011 heeft plaatsgevonden. Dat blijkt uit de afwezigheid van sporen in logboeken, die na verloop van tijd geautomatiseerd worden gewist. Kennelijk gaan de initiële aanvallen ongemerkt aan het verantwoordelijke bedrijf voorbij. Daarnaast staan de databases soms maanden open. Daarbij is er wel iets fundamenteels veranderd: het beheerderswachtwoord is verdwenen.

Allemaal signalen die bij normaal beheer zouden moeten worden opgepikt - wat dus niet gebeurt. Veel organisaties regelen de meest basale zaken dus niet; ook zouden deze kwetsbaarheden met een paar scripts kunnen worden ontdekt.

Dit zijn allemaal signalen dat de problemen waarschijnlijk veel groter zijn dan we nu beseffen. Een beetje hacker laat namelijk geen makkelijk te ontdekken achterdeuren achter en stil groeten is bij de professionele criminelen al helemaal taboe.

Cookies en privacy

De cookiewet is er gekomen vanwege zorgen over de privacy. Doet het cookie ook maar iets op het gebied van gegevensvastlegging over het gebruik van verschillende diensten door de gebruiker - bijvoorbeeld analyse van bezoek vanaf diverse websites - dan bepaalt de Nederlandse wet dat dit 'vermoed wordt' onder de Wet bescherming persoonsgegevens te vallen. Vermoed, dus de bewijslast ligt bij de webmaster dat hier géén sprake van is. Een cookie dat onder deze privacywet valt, mag alleen met ondubbelzinnige toestemming op uw computer worden gezet.

Maar er is meer. Organisaties die persoonsgegevens verzamelen of gebruiken, hebben een informatieplicht. Dit betekent dat zij de personen op wie de gegevens betrekking hebben, moeten laten weten wat ze met hun gegevens gaan doen, en wel vooraf.

Daarnaast hebben personen die in een bestand zijn opgenomen, het recht om hun geregistreerde gegevens in te zien, en om te vragen hoe en waarvoor deze worden gebruikt. Een websitebezoeker kan dus opvragen wat een site of adverteerder via cookies allemaal bijhoudt.

WAT SCHIET UW PRIVACY ERMEE OP?

COOKIEWET

Een cookie is eigenlijk niets meer dan een tekstbestandje dat een website op de computer van bezoekers plaatst. In zo'n file staat een code, die bij elk vervolgbezoek aan die website door de browser wordt meegestuurd. Met die code kan de website bijvoorbeeld een eerder gemaakte keuze vastleggen, een ingevuld e-mailadres onthouden of het winkelmandje van vorige keer herstellen. Maar zo kan de bezoeker ook worden gevolgd, waarbij precies wordt bijgehouden welke pagina's hij bezocht en hoe lang.

Met name die laatste optie is aantrekkelijk voor adverteerders. Als ze weten wat iemand leuk vindt, kunnen ze hem een advertentie voorschotelen die daarbij past. En ze kunnen niet alleen de voorkeuren van de bezoeker op één site bijhouden, maar ook over diverse sites heen.

Advertenties worden namelijk op diverse websites ingevoegd vanaf één systeem van de adverteerder. Bij elk invoegen wordt een cookie geplaatst of uitgelezen. Wie dus eerst site A bezoekt en dan site B, stuurt bij site B informatie naar de adverteerder die bij site A een cookie liet plaatsen.

Op die manier kan de adverteerder de bezoeken aan A en B koppelen en daaruit conclusies trekken. Is A de sportpagina van Nu.nl en B de site Autoweek.nl? Aha, dan zal deze bezoeker wel een man zijn. Ging men daarentegen van de Achterklap-pagina van Nu.nl naar de Viva? Dan is dit hoogstwaarschijnlijk een vrouwelijke bezoeker.

Profielen samenstellen

En het blijft niet bij zulke algemene conclusies. Door maandenlang het bezoekgedrag bij te houden ontstaan heel gedetailleerde profielen. Die zijn buitengewoon waardevol voor het bedrijfsleven. Zo kan worden geadverteerd op het niveau van 'mannen 35-50 met een iPad en vakantieplannen, regio Noord-Holland'.

Dat idee van 'ze weten precies wat u online uitspookt' gaf aanleiding tot de 'cookiewet', die per 5 juni bepaalt dat een website voor elk cookie toestemming moet vragen. Ja, elk cookie, ook als het bestandje bezoekers helemaal niet volgt over diverse websites heen of eigenlijk niet eens wordt gebruikt om überhaupt bij te houden wat bezoekers doen.

De enige uitzondering werd gemaakt voor de 'technisch noodzakelijke' cookies, die integraal onderdeel van de techniek van een dienst zijn. Voorbeelden zijn het exemplaar dat vastlegt wat u vorige keer in uw winkelwagentje deed en het bestandje dat onthoudt dat u *Nee* antwoordde op de vraag 'Wilt u meedoen aan onze enquête?', zodat u niet wéér die pop-up met die vraag bij uw volgende bezoek krijgt voorgeschoteld.

Irritant

Toestemming krijgt een site alleen als deze erom vraagt. Het eenvoudigst gebeurt dat door middel van een pop-up. Zo'n schermpje is niet te missen en drukken op de *Akkoord*-knop geldt natuurlijk als toestemming. Maar irritant is het wel. De meeste mensen zullen geneigd zijn blindelings op het kruisje of *Nee* te klikken, gewend als ze zijn aan het wegklikken van pop-ups die vragen of u wilt meedoen aan een enquête of die u een nieuwsbrief aanbiedt.

Een andere populaire optie is een mededeling bovenaan - of onderaan - elke pagina waarop cookies kunnen worden gezet. De bezoeker kan die mededeling dan verwijderen door te klikken op *Ja, ik wil een cookie* of een vinkje te zetten bij die mededeling.

Tot slot, als bezoekers zich op een site moeten aanmelden of registreren, dan kan de toestemming voor cookies ook op dat moment worden gevraagd.

Een site mag mensen wegsturen die cookies weigeren. Wel moet die consequentie vooraf worden gemeld - of moet de bezoeker alsnog cookies kunnen accepteren en dan toch worden binnengelaten.

Niet via de browser

Al die pop-ups, balken en andere toevoegingen aan websites om toestemming te vragen - echt gelukkig wordt u er niet van. Veel handiger is de instelling in uw browser over cookie-acceptatie, waar de site automatisch naar zou moeten luisteren. Enkele browsers accepteren momenteel de HTTP-header Do Not Track, die deze functionaliteit heeft. Maar dan nog zullen sites altijd rekening moeten houden met oude browsers en bij deze apart nog om toestemming moeten vragen. Bovendien speelt hier één cruciaal punt: wat moet de standaardinstelling van dit systeem zijn? De cookiewet eist eigenlijk dat niets mag, tenzij u expliciet uw instellingen op *Ja* zet.

Maar adverteerders zien de bui al hangen: tachtig procent van de mensen verandert nooit zijn instellingen, dus dan valt er geen droog brood meer te verdienen met adverteren op websites.

De cookiewet vereist toestemming voor het plaatsen van cookies, maar niet alléén toestemming. Een site moet namelijk ook uitleggen waaróm de bestandjes worden geplaatst. Om die reden hebben sites steeds vaker een cookieverklaring, vergelijkbaar met de privacyverklaring. Die legt uit welke privacygevoelige gegevens worden verzameld en met welk doel, en standaard staat er al een uitleg over cookies en hun impact op de persoonlijke levenssfeer. Maar omdat de cookiewet óók geldt voor soorten die niets met privacy te maken hebben, is zo'n privacyverklaring niet meer afdoende. De informatie moet duidelijk en volledig zijn, wat zoveel tekst oplevert dat een apart document verplicht is.

De cookiewet heeft tanden: de telecommunicatietoezichthouder OPTA is bevoegd om boetes op te leggen. En wanneer de cookies worden gebruikt voor profielen van bezoekers, is het College Bescherming Persoonsgegevens bovendien bevoegd om toezicht te houden en dwangsommen op te leggen. Maar of er heel actief gehandhaafd gaat worden, is nog maar de vraag. OPTA heeft al aangegeven zich in eerste instantie te richten op 'schrijnende gevallen'. Waar deze uit bestaan? Daarop moet nog beleid worden ontwikkeld. Zeer recent maakte OPTA bekend een stagiair te zoeken die een 'CookieMonitor' moet gaan bouwen, waarmee men volautomatisch sites kan afspeuren op illegaal gezette cookies.

De marketingbranche heeft een alternatief ontwikkeld: het cookie-icoon dat bij advertenties wordt getoond. Wanneer de internetter op dit teken klikt, komt hij op een website [1] die informatie geeft en de mogelijkheid biedt om niet meer via deze banners te worden gevolgd. Toen dit alternatief net werd gelanceerd, begaf de website het meteen onder de massale belangstelling van mensen die zich wilden afmelden.

Fok wil pers se toestemming hebben

Dit alternatief voldoet strikt genomen niet aan de wet, omdat u zich pas ná het volgen kunt afmelden. Maar voor de marketingbranche is het omgekeerde bijna dodelijk: immers, wie gaat naar een aparte site om daar te vragen om meer advertenties? Grote sites nemen dus massaal het risico voor lief, en de meeste kleintjes zullen redeneren: "Ze pakken mij toch niet als eerste." Daarmee zal de cookiewet waarschijnlijk massaal worden genegeerd. En dat is jammer.

‘Digitaal onderzoek politie schiet tekort’

Dat vindt Hans Henseler, forensisch computeronderzoeker bij Fox-IT en lector e-discovery op de Hogeschool Amsterdam.

Henseler vindt dat ‘gewone’ agenten en rechercheurs zelf meer digitaal onderzoek moeten kunnen doen en niet voor alles maar een digitale expert moeten inschakelen.
‘Al het digitale werk komt terecht op het bordje van speciaal opgeleide digitale experts’ maar met simpele tools kan elke rechercheur al belangrijke informatie op computers achterhalen, stelt Hensele. En dat is hard nodig, nu de snelheid waarmee de wereld digitaliseert, nauwelijks nog bij te benen is. En ‘als je alles aan experts overlaat, krijg je enorme wachttijden’ en blijven veel zaken op de plank liggen.

Als voorbeeld noemt hij een gestolen fiets die op Marktplaats aangeboden wordt. Heb je dan meer aan een digitaal expert of juist aan een rechercheur die met een helingzaak bezig is? In de korpsen Haaglanden/Hollands-Midden en Oost-Nederland zijn onlangs pilots gestart waarbij het digi-werk door rechercheurs gedaan wordt. Henseler ziet zulke pilots graag en hoopt dat ze tot een landelijke werkmethode leiden. ‘Het ene korps geeft rechercheurs een tool om foto’s van mobiele telefoons terug te halen, het andere korps is nog een stapje verder, maar er zijn ook regio’s waar rechercheurs echt alles overlaten aan experts’.

In een reactie vraagt NPB-voorzitter Han Busker zich af op het plan haalbaar is. ‘Het is een illusie om te denken dat politiemensen er extra werk bij kunnen nemen’.

Facebookfoto’s beschermd met plugin

Heeft iemand ‘m al uitgetest?
De Social Protection app van virusbestrijder McAfee om facebookfoto’s te beschermen?

Met de app kunnen gebruikers per foto aangeven of die openbaar is, wie ‘m mag bekijken, delen of downloaden. Ben je niet geautoriseerd, dan zie je een onscherpe foto. Ben je wel geautoriseerd, dan zie je de foto pas als je de app geïnstalleerd hebt.

Volgens McAfee is de app een antwoord op de toenemende online-kwetsbaarheid van consumenten: hoe meer foto’s je online deelt, hoe minder controle je hebt over waar die foto’s uiteindelijk terechtkomen.

Interessant is ook dat de (gratis) app (voor IE en Firefox) de foto’s opslaat op servers van McAfee en niet op die van facebook. Daardoor is ook het het maken van screenshots geblokkeerd.

Nederlanders doelwit valse Rechtspraak.nl e-mails

Op dit moment vindt er een nieuwe campagne tegen Nederlandse internetgebruikers plaats waarbij van Rechtspraak.nl afkomstige e-mails worden gebruikt om malware te verspreiden. De e-mails beweren dat de rechtbank een vordering heeft opgelegd en de ontvanger die moet betalen. "Indien wederpartij de vordering niet voor 3 oktober betaald kunnen wij als deurwaarder beslag leggen op uw bankrekeningen", aldus het bericht.

De e-mail bevat een bijlage met een afschrift van het exploot, maar in werkelijkheid is dit malware. "De afzender van deze e-mail is noreply@rechtspraak.nl, maar is niet afkomstig van de Rechtspraak. Het advies is om de bij de e-mail behorende bijlage niet te openen en de e-mail te verwijderen", zo laat de Rechtspraak op de eigen website weten.

Secure Computing