Secure Computing

Nieuwsbrief Juli - Augustus 2013

W.Bosgra taakaccenthouder digitale criminaliteit

In dit nummer:

Internetoplichting verschuift naar webshops

In 6 stappen buiten bereik van PRISM

Nieuwe Ransom-ware: Enquete invullen

Spionagevrije chat-app

Vakantietips……

en meer…….
(nu met onderwerp index vorige nummers)

Dit digitale magazine wordt verzorgd door Secure Computing.

Doel is bewustwording van wat u doet met de computer , kennis opdoen gericht op de opsporing van strafbare feiten (cybercrime) en veilig computergebruik.

U kunt deze nieuwsbrief opslaan op uw eigen "Home"-omgeving en als naslagwerk blijven gebruiken.

Indien u dit magazine tevens in uw eigen thuisomgeving bewaart, kunt u gebruik maken van de ingebouwde hyperlinks.

E-mail? klik hier !

Internetoplichting verschuift naar webshops

Oplichting op internet verschuift de komende jaren van handelssites als Marktplaats.nl naar malafide webshops. Dat verwacht Jesse van der Putte, officier van justitie die zich bezighoudt met fraude op internet.

Door de gezamenlijke aanpak de afgelopen jaren zal de oplichting op sites als Marktplaats afnemen. „Die worden steeds vaker gebruikt als advertentieplatform, waarna een koper wordt weggelokt naar de site van een malafide webwinkel."

In 2012 waren er 40.000 aangiftes van internetoplichting. Gemiddeld werd daarbij 196 euro schade geleden. Dat kwam neer op een totale schade van ongeveer van 7,8 miljoen euro. Dat is waarschijnlijk een deel van de werkelijke schade. Volgens Van der Putte tekent zich steeds een patroon af. „Achter elke 20 aangiften zitten zo'n 40 tot 60 bijschrijvingen. Je mag het niet helemaal één op één overnemen, maar als vuistregel, als schatting, kun je dus zeggen dat er in een derde tot de helft van het aantal fraudegevallen aangifte wordt gedaan."

Het daadwerkelijk aantal fraude-incidenten ligt waarschijnlijk op 80.000 tot 120.000. Dat laatste getal zou overigens nog altijd veel minder dan 1 procent van het totale aantal handelstransacties op internet bedragen. De grote frustratie van slachtoffers is dat zij meestal kunnen fluiten naar hun geld. „De bank heeft netjes de betalingsopdracht uitgevoerd die zij dan hebben gewild. Dan zeggen de banken niets te kunnen doen."

Volgens Van der Putte is de aanpak van internetoplichting de afgelopen jaren sterk verbeterd. Vroeger kwamen aangiftes terecht op de wijkbureaus, maar ontbrak het overzicht om landelijke verbanden te zien.
Dat zou zijn veranderd sinds de komst van het Landelijk Meldpunt Internet Oplichting. Daar worden aangiftes geclusterd. „Dat is bijvoorbeeld het geval als bij meerdere aangiftes sprake is van hetzelfde telefoonnummer of bankrekeningnummer."

TIPS

Betaling
Normaal heeft een beetje webwinkel betaalmethoden als IDeal, credit cards en vooraf overmaken, of zelfs rembours.
Een webshop die alleen maar vooraf betalingen accepteert is per definitie al verdacht.

Contactgegevens
Elke bonafide shop heeft online leveringsvoorwaarden en contactgegevens staan.
Zijn die er niet dan is dat per definitie al erg verdacht, zijn ze er wel controleer dan even via www.detelefoongids.nl of deze leverancier daar ook daadwerkelijk zit.
Gooi al die gegevens ook even door Google.
In Nederland zijn ondernemers in ieder geval verplicht om hun zakelijke gegevens inclusief KvK registratie te vermelden.

Webwinkel
Een nieuwe trend op het internet is dat je als particulier zelf een gratis webwinkel kan opzetten om je spullen te verkopen.
Uiteraard zijn er heel veel onschuldige verkopers die hier gebruik van maken, en waarom ook niet? Helaas heeft het oplichtersgilde deze gratis mogelijkheid ook gevonden, dus wees op je hoede als je op een shop beland die geen eigen domein heeft maar zo'n gratis tokootje.... per definitie zou dat een belletje moeten laten rinkelen in je achterhoofd.

thuiswinkel waarborg

Wij gaan een kijkje nemen bij een van de vaagste en meest uitgebreide begrippen van het nieuwe wetsvoorstel Computercriminaliteit : het begrip geautomatiseerd werk. Elk geautomatiseerd werk kan straks door de politie worden gehackt. Benieuwd wat daaronder valt?

Een geautomatiseerd werk

Het begrip zelf is al enige tijd opgenomen in het Wetboek van Strafrecht, maar in het wetsvoorstel zal dit begrip sterk worden uitgebreid. Simpel gezegd: alles wat in verband staat met een netwerk kan dan door de politie gehackt gaan worden. Ja, dat is ruim; er hoeft zelfs niet eens sprake te zijn van verbinding met het internet.

Standaard denk je dan aan: de computer, smartphone en tablet. Maar laten we een stapje verder gaan. De nieuwe televisies, routers, netwerkprinters en mediacenters mogen ook gehackt worden. En wat te denken van een server, het boordsysteem in je auto, je iWatch of Google Glass?

Zoals je ziet zijn er dus heel veel apparaten die hieronder vallen. En dat wordt in de toekomst alleen nog maar meer, want steeds meer apparaten maken gebruik van netwerken, waaronder dus ook het internet. Jij wil je verwarming vast aanzetten voor je thuis bent? Handig, maar waarom altijd zo warm: heb je soms een wietplantage?
Of een ander voorbeeld: je kijkt televisie en de politie kijkt mee naar het programma.

Nog serieuzer wordt het als je denkt aan nieuwe generaties gehoorapparaten of andere medische apparatuur. Zo lijkt het een leuk idee als je niet meer naar het ziekenhuis hoeft om je pace-maker te laten uitlezen, maar ook deze kan worden gehackt door de politie. Dit zal niet de bedoeling zijn , maar door de uitbreiding van het begrip is dit in de toekomst wel mogelijk.

In een eerder artikel is al aangehaald dat de nieuwe wet mogelijkheden biedt over onze landsgrenzen heen. Maar wat let een land als bijv. China, niet om hetzelfde bij ons te doen?

De makers van ransomware, de malware die computers voor losgeld vergrendelt, hebben een nieuwe manier gevonden om aan besmette Windows-machines te verdienen.

Ransomware dwingt Windows-gebruiker tot enquête

De meeste ransomware laat aan slachtoffers uit naam van een opsporingsdienst een melding zien, dat ze zich aan een misdrijf hebben schuldig gemaakt en een bepaald bedrag als boete moeten betalen.

Een nieuwe variant pakt het echter anders aan. Deze ransomware wordt op fora voor cybercriminelen aangeboden. De malware werkt op alle Windows-versies en schakelt Windows-applicaties zoals Taakbeheer, CMD, Regedit en het Start Menu uit.

Code
Daarnaast worden Media Player, VLC Player, MSN, Mirc, Calculator, Skype, PowerPoint, Word, Outlook, Excel, Access, WinRar, Minecraft, Steam, Photoshop en andere programma's geblokkeerd. De grootste nieuwigheid is echter de mogelijkheid om slachtoffers twee enquêtes in te laten vullen.

In plaats van het betalen van een bepaald bedrag, waarna het slachtoffer een code krijgt waarmee de computer ontgrendeld kan worden, moeten slachtoffers nu de enquêtes invullen om deze code te bemachtigen,

De minimale maximumstraffen voor cybercriminelen die data-inbreuken of cyberaanvallen plegen wordt binnen de Europese Unie verhoogd. De afzonderlijke landen zijn voornemens hun wetgeving aan te passen, waaronder Nederland.

Straffen cybercriminaliteit verhoogd in Europa

Het Eurpees Parlement heeft in Straatsburg een wetsvoorstel goedgekeurd om de minimale maximumstraffen voor cybercriminaliteit te verhogen, in het bijzonder wanneer die gericht is op kritieke infrastructuren of gevoelige informatie.

De 28 EU-lidstaten keurden het voorstel goed met 541 stemmen tegen 91 en 9 parlementsleden onthielden zich van stemming. Alleen Denemarken doet niet mee en kiest ervoor om haar eigen regels in stand te houden, zo meldt Reuters.

Momenteel variëren de straffen van lidstaat tot lidstaat, maar de meesten hanteren een maximumstraf van vijf jaar. De landen krijgen twee jaar de tijd om de nieuwe minimale maximumstraffen in hun nationale wetgeving te implementeren.

Hackers die proberen op een illegale manier toegang te krijgen tot informaticasystemen, kijken vanaf nu aan tegen een maximale gevangenisstraf van minstens twee jaar. Voor aanvallen tegen kritieke infrastructuren - kerncentrales, transport, overheidsnetwerken - loopt dat op tot ten minste vijf jaar.

Ook de straffen voor het illegaal onderscheppen van communicatie of het produceren en verkopen van instrumenten die dit mogelijk maken, worden in de nieuwe wet verhoogd. Bedrijven of organisaties die voordeel halen uit botnets of hackers inhuren om gegevens te stelen, kunnen vanaf nu aansprakelijk worden gesteld voor misdrijven die in hun opdracht werden uitgevoerd.

Een wachtwoord mag dan wel enige bescherming bieden, ze worden toch nog vaak gekraakt.

cijfers en speciale tekens. Het is onmogelijk te onthouden, mag nooit opgeschreven worden en moet om de paar maanden veranderd worden.

Hoe wachtwoorden gekraakt worden

Wachtwoorden worden nog steeds erg veel gebruikt. Dat heeft gevolgen. Wie je wachtwoord te pakken krijgt, kan in korte tijd heel wat schade aanrichten. Het is dus erg belangrijk dat je een exemplaar verzint dat krachtig genoeg is en niet zomaar achterhaald kan worden.

Een simpel wachtwoord is niet meer voldoende om uw account te beschermen. Gelukkig bieden bedrijven steeds vaker verificatie aan met meerdere stappen.Wanneer de dienst actief is, heb je behalve het wachtwoord van je account voortaan ook een verificatiecode nodig voor het inloggen. Die code ontvang je dan per sms en moet vaak maar een keer om de 30 dagen ingevoerd worden. Als alternatief voor de sms'jes kan je ook een app gebruiken om de verificatiecode te genereren.

Hackers aan het werk
Toch blijven wachtwoorden de eerste buffer, die best zo sterk en uniek mogelijk is. Een goed wachtwoord bestaat uit hoofdletters, kleine letters,

Hackers gaan op twee manieren achter je wachtwoord aan: ze gooien er ofwel brute rekenkracht tegenaan óf ze gaan meer gericht te werk.

Zo'n aanval met brute rekenkracht gaat veel nauwkeuriger dan zomaar willekeurige cijfer- en lettercombinaties uitproberen, omdat het heel veel kostbare tijd zou kosten om alleen al de 308 miljoen lettercombinaties tussen aaaaaa en zzzzzz te proberen. Voor een kraker is het zinvoller om meer gericht te gaan zoeken.

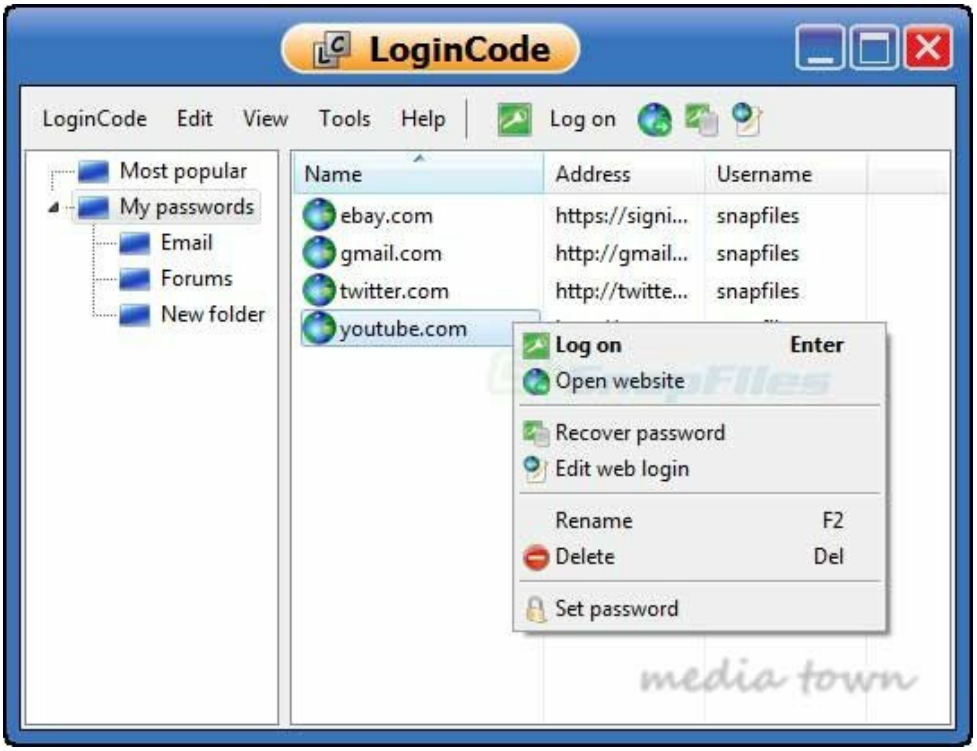
Eerst jaagt de kraker er een lijst van de duizend vaakst gebruikte wachtwoorden door. Daarna doet hij hetzelfde met de honderd vaakst voorkomende achtervoegsels. Op deze manier wordt al 24 procent van de wachtwoorden geraden.

Vervolgens probeert de kraker moeilijkere combinaties uit: stammen met voor- en achtervoegsels zoals combinaties van twee cijfers of jaartallen sinds 1900. In een paar weken tot een maand raadt hij zo tot 65 procent van de wachtwoorden.

Om te vermijden dat je wachtwoorden vergeet, gebruik je wellicht hetzelfde wachtwoord voor verschillende diensten. Begrijpelijk, maar niet zo verstandig.

Stop je wachtwoorden in een (lokale) kluis

Komt iemand je wachtwoord te weten, dan kan die meteen aan je gegevens bij diverse services. Verschillende – en liefst complexe – wachtwoorden dus, maar hoe onthoud je die op een veilige manier? Door die in een digitale kluis onder te brengen bijvoorbeeld. Dat is precies wat LoginCode voor je doet.



LoginCode is beschikbaar voor zowel 32- als 64-bits Windows. In principe kan je de tool ook in 'portable' modus op een stick zetten, maar die optie leverde op ons testtoestel weinig meer dan een foutmelding op. De klassieke manier van installeren dus… Na deze installatie start een database-wizard op. Die vraagt je of hij meteen maar alle reeds opgeslagen wachtwoorden van je browsers moet importeren.

Even later krijg je dan het venster van LoginCode te zien. Is dat niet het geval dan laat het programma zich altijd nog openen vanuit het systeemvak van Windows. In dit venster staan alle geïmporteerde sites al opgelijst.

Als het goed is, inclusief de naam van je login-ID's. Uiteraard kan je op elk moment ook zelf nieuwe sites en login-id's toevoegen en bestaande items aanpassen. Het spreekt vanzelf dat (de database van) LoginCode met een stevig wachtwoord is afgegrendeld en dat de inhoud van de database versleuteld wordt.

"Je bent keyloggers te slim af "

In tegenstelling tot veel andere wachtwoordmanagers moet je bij LoginCode vanuit dit venster de site aanklikken waar je je wil aanmelden. Er is dus geen LoginCode-knop in de browser(s) zelf te zien. Een alternatieve manier om je bij een site aan te melden is vanuit het LoginCode-venster het bijhorende wachtwoord naar het Windows klembord te kopiëren, waarna je het in de gewenste browser via Ctrl+V kan plakken. Let wel, na één minuut verdwijnt dit wachtwoord automatisch weer uit het Windows klembord.

Op deze manier hoef je in elk geval geen wachtwoorden meer te onthouden – zodat je probleemloos ook ijzersterke exemplaren kan kiezen - en ben je ook keyloggers te slim af. Immers, je hoeft wachtwoorden ook nooit meer in te tikken om je ergens te kunnen aanmelden.

KLIK HIER VOOR DE DOWNLOAD

Is het jou ook opgevallen hoe anders onze online ervaringen zijn tegenwoordig? Er zijn nu bijvoorbeeld een aantal nieuwe diensten, zoals Timeline op Facebook, waarop je ook gesponsorde berichten kunt vinden. Ook is het tegenwoordig mogelijk om een cadeau te kopen voor je vrienden via een sociaal netwerk, zoals de Facebook-cadeautjes voor verjaardagen.

Untag jezelf in Facebook-foto's

Deze vernieuwingen zijn leuk, maar helaas kunnen ze ook nieuwe malware, scam-trucs en valse advertenties met zich meebrengen.

Omdat Facebook een geweldige manier is om geïnformeerd te blijven over de levens van vrienden en familie, willen we natuurlijk wel dat het leuk blijft. Daarom zijn hier aantal tips over privacy-instellingen op Facebook (deze kun je aanpassen via het icoon rechtsboven in je Facebook-account):

Controleer hoe je 'deelt'
Je kunt standaard instellen dat je alleen dingen deelt met vrienden of zelfs alleen met je meest hechte vrienden. Het is belangrijk om via de standaardinstellingen je privacy te beschermen, omdat je hier de mogelijkheid krijgt om berichten alleen te laten zien aan bekenden. Per post kun je besluiten of je een bericht wilt delen met alleen vrienden of iedereen. Facebook heeft ook de optie om dit met terugwerkende kracht te doen, zodat je oude berichten onder de nieuwe veiligheidsregels kunt laten vallen.

'Untag' jezelf in foto's
Iedereen kent wel iemand die het leuk vindt om anderen te taggen in rare foto's; dit kunnen foto's zijn waar je daadwerkelijk op staat, of afbeeldingen die van het internet zijn geplukt en waarin je getagd wordt. Verwijder de tag bij alles waar je niet mee geassocieerd wilt worden. Je kunt ook via de instellingen aangeven dat Facebook jouw goedkeuring nodig heeft voordat je getagd kunt worden in een foto.

Gebruik de 'Lijstfunctie' van Facebook
Je hoeft niet bang te zijn dat je niets meer kunt posten op sociale media, want met de lijstfunctie van Facebook kun je aangeven wie jouw post kan zien. Je kunt bijvoorbeeld een lijst hebben met hechte vrienden en een andere lijst met familieleden en weer een andere met collega's. Wil je wat foto's posten van die toffe avond in de kroeg? Ga je gang, maar deel ze bijvoorbeeld alleen met je beste vrienden door de lijstfunctie te gebruiken.

Controleer de privacy-instellingen van je profiel
Het zijn niet alleen wallposts die verschillende privacy-instellingen hebben, maar ook de algemene informatie op jouw profiel, zoals je contactgegevens, adres, werkgever of school, kan op verschillende manieren bekeken worden. Bekijk daarom even goed wie wat kan zien van je profiel en verander dit indien nodig.

Zeker nu Facebook het makkelijker heeft gemaakt om informatie te achterhalen. Sociale netwerken zijn een geweldige manier om geïnformeerd te blijven, zorg er alleen wel voor dat je veilig blijft. Veel plezier!

De Amerikaanse NSA en FBI tappen in het PRISM-project verkeer af van buitenlandse internetters. Hoewel het programma ook in Nederland actief blijkt, is de regering Rutte II niet van plan iets te doen. Tijd om zelf tegenmaatregelen te treffen.

In 6 stappen buiten bereik van PRISM

Het spionageprogramma PRISM stelt de Amerikaanse inlichtingendienst NSA sinds 2007 in staat allerlei vormen van communicatie van buitenlanders die van Amerikaanse diensten gebruikmaken af te tappen en indien nodig te ontsleutelen.

PRISM is het eerste echte schandaal wat door alle media wordt opgepikt, maar natuurlijk waren er al jaren eerder zorgen over de toegang van Amerikaanse overheidsdiensten tot data van Europese cloudgebruikers. Die zorgen zijn nu terecht gebleken.

Ook al heb je niets te verbergen, dan nog is het goed voor te stellen dat je buiten het bereik van de tentakels van de Amerikaanse (en Europese) spionageinstituten wilt blijven, bijvoorbeeld om enig misbruik van jouw gegevens in de toekomst te voorkomen. Voor die mensen volgt hier een korte handleiding met alternatieven voor de in PRISM-betrokken diensten van Facebook, Apple, Microsoft, Yahoo, PalTalk, AOL, Skype, Google en YouTube.

1. Een PRISM-vrije manier van toegang

Hoewel op de Nederlandse markt AOL en Google (nog) niet vertegenwoordigd zijn, doe je er verstandig aan je toegang tot het internet te regelen met behulp van Nederlandse partijen die zo min mogelijk zaken doen met Amerikaanse partijen. Sinds de SWIFT-affaire uit 2005 weten we namelijk dat als een Nederlandse bedrijf servers in de VS heeft staan, de veiligheidsdiensten zichzelf toegang tot de (klant)gegevens mogen verschaffen.

Kies dus voor een provider met zo min mogelijk banden met de VS en gebruik Tor om de gegevens die je met je internetprovider uitwisselt via een anonieme en versleutelde lijn te laten verlopen. Een alternatief voor Tor is het geanonimiseerde overlaynetwerk I2P.

2. Browsen

Microsoft maakt Internet Explorer, Google de browser Chrome en Apple probeert al jaren aan de weg te timmeren met Safari. Gebruik je één van deze Amerikaanse browsers, dan vraag je erom afgeluisterd te worden.

Veiliger is het om een open-source browser als Firefox te gebruiken of over te stappen op een meer obscure browser als Midori, Konqueror of K-Meleon. Ook het Noorse Opera lijkt privacyveilig.

3. E-mail

De e-maildiensten van Microsoft, Yahoo en Google worden door de NSA in de gaten gehouden, dus daarmee zijn Outlook.com, Yahoo Mail en Gmail verboden terrein.

Het meest veilige alternatief is een eigen mailserver opzetten, bijvoorbeeld via Ubuntu. Naast dat je hiermee voorkomt dat je e-mailgegevens centraal worden opgeslagen op een Amerikaanse server, zijn andere voordelen dat je IMAP kunt gebruiken in plaats van POP, een onbeperkt aantal accounts kunt aanmaken en een nagenoeg onbeperkte capaciteit qua mailbox en bijlagen tot je beschikking krijgt. Ook kun je anti-spam volledig naar eigen inzicht configureren. Wel zul je hiervoor een computer moeten hebben die constant met internet verbonden is.

Een andere optie is gebruikmaken van een webmaildienst die geen zaken doet met de VS en waar privacy hoog in het vaandel staat. Je kunt bijvoorbeeld kiezen voor het Canadese Hushmail, het Britse Cyber-Rights of de webmail van je provider.

4. Zoeken

Hoewel 99 procent van de Nederlandse bevolking zoeken via Google in de vingers heeft zitten, kun je verwachten dat onder het PRISM-programma alle zoektermen die Nederlandse internetters ingeven in een grote database belanden. Vergis je niet, in Nederland kan het gebruik van Google al helpen bij het bewijzen van moord.

De zoekdienst van Yahoo is al een tijdje dood, maar Microsoft heeft nog altijd Bing in de race, al is ook die machine even risicovol als het gebruik van Google.

Een alternatief voor privacyveilig zoeken is DuckDuckGo, dat geen informatie van gebruikers opslaat, maar wel in de Verenigde Staten gevestigd zit. IxQuick is een Nederlands/Amerikaanse zoekmachine die ook privacy centraal stelt, maar wil je echt anoniem door het internet grasduinen, dan kun je het beste het volledig gedecentraliseerde YaCy gebruiken.

5. VoIP en chat

Skype, Google Hangout, Facebook, iMessage, Facetime, AIM en PalTalk worden waarschijnlijk afgeluisterd, dus mogen niet meer worden gebruikt. Als alternatief voor chatten kom je snel uit bij het oude vertrouwde ICQ, dat in 1998 weliswaar in handen van AOL kwam, maar sinds 2010 wordt beheerd door de Russische Mail.ru Group.

Een andere oude bekende is IRC, waarmee je met een client op een server inlogt die je toegang biedt uit duizenden chatkanalen. Wil je op een meer directere, moderne manier chatten, dan kun je CryptoCat proberen. Deze webgebaseerde dienst versleutelt gesprekken direct in Chrome, Firefox en Safari.

Een alternatief voor VoIP-bellen kan VoIP Buster zijn, dat gebruiksinformatie weliswaar opslaat, maar dat dichtbij in Luxemburg doet. VBuzzer is een Canadees alternatief.

Op gebied van video-chat zijn er helaas weinig populaire non-Amerikaanse alternatieven te vinden.

6. Mobiel

Apple, Google en Microsoft delen de lakens uit op mobiel gebied en dat maakt toestellen op basis van iOS (alle iPhones dus), Android en Windows Phone tot ongewenste metgezellen.

Wil je jouw privacy van bellen, tekst en mobiel internet beter onder controle houden dan kun je kiezen voor een Canadese BlackBerry telefoon of wachten op een toestel met Firefox OS, Ubuntu Touch, Sailfish of Tizen.

Bonustip: Veel webdiensten en apps vragen tegenwoordig om een login via Google of Facebook om in te kunnen loggen. Voorkom delen van gegevens tussen de dienst en je Google- of Facebook-account door een apart account met je eigen e-mailadres aan te maken of, indien mogelijk, voor een alternatieve app of dienst te kiezen.

Verschillende beveiligingsbedrijven zijn een initiatief gestart waarbij internetgebruikers kunnen controleren of hun IP-adres onderdeel van een botnet is.

Is jouw IP-adres onderdeel van een botnet?

De 'Check and Secure' website is opgezet door Cyscon, Avira en SurfRight en telecomaanbieder Vodafone. Oorspronkelijk is de campagne op de Duitse markt gericht, maar iedereen kan zijn computer laten controleren.

De campagne bestaat uit verschillende stappen, waarbij er als eerste naar het IP-adres gekeken wordt of dit geen onderdeel van bekende botnets is. Hiervoor gebruikt de website een actuele dataverzameling die uit zo'n '700.000 botnet-vermeldingen' bestaat en elk kwartier wordt bijgewerkt.

Het gaat om IP-adressen die afkomstig zijn van Command & Control (C&C)-servers waarmee botnetbeheerders besmette servers aansturen, maar die door beveiligingsbedrijven zijn overgenomen.

Op deze manier kunnen de beveiligingsbedrijven zien welke IP-adressen met de C&C-servers communiceren en dus onderdeel van een botnet zijn.

Plug-ins
Bij de volgende stap wordt er naar geinstalleerde plug-ins gekeken. 83% van alle computerinfecties ter wereld hadden voorkomen kunnen worden als de eindgebruiker zijn browserplug-ins, bijvoorbeeld van Adobe Reader, Java of Flash Player, met de meest recente versie had bijgewerkt, zo stellen de beveiligingsbedrijven.

Als laatste wordt het gratis HitmanPro.Alert van het Nederlandse SurfRight aangeboden, onder de noemer 'cyber-vaccinatie', die gebruikers tijdens het internetbankieren tegen banking Trojans beschermt.

Deze malware is speciaal ontwikkeld om geld van online bankrekeningen te stelen, maar het programma herkent als dit soort Trojans op de computer actief zijn en waarschuwt vervolgens de gebruiker.

Het gaat de laatste dagen alsmaar over onze privacy. Door het hele Snowden-verhaal en de spionageprogramma's van de NSA weet iedereen dat telefoongesprekken, e-mails en sms'jes helemaal niet zo privé zijn als dat we in eerste instantie dachten.

Oprichter Pirate Bay maakt spionagevrije chat-app

Deze heisa is perfect voor Peter Sunde, mede-oprichter van de BitTorrent-tracker The Pirate Bay. Hij werkt immers aan een berichtenapplicatie die niet te traceren valt. "Volledig spy-proof", meldt GigaOM.

"Alle communicatie wordt vandaag gecontroleerd door overheidsinstanties en particuliere bedrijven. En politici zijn niet van plan om hier een einde aan te maken", zegt Sunde in een videobericht. "Daarom hebben we besloten om een berichtenplatform te ontwikkelen dat niemand kan bespioneren. Zelfs wij als makers niet."

De app zal de naam Heml.is krijgen. Dat betekent 'geheim' in het Zweeds. De app zal binnenkort beschikbaar zijn voor iPhone en Android en is gebaseerd op end-to-end encryptie. Dat betekent dat enkel de zender en de ontvanger het bericht kunnen lezen.

Afluisteren of 'tappen'? Helaas, ……..vrij spel voor criminelen……

Bron: ZDnet

Uit recent onderzoek uitgevoerd door blijkt dat meer dan de helft van de Nederlanders die browsen in draadloze netwerken (hotspot) geen veiligheidsmaatregelen nemen.

Veilig onderweg surfen

Op de vraag: Denkt u aan uw digitale beveiliging bij gebruik van draadloze netwerken? wordt als volgt geantwoord:
• 23%: Nee, ik vind het vanzelfsprekend dat het netwerk veilig te gebruiken is;
• 9%: Ja, maar ik waag het erop;
• 30%: Nee, daar heb ik niet over nagedacht;
• 38%: Ja, en ik neem voorzorgsmaatregelen.

Mannen zijn ook beveiligingsbewuster dan vrouwen. Met een respectievelijk 43% en 33% van de respondenten die: "Ja, en ik neem voorzorgsmaatregelen" antwoordden. Volgens de enquête neemt minder dan 15% van de ondervraagden hun werk PC mee op vakantie. Hierbij doen mannen dit vaker (15%) ten opzichte van de vrouwen (10%).

Surfen zonder wachtwoord

Volgens dezelfde enquête heeft ongeveer een kwart van ons in het afgelopen jaar gebruik gemaakt van hotspots waarbij geen wachtwoord nodig is:
• 24%: Ja;
• 67%: Nee;
• 9%: Weet ik niet.

Ook hier is er een verschil tussen mannen en vrouwen. Waar 26% van de mannen draadloos surft zonder wachtwoord, doen maar 22% van de vrouwen dit. Echter twee keer zoveel vrouwen weten niet of ze gebruik hebben gemaakt van draadloze zones (11% tegenover 6%).

De cijfers tonen een laconieke houding ten opzichte van draadloze zones en de veiligheidsrisico's van het gebruik van onveilige zones. Voor iemand met enige kennis kost het weinig moeite om toegang te krijgen tot uw PC, tablet of mobiele telefoon, waarbij ze toegang kunnen krijgen tot uw zakelijke informatie, e-mail en documenten. Je laat vreemden toch ook niet toe in je bedrijfsnetwerk, probeer te denken aan dezelfde strenge maatregelen als je op een hotspot zit.

Aandachtspunten bij het surfen op hotspots:

1. Gebruik beveiligingssystemen: Zorg ervoor dat de beveiligingssoftware op uw computer echt is geactiveerd en dat deze ook regelmatig geüpdate wordt. Een antivirusprogramma dat niet wordt geüpdate kan uw PC niet voldoende beschermen tegen de nieuwste bedreigingen.
2. Maak alleen verbinding met beveiligde draadloze zones: sluit uw PC niet aan op draadloze zones die onbeveiligd zijn. Bij deze is meestal geen wachtwoord vereist.
3. Vermijd hotspots met onbekende namen. De meeste café's, hotels en andere plaatsen met een WiFi-hotspot hebben de bedrijfsnaam in de hotspotnaam staan. Maak verbinding met deze hotspots en vermijd verleidelijke hotspots met namen als "Free WiFi" en hotspots waarvan je de eigenaar niet kent.

Velen gaan binnenkort op vakantie. Laptop, notebook of tablet gaan uiteraard ook mee. Thuis of op het werk is de computer als het goed is extra beveiligd door middel van een firewall, antispam en een beveiligde verbinding. Onderweg is iedereen verantwoordelijk voor de bescherming van zijn/haar eigen mobiele apparaten. Met een kleine inspanning kunt u voorkomen dat u voor onaangename verrassingen komt te staan.

Beveiligingstips voor vakantiegangers

Een paar waardevolle tips voor vakantiegangers:

Voor vertrek

- Maak een back-up van al uw gegevens. Hardware en software kunt u makkelijk vervangen maar met gegevens is dit meestal niet zo eenvoudig. Een back-up voordat u op vakantie gaat zorgt ervoor dat u uw gegevens niet kwijt bent als uw mobiele apparaat wordt gestolen, u het verliest of als het beschadigd raakt. Voor data back-up kunt u gebruik maken van een externe harde schijf of van een online back-up dienst.
- Antivirusbescherming updaten. Als uw antivirussoftware niet up-to-date is, heeft u kans dat uw computer niet goed beveiligd is tegen de nieuwste bedreigingen. Tenminste éénmaal per dag heeft Norman een update van virusdefinities beschikbaar. Het weren van de nieuwste malware gebeurt op onregelmatige tijdstippen ter verbetering van de software. Zorg dat het product up-to-date is en dat de updates automatisch worden binnengehaald.
- Repareren & updaten van programma's en toepassingen. Kwetsbaarheden in softwareproducten zijn zeer populair onder cybercriminelen. Ze kunnen zo kwaadaardige code in de computer plaatsen. Op de dag van vertrek moeten dus het besturingssysteem en alle toepassingen waaronder de browser geüpdate zijn.

Toegang tot draadloze netwerken

- Schakel antivirus in en houd het bijgewerkt. Als u uw laptop onderweg gebruikt, controleer dan of de antivirussoftware ingeschakeld staat en up-to-date is.
- Gebruik opgeslagen WLAN's. Verbind uw computer met beveiligde WLAN's, u herkent deze omdat ze een wachtwoord vereisen voor toegang.
- Vermijd naamloze WLAN's. Bij de meeste café's, hotels en vergelijkbare openbare ruimtes die zijn voorzien van een WIFI hotspot, moet u een naam invoeren, die kan worden toegewezen aan een provider. Maak GEEN verbinding met netwerken die bijvoorbeeld "Free WIFI" heten.

WiFi op de camping of in het hotel

Het is handig om bij het zoeken naar een geschikte camping of hotel te controleren over er (gratis) WiFi aanwezig is. Op online booking sites en in camping en hotelgidsen staat vrijwel altijd aangegeven of WiFi aanwezig is en tegen welke tarieven en voorwaarden. Onbeperkt gratis WiFi zie je regelmatig voorbij komen. Hierdoor heb je geen zorgen over het dataverbruik op je tablet.

Internet op je tablet in het buitenland

WiFi hotspots

Verschillende bedrijven en telecom aanbieders bieden gratis en betaalde WiFi hotspots aan in het buitenland. In dit overzicht vind je enkele mogelijkheden waar je gebruik van kunt maken:

T-mobile – Ben je T-mobile klant in Nederland met een Internet, Internet Plus of i-Abonnement, of heb je een 3G abonnement voor je laptop? Dan kun je in het buitenland gratis gebruik maken van meer dan twintigduizend hotspot locaties. Meer informatie en de locatie van de hotspots vind je hier.
KPN – Ook KPN heeft hotspots voor haar klanten. Deze bevinden zich alleen in Nederland. Je kunt je aanmelden als KPN-klant bij een hotspot via MyKPN. Heb je een iPad met KPN abonnement? Dan moet je een speciale procedure volgen. Zoek daarvoor binnen kpn.com op hotspot ipad.
McDonalds – McDonalds biedt in vrijwel al haar filialen in de hele wereld gratis WiFi spots aan. Je kunt gratis gebruik maken van de open WiFi verbinding voor een beperkte periode, meestal 1 uur.

Zelf WiFi hotspots zoeken

Een overzicht van veel gratis WiFi hotspots vind je op deze website. Ook zijn er apps om hotspots te zoeken: Android en iOS.

Handige applicaties

Er zijn oneindig veel applicaties beschikbaar voor je iPad of Android tablet die handig zijn op vakantie. We raden je aan om je vakantiebestemming in te voeren in de Android Market, of in de Apple App Store, en te kijken wat voor een apps beschikbaar zijn. Dit zijn handige applicaties om te downloaden:

- Kaarten downloaden. Door een app te downloaden die de kaarten van de stad en omgeving offline kan gebruiken, hoef je in het buitenland geen connectie te maken met internet.

- Stadsgidsen downloaden. Van veel grote steden zijn gratis en betaalde apps te downloaden met daarin offline stadsgidsen met populaire bezienswaardigheden. Onze ervaring is dat de betaalde apps vaak niet veel beter zijn dan de gratis apps.

- Toeristische informatie. Voor veel populaire vakantiebestemmingen, vooral grote steden, zijn apps beschikbaar met toeristische informatie.

- Openbaar vervoer informatie. Ook hier zijn weer verschillende apps per land (trein, boot, bus), of per stad (bus, metro, tram) beschikbaar om actuele OV-informatie op te halen. Voor deze apps is vaak een Internet verbinding vereist.

- Leer de taal. Honderden gratis apps zijn hiervoor beschikbaar zodat je de meest voorkomende woorden en zinnen in een andere taal kunt leren. Handig als voorbereiding en voor onderweg!

Velen onder u trekken deze vakantiemaanden naar het buitenland. Daar wordt gebeld met de familie, worden sms'jes gestuurd naar vrienden en wordt het weer op de voet gevolgd. Hoe zorg je ervoor dat dit allemaal zorgeloos kunt doen, zonder een torenhoge telefoonrekening op de deurmat te ontvangen?

Mobiel blijven op vakantie? Dat doe je zo!

Tip 1: neem een vakantiebundel
De meeste telefoonproviders bieden pakketten, bundels en andere constructies aan om het je zo eenvoudig mogelijk te maken in het buitenland. Ga bij jezelf na of dit nu echt allemaal nodig is. Haal je die 20 minuten bellen uit dat ene aanbod wel? Ga je echt die 100 MB aan internet gebruiken bij die andere bundel? Mobiel internet in het buiteland kan behoorlijk in de papieren lopen omdat het harder gaat dan je denkt. Door contact op te nemen met je provider ben je ervan verzekerd dat je de deal krijgt die het beste bij jouw wensen aansluit. Tegenwoordig heeft iedere provider ook de mogelijkheid om online je zaken te controleren. Dit geeft je snel een goed overzicht van je huidige abonnement en de mogelijkheden om dit voor een buitenlandse trip uit te breiden.

Tip 2: gebruik WiFi
Met WiFi kan je draadloos op het internet door verbinding te maken met een bestaand WiFi-netwerk. Veel campings en hotels bieden WiFi aan. De ene keer is dit gratis, de andere keer betaal je hiervoor. Tenzij de prijs voor WiFi-gebruik bij een camping of in een hotel zeer hoog is, kan je veel geld besparen door deze WiFi-verbindingen te gebruiken. Hierdoor hoef je geen aanspraak te maken op je databundel.

Tip 3: schakel roaming uit
Wanneer roaming aan staat, kunnen applicaties die continue dataverbinding nodig hebben ook continu verbinding maken met het internet. Om hier een stokje voor te steken (en jezelf een fikse rekening te besparen), ga je naar de instellingen op je telefoon. Elke telefoon heeft in het menu 'verbindingen', 'draadloos en netwerken' of 'mobiele netwerken' staan. In zo'n menu staat de mogelijkheid om roaming toe te staan. In het buitenland is het dus verstandig om ervoor te zorgen dat het apparaat geen verbinding kan maken; kijk daarom goed of het vinkje voor 'gegevensroaming' weg is.

Tip 4: koop een lokale prepaid simkaart
Door een lokale prepaid simkaart aan te schaffen, maak je gebruik van de internetverbindingen van het land waar je bent. Daarvoor betaal je niet je eigen landelijke tarieven maar de lokale. Deze zijn een stuk voordeliger. Deze simkaart kan je alleen gebruiken in het land waar je hem koopt en alleen als je telefoon simlockvrij is. Wanneer een telefoon niet simlockvrij is, zal hij geen andere simkaarten accepteren. In de papieren die je bij aanschaf van je telefoon krijgt staat of je telefoon simlockvrij is of niet. Vaak zijn toestellen die in combinatie met een abonnement zijn gekocht niet simlockvrij.

Tip 5: download van tevoren
Er zijn allerlei soorten apps te bedenken die van pas kunnen komen op vakantie. Denk aan een valuta-applicatie, een digitaal woordenboek of een navigatie-applicatie. Het downloaden van deze applicaties vereist vaak veel internetgebruik. Daarom is het slim om voordat je op reis gaat na te gaan welke applicaties je nodig kunt hebben, die je onder het motto 'beter ermee verlegen dan erom verlegen' vast kunt downloaden. Ook is het verstandig applicaties van te voren te updaten. Bedenk wel dat het gebruiken van sommige apps ook vaak nog data kost.

Ga je in de vakantie naar Engeland? Zorg dan dat er geen For your eyes only bestanden op staan. De Britse politie gebruikt anti-terrorismewetgeving om van duizenden onschuldige reizigers en vakantiegangers de telefoongegevens te downloaden, die vervolgens verder worden geanalyseerd.

Britse politie trekt telefoons vakantiegangers leeg

Politieagenten kunnen op vliegvelden, treinstations en havens willekeurige passagiers dwingen om hun telefoon af te staan, die vervolgens wordt leeg getrokken.

De wetgeving waaronder de dienders te werk gaan is zo breed, dat er geen 'redelijke verdenking' hoeft te zijn. Daarnaast kunnen de gedownloade gegevens worden bewaard 'zolang nodig' is. De gegevens bestaan uit gespreksgeschiedenis, adresboeken, foto's en met wie de persoon sms't en e-mailt. De inhoud van de berichten zou niet worden gedownload.

Elk jaar worden 60.000 mensen onder de terrorismewetgeving van 2000 'gestopt en gecontroleerd' als ze Groot-Brittannië betreden of terugkeren. Het is onbekend van hoeveel mensen de telefoon wordt geanalyseerd.

Volgens David Anderson, onderzoeker van terrorismewetgeving, is de maatregel een 'handige tool' in de strijd tegen terrorisme, maar moet het wel juist worden toegepast. Hoeveel terrorismegevallen er via de wet zijn voorkomen of opgelost is onbekend.

Op dit moment in de schatkist:
(Klik op de kist om het te downloaden)

Wet Computercriminaliteit III

Memorie van Toelichting

Recuva

Bootkit Removal Tool

UnstoppableCopier

Blackberry Desktop Software

Format Factory

Al vaker betoogd, maar nu ook wetenschappelijk onderbouwd, is dat er nauwelijks een relatie is tussen sociale media en woninginbraken. Linda Nagelhout van Adviesbureau VDMMP toont in haar rapport aan dat 'inbraakresearch' via sociale media een stuk moeilijker is dan gedacht én dat inbrekers nog steeds op hun oude vertrouwde manier te werk gaan. Hoewel de 'digitale voordeur' nog regelmatig openstaat, blijkt het lastig om via sociale media een geschikte woning te vinden 'waarin naar hartenlust kan worden ingebroken'. Nagelhout liet een groep agenten in opleiding zoeken naar geschikte woningen om in te breken, een andere groep ging gewoon de straat op, 'de wijk in' zoals inbrekers dat al 'sinds jaar en dag doen'. De tweede methode bleek het meest rendabel. Via sociale media bleek het weliswaar mogelijk om te vinden welke twitteraar op vakantie is, maar 'erg tijdrovend' en 'zeer lastig' om het daarbijbehorende adres te vinden. Makkelijker wordt het bij twitteraars die voor- en achternaam én woonplaats in hun bio hebben staan. Uit Nagelhouts onderzoek blijkt dat 86% van de gebruikers van sociale media evenwel denkt dat inbrekers sociale media gebruiken om potentiële slachtoffers te vinden, deze te googlen en daarna op het gevonden adres in te breken. Preventie blijft echter belangrijkste, zie ook de tips op VeiligFacebook.nl: kijk nog eens goed met wie je updates en postings deelt. Maar verder geldt: 'eerst de deuren op slot, dan de sociale media'.

Als eerste Nederlandse provider heeft XS4ALL een 'transparantierapport' gepubliceerd. Daaruit blijkt dat de politie in 2012 in totaal 42 taps bij deze provider zette: 21 keer internetverkeer, 19 keer telefonie, 2 keer e-mail. De provider moest verder 21 keer verkeersgegevens afstaan. XS4ALL, dat andere providers oproept deze gegevens ook te publiceren, kan niet aangeven of het aantal taps stijgt of daalt. Wel dat het alleen op taps van politie en justitie gaat, en niet om die van AIVD of MIVD.

Of we zoiets in Nederland durven? Hm …. Maar in Engeland, in Sussex om precies te zijn, kunnen burgers kiezen welke agent het beste gebruik maakt van sociale media. Het nadeel van zulke enquetes is dat ook Inspector Gadget voorgedragen wordt, maar daar zullen ze wel een slim filterje op zetten. 'Voting now open'.

Vakantietijd. Dus fraudetijd! Wie boekte bij Fantasie Reizen in Utrecht, moet een goede fantasie hebben. Want op de geboekte accommodatie weten ze van niks. Het reisbureau, december 2012 bij de KvK ingeschreven, verkocht luxe reizen naar Turkije, Egypte of Bulgarije, tegen 'spotprijzen' die 'niet te koste gaan van de kwaliteit'. De zaak kwam aan het rollen toen Belgische vakantiegangers er op hun bestemming achter kwamen dat hun boeking was geannuleerd.
In De Telegraaf (4 juli 2013) vertelt een gedupeerde familie over een andere 'louche bemiddelaar', Sunnyrenta.nl. Gelokt met mooie plaatjes van luxevilla's voor lage prijzen, kan de familie Van Henne fluiten naar 1600 euro. Ze boekten via Marktplaats een prachtige vakantiewoning met zwembad, wifi en vier slaapkamers. Omdat ze op internet geen negatieve beoordelingen vond, boekte vader Theo. Hij moest de gehele reissom overmaken maar hoorde vervolgens niets meer. Bij het online reserveringssysteem Uwboeking.com, dat met Sunnyrenta.nl werkte, kwamen meer klachten. 'Wij leveren alleen software maar zijn wel onmiddellijk met Sunnyrenta gestopt'. Ook directeur Reuver van de Stichting Garantiefonds Reisgelden (SGR) waarschuwt voor internetaanbiedingen. 'Als het te mooi lijkt om waar te zijn, is het dat meestal ook'. Reuver adviseert eerst op de site te kijken of een aanbieder is aangesloten en nooit hoge bedragen over te maken naar onbekende rekeningen. Volgens hem neemt het aantal meldingen van gedupeerden schrikbarend toe.

Dit magazine verschijnt maandelijks.
De inhoud bestaat uit verzameld werk uit openbare internetbronnen.
Voor zover mogelijk zal de bron worden vermeld.

Opmerkingen kunt u mailen naar de redacteur.

Onderwerp index edities 2012:

12-01 > Computercriminaliteit, Definitie van Cybercrime, Strafbare gedragingen, Aftappen van gegevens, MSN chat via Windows, E-mail headers zichtbaar maken, Botnet, Hacking, Spyware,

12-02 > Kwaadaardige software, Phishing, Keyloggers, DNS aanval, Politiemethodes voor bewijs

12-03 > Man in the Middle, ID alert, Meldingsformulier identiteitsfraude, Meldpunten, Wetsartikelen voor computercriminaliteit in enge zin, Cyberstalking, Grooming

12-04 > E-mail spoofing, Elektronisch briefgeheim, Afgeven klantgegevens, Gebruik een live cd/dvd voor veilig internetbankieren, Cloudcomputing

12-05 > Van password naar passphrase, Nieuwe phishing scams, E-mail blunder, Word documenten kunnen virussen bevatten, Hoe hackers u misleiden, Cyberkatvanger, Gratis Windows-tool voor veilig internetbankieren, HP USB disk storage format tool, Muis smeriger dan wc bril

12-06 > Microsoft calling?, Computer in slaapstand of uitschakelen, EU wil internetidentiteitskaart, BVH kan het nog slechter, Wat is Facebook echt waard, Browser voor liefhebber social media, Politievirus, Wardriving, Vind gratis wi-fi op je vakantiebestemming

12-07/08 > Facebook: Nieuwe tactiek om verblijfsvergunning te krijgen, Facebook scant chatconversaties van gebruikers, Lokpuber ontmaskert pedofiel in chatbox, Uw smartphone virusvrij, Facebook Hyves Twitter: zo komt u van uw accounts af, Hoe hackers hacken, Vakantie? Smartphone mee, Beelden bewakingscamera's sneller online, Nederland mist urgentie in aanpak cyberdreiging, Antivirus bedrijf AVG lanceert social media beheertool

12-09 > Veilig WiFi, ID alert, Versnel je windows PC, Windows 7 administrator account activeren, Anders knippen en plakken, Open DNS, Beter geluid uituw PC, Instellingen makkelijk terug vinden, XBMC het alternatief voor Windows media center, Windows 7 sneltoetsen, De windows toets, Free Video Converter, Je gegevens zijn op internet gelekt, wat nu, PC gekaapt, Money mules, I-frame injection, Zoekmachine misbruik, Hardware printers, Opinie: Cybercrime, Social engeneering, WhatsApp berichten veiligstellen, E-boeken downloaden, Beter zoeken met Google, Studeren doe je met YouTube, Handige freeware, I-doser, Tablet kopen, Smartphone beveiliging, Find my Phone,

12-10 > Is spyware illegaal, Wanneer valt website onder cookiewet, Wapen uit 3d printer, Facebook plug-in beschermt foto's tegen pottenkijkers, Hackpreventie, Libre Office, Hardware videokaart, Apps: wat moet je weten, Variaties op de Nigerian scam, Handige hulpprogramma's voor je PC, Tips om je smartphonebatterij te sparen, Meeste Torrent-downloaders gemonitord, Populaire vingerafdruklezer lekt Windows wachtwoord, Grote bestanden verzenden, De Russen komen, Digitaal onderzoek politie schiet tekort, Facebookfoto's beschermd met plug-in, Nederlanders doelwit valse Rechtspraak.nl e-mails

12-11 > Politievirus waarchuwt slachtoffers via Mp3, Trusteer voor veilig internetbankieren, Veilig internet: behaal het certificaat, Cameratoezicht: mag wel/ mag niet, Panopticon, Laat u niet volgen, Key generators, Opt-in botnet probleem voor banken en landen, Zo redt u foto'd, Facebook: geen toegang voor spammers, Backup van uw online data, repareer je internet explorer, Herken een besmette PC en doe er wat aan, Illegale torrents: wat zijn de gevolgen,

12-12 > Ontsleutelen, Malafide webwinkels, Romance scam, Phiishing mail vraagt om foto van TAN-codes, HTTPS Everywhere, Metadata Cleaner,

Onderwerpen Index edities 2013

2013-01 > Voorspellingen 2013: maatschappelijke trends, Herken jij alle nep-virusscanners, Overheid onthult richtlijnen voor hackers, Anti-virus boot cd/dvd's, Browser plug-ins, Hoe weet je dat je smartphone is gehackt,
Hoe gezond is je harde schijf, Halkf miljoen wifi routers lek, Telefoneren via Facebook, Voicemails sturen met Facebook messenger, Data verbergen, USB sneller verwijderen, Beter zoeken met Google, Tips voor Windows 8,
Internetprovider, De gevaren van een enkele Net identiteit

2013-02 > Nederlandse politie worstelt met TOR, Nieuwe versie Police Ransomware, Cloudopslag vereist nieuwe wetgeving, Drugs bestellen via de post: sure we can, Cybercrises in aantocht, Ultieme dataredder bij stervende schijf, Virusdoder vermomt zicht om besmette pc's te ontsmetten, Microsoft bestrijdt processor-dief op Windows pc's, WiFi Protector beschermt je WiFi buiten de deur, Politie en NCSC laks na hack duizenden bedrijven, Opinie: opofferen privacy helpt niet tegen cybercrime

2013-03 > Toebname phishingmails, Angifte phishing: stel de volgende vragen, Cybertaal,: bezemen - Vishing _ Sexting, SSID, Valse Flash player update verspreidt politievirus, Een veilige smartphone in toe stappen, Opinie: het neerhalen van botnets is zinloos

2013-04 > Wat is een Ddos aanval, Cybercriminelen zetten buitenwipper in, Antiwaskist mobiele telefoons, Inbreken op router wel strafbaar, Vaker kinderporno op Nederlandse servers, Meeste mailmalware verstopt in ZIP bestanden, Gestolen mobiel voor de zomer onklaar, Visie rapport Trends in Veiligheid 2013, Zoeken op internet in alle privacy, Sociale media vast onderdeel van politiewerk, Glasvezel internet, PhoXo gratis forobewerking,
Geen downloadverbod voor particulieren, 20% websites bevat kwaadaardige code, Nep muiscursor beschermt t wachtwoord tegen gluurders, Zo maakt u sterke wachtwoorden, In de schatkist, Opinie: wij sturen online criminelen de verkeerde boodschap

2013-05 > VPN, PGP, Malware in BING, Notice & Takedown, uKAsh politievirus verwijderen, Wachtwoord kwijt?, Identiteit uitfilteren, Facebookprofiel gekaapt, Beschadigde bestanden leesbaar maken, Steganografie, HOAX, Netneutraliteit

2013-06 > Wet Computercriminaliteit III, Darknet, NSA tapt servers, TOR adviseert privacycocktail, Virusinformatie, Alles over een bootsectorvirus, Klaar voor Ipv6, Marktplaatsoplichting vrijspraak, Zoek je eigen digitale sporen, Herstart gecrashte computer

2013-07/08 > Internetoplichting verschuift naar webshops, Een geautomatiseerd werk, Ransomware dwingt gebruiker tot enquete, Straffen cybercriminaliteit verhoogd in Europa, Hoe wachtwoorden gekraakt worden, Stop je wachtwoorden in een kluis, In 6 stappen buiten bereik van PRISM, Is jouw Ipadres onderdeel van een Botnet, Beveiliginsgtips voor vakantiegangers, Veilig onderweg surfen,