Secure Computing

05-2014

W.Bosgra taakaccenthouder Digitale Criminaliteit

Boete bij niet betalen ransomware

Contactloos betalen gebruikt voor phishingmail

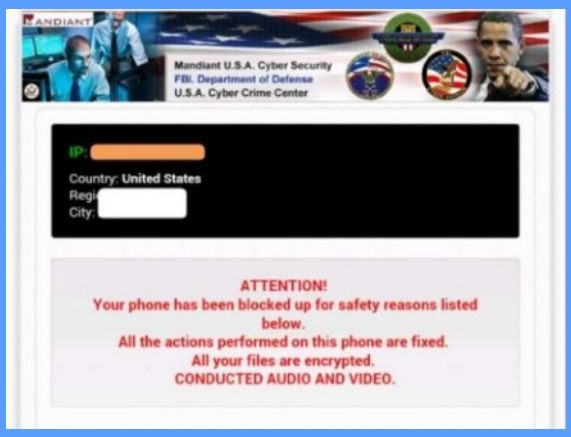
Cryptolocker op Android

Twitter wachtwoord herstellen

TAILS. Tails?

Geen bestanden opslaan op je bureaublad

Cybercriminelen meer kans bij vrouwen



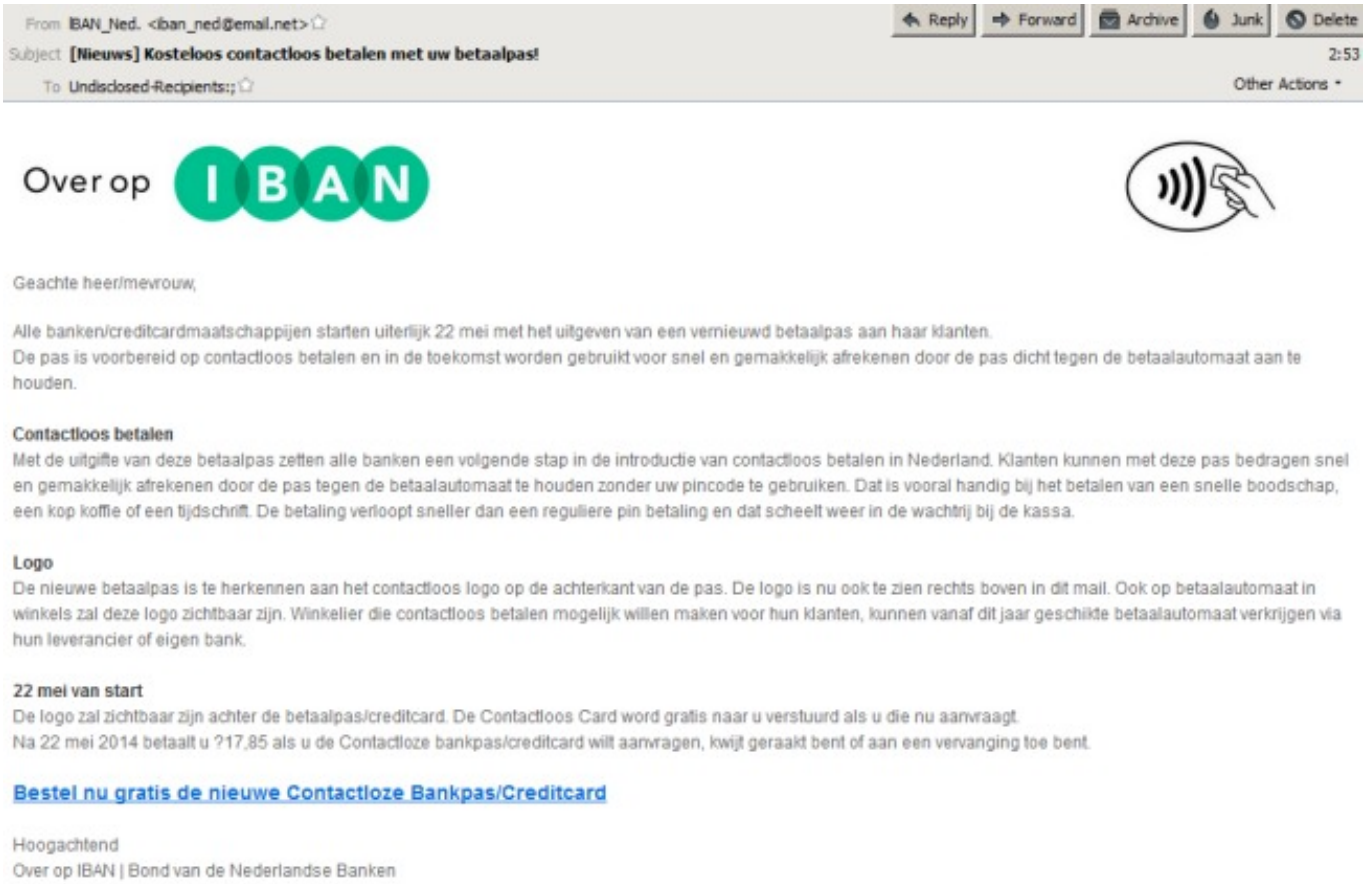
Contactloos betalen gebruikt voor phishingaanval

Cybercriminelen lijken de ontwikkelingen bij Nederlandse banken op de voet te volgen, zo blijkt uit een phishingmail die rondgaat en waar ontvangers op contactloos betalen wordt gewezen. Volgens de e-mail zullen alle banken en creditcardmaatschappijen een vernieuwde betaalpas onder klanten uitgeven.

Deze betaalpas kan worden gebruikt om contactloos mee te betalen. Het bericht laat weten dat de contactloze betaalpas tot 22 mei gratis via de meegestuurde link kan worden aangevraagd. Daarna moet er 17,85 euro voor worden betaald. De link in de e-mail wijst naar een domein met het Top Level Domein van Samoa en was op het moment van schrijven nog steeds operationeel.

Op deze website moet er een bank worden gekozen, waarna de echte phishingpagina wordt geladen. Die wordt door de Google Safe Browsing API herkend en geeft dan ook een waarschuwing in browsers zoals Google Chrome, Mozilla Firefox en Safari. De phishingsite vraagt vervolgens om een gebruikersnaam, wachtwoord, geboortedatum, rekeningnummer, vervaldatum, pasnummer en pincode.

Vorige maand introduceerde ING contactloos betalen. Klanten kunnen bedragen tot en met 25 euro afrekenen door de betaalpas kort en dicht tegen de betaalautomaat aan te houden. Meer dan de helft van de ING-klanten zou inmiddels een pas hebben die voor mobiel betalen geschikt is.



From IBAN_Ned. <iban_ned@email.net>
Subject [Nieuws] Kosteloos contactloos betalen met uw betaalpas!
To Undisclosed-Recipients:;

Reply Forward Archive Junk Delete
2:53
Other Actions

Over op IBAN

Geachte heer/mevrouw,

Alle banken/creditcardmaatschappijen starten uiterlijk 22 mei met het uitgeven van een vernieuwd betaalpas aan haar klanten.
De pas is voorbereid op contactloos betalen en in de toekomst worden gebruikt voor snel en gemakkelijk afrekenen door de pas dicht tegen de betaalautomaat aan te houden.

Contactloos betalen
Met de uitgifte van deze betaalpas zetten alle banken een volgende stap in de introductie van contactloos betalen in Nederland. Klanten kunnen met deze pas bedragen snel en gemakkelijk afrekenen door de pas tegen de betaalautomaat te houden zonder uw pincode te gebruiken. Dat is vooral handig bij het betalen van een snelle boodschap, een kop koffie of een tijdschrift. De betaling verloopt sneller dan een reguliere pin betaling en dat scheelt weer in de wachtrij bij de kassa.

Logo
De nieuwe betaalpas is te herkennen aan het contactloos logo op de achterkant van de pas. De logo is nu ook te zien rechts boven in dit mail. Ook op betaalautomaat in winkels zal deze logo zichtbaar zijn. Winkelier die contactloos betalen mogelijk willen maken voor hun klanten, kunnen vanaf dit jaar geschikte betaalautomaat verkrijgen via hun leverancier of eigen bank.

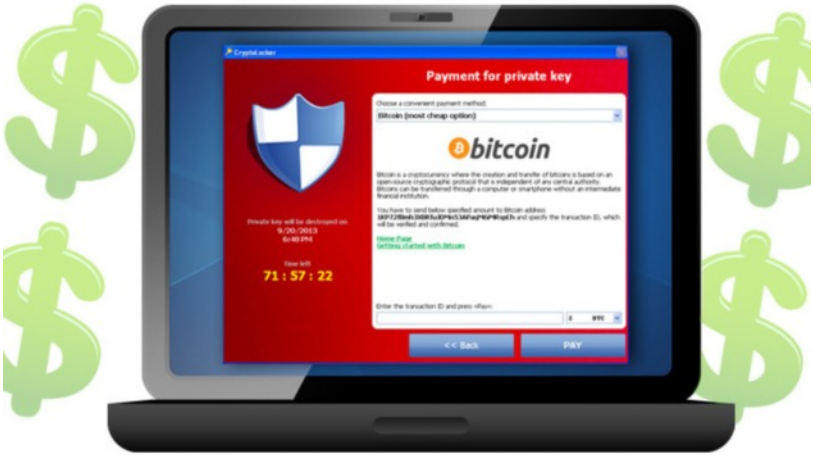
22 mei van start
De logo zal zichtbaar zijn achter de betaalpas/creditcard. De Contactloos Card word gratis naar u verstuurd als u die nu aanvraagt.
Na 22 mei 2014 betaalt u ?17,85 als u de Contactloze bankpas/creditcard wilt aanvragen, kwijt geraakt bent of aan een vervanging toe bent.

Bestel nu gratis de nieuwe Contactloze Bankpas/Creditcard

Hoogachtend
Over op IBAN | Bond van de Nederlandse Banken

Valse Cryptolocker op Android gesignaleerd

Cryptolocker, de fameuze ransomware die pc-bestanden versleutelt en pas weer beschikbaar maakt als je 300 dollar betaalt, zou de sprong van Windows naar Android gemaakt hebben.



"Een vermoedelijk valse versie van Cryptolocker, die gebruikers beschuldigt van het bekijken van kinderporno, is opgedoken voor Android. "

Volgens de gespecialiseerde website Threatpost adverteert de Reveton cybercrimebende een Android-versie van de software. Om besmet te raken met de ransomware, moet je het programma zelf downloaden, je kan voorlopig niet op een andere manier besmet geraken.

Om dat voor mekaar te krijgen doet de software zich voor als een porno-applicatie. (Om nog maar eens een open deur in te trappen: download nooit Android-apps van niet-officiële app-winkels en download ook nooit apps van pornosites.)

'Vijf tot elf jaar gevangenis'

Wie toch zo gek is om de app te installeren krijgt, telkens als je je smartphone probeert te gebruiken, een waarschuwing te zien. Je bent zogezegd betrapt op het bekijken van kinderporno en je zal vijf tot elf jaar in de gevangenis vliegen. Tenzij je natuurlijk 300 dollar betaalt via de betaalservice Moneypak.

Momenteel is het nog niet helemaal duidelijk of deze ransomware, die als Koler.A door het leven gaat, echt een variant van Cryptolocker is of gewoon een ander programma dat de naam van zijn beroemde soortgenoot "leent".

Vijf seconden

Erg veel tijd hebben veiligheidsfirma's ook nog niet kunnen besteden aan de app, maar het lijkt er ook op dat het programma helemaal je bestanden niet encrypteert. Dat gezegd zijnde, is het een behoorlijk vervelende klus om het ding weer van je telefoon te krijgen. De antivirusprogramma's voor Android hebben nog geen oplossing.

Het programma naar de prullenbak slepen lijkt te werken, maar dan moet je het ook binnen vijf seconden verwijderen alvorens het je scherm weer overneemt.

Ransomware geeft slachtoffers 500 euro boete bij late betaling

Een nieuwe ransomware-variant die in omloop is geeft slachtoffers een boete als ze te laat met betalen zijn. Het gaat om de CryptoWall-ransomware, die erg veel op de CryptoDefense-ransowmare lijkt die in maart werd ontdekt. Net als CryptoDefense versleutelt CryptoWall bestanden op de computer.

Vervolgens krijgen gebruikers een aantal dagen de tijd om het gevraagde losgeld van 500 euro te betalen. Betalen slachtoffers niet op tijd, dan wordt het losgeld verdubbeld en moet er 1000 euro worden betaald. De gebruikte versleuteling is zo sterk dat slachtoffers in principe hun bestanden kwijt zijn, tenzij ze over een back-up beschikken.

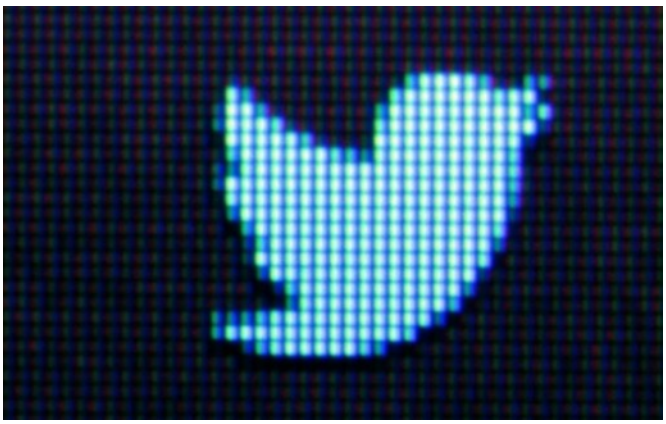
Volgens het Bleeping Computerforum hebben de ontwikkelaars van CryptoDefense de nieuwe variant mogelijk uitgebracht omdat het origineel te bekend werd bij anti-virusleveranciers. Een andere mogelijkheid is dat de code van CryptoDefense aan andere malwaremakers is verkocht.

Internetgebruikers kunnen zich tegen ransomware beschermen door beveiligingsupdates te installeren, geen ongevraagde e-mailbijlagen te openen en software alleen van de officiële website van de leverancier te downloaden. Om de impact van een eventuele infectie te beperken wordt aangeraden om over actuele en geteste back-ups te beschikken.

"Betalen slachtoffers niet op tijd, dan wordt het bedrag verdubbeld"

Twitter-wachtwoord herstellen kan met sms'je

Twitter heeft zijn veiligheidsmaatregelen aangepast zodat gebruikers gemakkelijker een nieuw wachtwoord kunnen instellen. Dit kan voortaan door een sms'je te sturen.



Ook via e-mail of je account-naam kunnen accounts van een nieuw wachtwoord voorzien worden. Twitter volgt met deze maatregelen in de voetstappen van heel wat andere grote websites die al langer toelaten om wachtwoorden met sms'jes te herstellen.

Gsm-nummer koppelen

Om deze functie te gebruiken, moet je eerst je gsm-nummer koppelen aan je Twitter-account. Hoe dat precies in zijn werk gaat, vind je hier uitgelegd. Om je wachtwoord te veranderen via sms of mail, klik je op Forgot Password op de homepage van Twitter. Dit werkt zowel op de mobiele site als op de gewone site. Daarna geef je je gsm-nummer of je mailadres in.

Wie z'n gsm-nummer intikte, krijgt een code teruggestuurd die je moet intikken op de Twitter Sign In-pagina. Daar kan je dan meteen ook een nieuw wachtwoord aanmaken. Je kunt ook de veiligheidsinstellingen van je account nakijken en eventueel aanscherpen, bijvoorbeeld door Twitter zowel je gsm-nummer als je e-mailadres te laten vragen als je wachtwoord veranderd moet worden.

Verdachte inlogpogingen onderscheppen

Twitter zal ten slotte ook strenger gaan toekijken op verdachte inlogpogingen. De site zal die beoordelen op basis van locatie, het gebruikte apparaat, de log-ingeschiedenis en andere factoren. Als het vermoedt dat er iets aan de hand is, zal er sneller informatie opgevraagd wordt om de gebruiker te verifiëren. Zo nodig wordt er ook een mailtje gestuurd om het wachtwoord te veranderen.

Tails

Iedereen weet dat Edward Snowden veilige e-mail aanraadt. Hij is echter ook heel kieskeurig in de keuze van zijn besturingssysteem. Hij gebruikteen gratis, superveilige versie van Linux. Tails past op een USB stick en kan op elke computer gebruikt worden zonder dat het een spoor achter laat.

"De hard disk wordt niet ge-bruikt"

Linux op een USB stick is niets nieuws, maar Tails is een besturingssysteem dat geoptimalizeerd is voor anonimiteit. Het systeem wordt daarom gebruikt door onder andere Edward Snowden en journalist Glenn Greenwald. Zoals de (uiteraard) anonieme ontwikkelaar het zelf zegt is "Tails een systeem dat zich richt op het behoud van privacy en anonimiteit. Het helpt je om het internet anoniem te gebruiken en censuur te omzeilen. Het systeem werkt op bijna alle computers en laat geen enkel spoor achter tenzij je er om vraagt. Het is een compleet besturingssysteem dat gebruikt kan worden vanaf een DVD, USB of SD kaart onafhankelijk van het besturingssysteem dat al op de computer staat."

Dit klinkt zowel handig als verdacht. Het ligt er net aan hoe je het bericht leest. De ontwikkelaars van het systeem blijven anoniem om de overheid geen invloed te geven in het ontwikkelproces.

Tails gebruikt Tor, PGP, KeePassX om wachtwoorden te bewaren en een speciaal ontwikkelde chat code genaamd Off-the-Record om anoniem te blijven. Het besturingssysteem is zo ontwikkeld dat er geen spoor achterblijft op de computer waarop het draait. De ontwikkelaars leggen het uit:

"Tails is geprogrammeerd om geen gebruik te maken van de harde schijf. Het enige geheugen wat Tails gebruikt is RAM. De data in dit geheugen wordt automatisch verwijderd als de computer afgesloten wordt. Op die manier laat je geen sporen achter van het besturingssysteem of wat je hebt gedaan op de computer."

Veilig online bankieren met Bitdefender Safepay

Nu mag je wel over je schouder kijken en een ijzersterk wachtwoord of zelfs een kaartlezer gebruiken, je zal niet de eerste zijn die tijdens het online bankieren of winkelen het slachtoffer van hackers of malware wordt. Bitdefender Safepay maakt het die onverlaten alweer een flink stuk lastiger. Het geheim van Bitdefender Safepay? Een uitgeklede browser in een virtuele omgeving, veilig afgescheiden van de rest van je systeem! Ik ga alvast voor de gratis versie. De Premium-versie biedt je voor circa 25 euro per jaar ook een veilige wifi-omgeving.

"Bitdefender Safepay houdt hackers en malware uit je browser en geeft je wat meer gemoedsrust tijdens het online winkelen of bankieren."

Je kan Bitdefender Safepay downloaden via de downloadlink in dit artikel. Na de installatie moet je nog een account creëren: Create a new account, vul de gevraagde gegevens in en klik op de link in de bevestigingsmail. Je zal merken: standaard speurt Bitdefender Safepay eerst naar potentiële malware. Pas wanneer het licht op groen staat, schakelt die over naar de gevirtualiseerde browser. Je bureaublad lijkt geheel verdwenen, maar via de rode driehoek linksboven (Switch to Desktop) haal je je vertrouwde omgeving terug. Rechtsboven je bureaublad vind je dan een "terugkeer-knop" terug: Switch to Safepay.

Zo'n initiële scanronde is wel zo veilig, maar je moet telkens wat geduld uitoefenen. Als je dat echt wil, kan je die scan ook uitschakelen. Klik dan het kamwiel-icoontje van de browser aan (Settings) en stel Scan the system for active infections when starting Bitdefender Safepay in op Off.

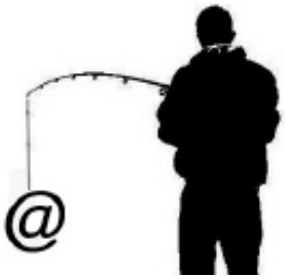
Verder werkt de browser zoals elke andere. Rechts van de adresbalk tref je wel nog een printerknop aan evenals de knop Add Bookmark. Met deze laatste voeg je de actuele site toe aan je favorietenlijst. De knop Bookmarks verschaft je toegang tot die lijst. Tot slot: links bevindt zich een knopje waarmee je een virtueel toetsenbord tevoorschijn haalt. Nog zo veilig om gevoelige informatie in te tikken en op die manier een eventuele keylogger te slim af te zijn. Als het werkt tenminste, wat op mijn toestel jammer genoeg niet het geval bleek.

Bron: ZDnet

Klik op het plaatje voor de download >

Waarschuwing: phishingmail in naam van het Rijk waart rond

De nog altijd actieve Waarschuwingsdienst van het Ministerie van Veiligheid en Justitie waarschuwt voor phishers. Die opereren zogenaamd namens de overheid zelf.



De phishingmail pretendeert namelijk afkomstig te zijn van de Rijksoverheid. De e-mail waarschuwt op zijn beurt voor de "non-actiefzetting van uw bank account", want op zichzelf al niet heel geloofwaardig overkomt. Desondanks komt de Waarschuwingsdienst van het Ministerie van Veiligheid en Justitie met een officieel alarm.

De e-mail in kwestie bevat kwaadaardig links naar nagemaakte website van de verschillende grote banken. In ieder geval de ING, Rabobank en SNS worden genoemd. Doel van de makers is om inloggegevens van het internetbankieren te bemachtigen.

Voorbeeld:

Van: RIJKSOVERHEID [mailto:beveiligdeupdate@rijksoverheid.nl]

Onderwerp: Let op! Voorkom non-actiefzetting van uw account

Geachte heer/mevrouw,

De overheid spendeert veel aandacht en zorg aan de beveiliging en integriteit van al onze banken in Nederland.

Vooral aan de volgende banken: ING BANK N.V., RABO BANK N.V. en SNS BANK N.V. Er zijn veel klachten in gekomen over bankproblemen en banken raken falliet. Om dit te stoppen moet u uw account beveiligen, zodat er geen fraude problemen meer kunnen gebeuren. De overheid heeft met de banken gesproken en die hebben een webpagina gemaakt om uw account te beveiligen.

Na de activatie word u automatisch uitgelogd, zodra u de activatie start bent uw die verplicht af te ronden om defecten te voorkomen. Kies de bank die bij uw past.

Klik hier om uw ING BANK N.V. account te beveiligen.

Klik hier om uw RABO BANK N.V. account te beveiligen.

Klik hier om uw SNS BANK N.V. account te beveiligen. Let op! ·

Om veiligheidsredenen is deze link maar enkele dagen geldig. ·

Deze e-mail kan niet beantwoord worden. · Dit e- mailbericht is alleen bestemd voor de geadresseerden. · Indien dit bericht niet voor u is bedoeld, wordt u verzocht de afzender hiervan op de hoogte te stellen door het bericht te retourneren en de inhoud niet te gebruiken. · Aan dit bericht kunnen geen rechten worden ontleend. · Het kan zijn dat sommige computers het moeilijk hebben met de capaciteit van de website en niet alles zichtbaar is. Om er zeker van te zijn dat de Rijksoverheid e-mails goed aankomen, voeg rijksoverheid@emailing.nl toe aan uw adresboek of safe list.

Met vriendelijke groet,

Rijksoverheid Afdeling Internetbankieren en Beveiliging

Cybercriminelen maken meer kans bij vrouwen

Cybercriminelen kunnen het beste hun pijlen richten op vrouwen. Die updaten niet of nauwelijks hun virusscanner of securitysuite en surfen onbekommerd op het internet.

Aan de andere kant hebben vrouwen wel meer zelfkennis: slechts 10 procent denkt voldoende kennis te hebben over online bedreigingen en bescherming hiertegen, zegt Kaspersky Labs, die onderzoeker MediaTest de beide seksen aan een stel vragen onderwierp om duidelijkheid te krijgen over de verschillen tussen man en vrouw.

Mannen beter gewapend, vrouwen nalatig

Het onderzoek is gehouden onder 2000 Nederlandse en Belgische mannen en vrouwen die frequent het internet gebruiken. de conclusie is: mannen wapenen zich beter tegen cybercriminaliteit dan vrouwen. Verder bleek dat het grootste deel van de beide seksen beveiligingssoftware gebruikt, maar dat vrouwen nogal nalatig zijn in het updaten ervan.

Opvallend is dat vrouwen het gevaar op de smnartphone hoger inschatten dan mannen, maar dat de risico's op de pc en tablets worden onderschat. Maar, zo zegt Kaspersky, vrouwen "zijn er over het algemeen goed van op de hoogte dat ze niet goed op de hoogte zijn."

Zoeken naar bewijs in digitale docs aan banden gelegd

Je mag niet zomaar beslag laten leggen op digitale documenten op zoek naar bepaalde steekwoorden. Die sleepnetmethode is door de rechtbank in Overijssel afgewezen in een civiele zaak.

Het leggen van een beslag op digitale documenten om die te doorzoeken op bewijs is niet toegestaan, vindt de kantonrechter. Hij vindt dat een sleepnetmethode die te ruim is. Iemand die beslag wil leggen op documenten moet eerst duidelijk maken welke documenten hij zoekt. Je mag geen bewijs zoeken in digitale documenten via het invoeren van zoektermen in Google als niet eerst precies is vastgelegd welke documenten dat zijn.

De kantonrechter in Overijssel deed die uitspraak in een zaak waarbij twee bedrijven die gewikkeld waren in overnamegesprekken alle digitale bestanden van een niet nader genoemde persoon wilden hebben door het laten opleggen van een beslag.

Alle informatie van alle gegevensdragers

Waarop die documenten stonden maakte niet uit, van een pc, een usb-stick, servers, CD's, DVD's, DAT tapes of smartphone, de twee bedrijven wilden alles hebben. Met als doel alle documenten te laten doorzoeken door een forensisch IT-specialist vanDigiJuris op een aantal steekwoorden, tien in totaal.

De rechter verwijst naar een eerder arrest van de Hoge Raad, die de reikwijdte van een dergelijk verzoek al eerder te ver zag gaan. "Een bewijsbeslag is een ingrijpend dwangmiddel waardoor onder omstandigheden aan de wederpartij aanzienlijke hinder of schade kan worden toegebracht. Het beslag mag slechts worden gelegd op de in het verzoekschrift genoemde bescheiden."

Geen visexpeditie!

Die beschrijving in het verzoekschrift moet zo precies zijn "omdat de beslaglegging niet mag ontaarden in een fishing expedition", meent de Hengelose rechter. "Maar in dit geval kunnen de bedrijven dus kennelijk pas na die doorzoeking en dus pas na kennisneming van de inhoud van die documenten aanwijzen van welke bepaalde bescheiden zij inzage, afschrift of uittreksel wil vorderen."

En dat is te ruim, vindt de rechter en dus gaat het feest niet door.

Bron: Webwereld

De gevaren van bestanden opslaan op je bureaublad

Zolang als ik me kan herinneren heeft geen enkele versie van Windows ooit standaard bestanden als documenten en spreadsheets op het bureaublad opgeslagen. En sinds XP is het ook niet bepaald een veilige plek om ze op te slaan. Toch kunnen sommige mensen de verleiding

Er zijn goede redenen om bestanden niet op het bureaublad op te slaan. Om te beginnen is het lastig te ordenen. Hoewel je bestanden op het bureaublad op naam en datum kunt sorteren, kun je ze niet op een tweede criterium groeperen. En het kan overweldigend druk worden, iets wat niet het geval is met een groepeerbare, doorzoekbare map.

En er staan bijna altijd applicatievensters voor, waardoor een deel van je bestanden niet te zien zijn. Je kunt natuurlijk altijd die vensters verbergen of minimaliseren, maar daardoor krijg je wel een extra laag met gedoe.

Niet goed beveiligd

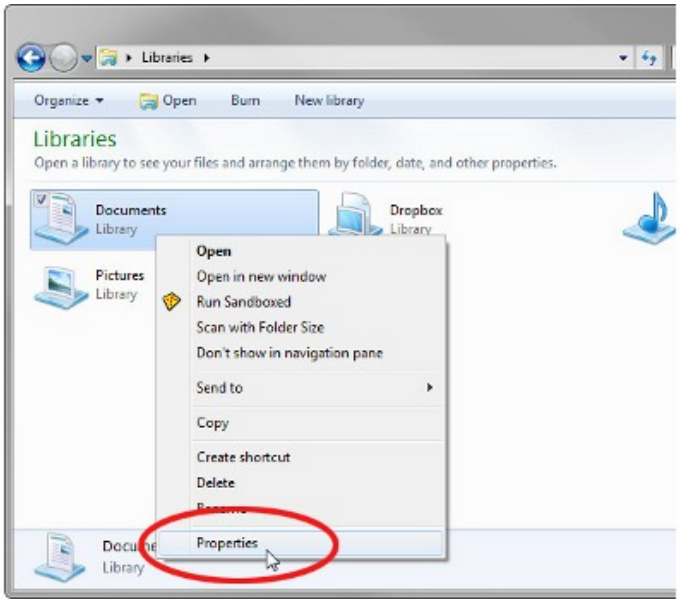
Het belangrijkste is, dat bestanden op het bureaublad niet zo goed beschermd zijn als bestanden in libraries zoals My Documents en My Pictures. Als je bijvoorbeeld System Restore gebruikt om Windows te herstellen naar de staat van afgelopen woensdag, dan zal deze functie alle bestanden die na deze datum aan het bureaublad zijn toegevoegd verwijderen. De bestanden in My Documents zullen echter onaangeroerd blijven.

Bovendien back-uppen veel back-up programma's niet standaard het bureaublad. Je kunt dat natuurlijk ergens in de instellingen van je back-up programma veranderen.

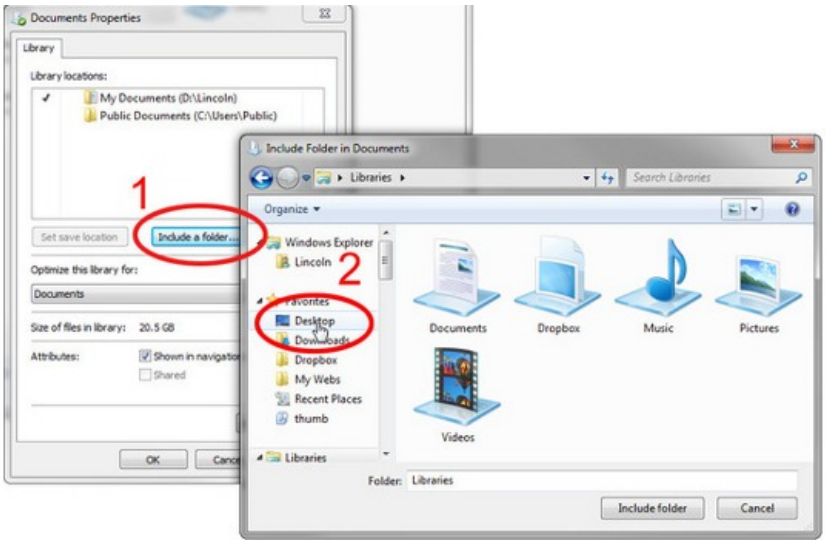
Als je toch naar het bureaublad wilt back-uppen zul je Windows een beetje aan moeten passen om het veiliger te maken - en handiger.

Ten eerste zul je het bureaublad aan de Documents library moeten toevoegen. Dit beschermt het bureaublad tegen veranderingen door System Restore en mogelijk wordt het bureaublad ook aan back-ups toegevoegd. Zo stel je het in:

In het Library gedeelte van Windows Explorer (File Explorer in Windows 8), klik met de rechtermuisknop op Documents en selecteer Properties.



Klik in het dialogvenster op de optie Include a folder en selecteer het bureaublad. Je kunt het bijna bovenaan in het Navigation paneel vinden, onder Favorites.



Als je wilt dat programma's standaard naar het bureaublad opslaan, selecteer Desktop in de Library locations lijst en klik op Set save location. Op die manier zal het bureaublad de eerste plek zijn waar een programma je document, spreadsheet, of alles wat geen foto, video, of muziekbestand is probeert op te slaan.

Bron: Security.nl

Security Essentials onderuit tijdens anti-virustest

Microsoft Security Essentials is tijdens een recente anti-virustest van Dennis Technology Labs hard onderuit gegaan. Tijdens januari tot en met maart werden in totaal tien beveiligingsoplossingen blootgesteld aan echte internetdreigingen, zoals drive-by downloads en webgebaseerde malware.

Van de 100 malware-exemplaren waar de verschillende scanners mee werden getest, wist Microsofts gratis scanner er uiteindelijk maar 60 te stoppen. 34 werden er direct gedetecteerd en in 26 gevallen werd de malware gestopt nadat die al op het systeem was verschenen. Alle overige producten stopten 90 of meer van de dreigingen, waarbij Kaspersky Lab zelfs een perfecte 100% scoorde.

Op het gebied van onterechte waarschuwingen voor legitieme, schone software, de zogeheten 'false positives', presteerde Microsoft wel feilloos. Samen met Kaspersky, Avira, AVG en BitDefender haalde Microsoft een 100% score.Aan de hand van de resultaten bij de detectie van malware en false positives kregen uiteindelijk Kaspersky Lab, Norton en ESET de hoogste beoordeling.

Bron: PCM

PROTECTION DETAILS

Product	Defended	Neutralized	Compromised
Kaspersky Internet Security 2014	98	2	0
McAfee Internet Security	99	0	1
Norton Internet Security	99	0	1
Trend Micro Titanium Internet Security	86	12	2
ESET Smart Security 7	91	6	3
BitDefender Internet Security	64	29	7
Avast! Free Antivirus 9	91	1	8
AVG Anti-Virus Free 2014	78	14	8
Avira Internet Security	46	44	10
Microsoft Security Essentials	34	26	40

Google maakt tool om jezelf uit zoekresultaat te halen

Google werkt aan een online tool om jezelf uit de zoekresultaten te laten filteren. De tool wordt ontwikkeld naar aanleiding van de uitspraak van het Europees Hof dat burgers het recht hebben 'vergeten' te worden.

Google werkt aan een tool om mensen makkelijker toegang te geven tot de procedure waarmee zoekresultaten over jezelf kunnen worden gefilterd uit Googles zoekmachine. Dat zegt Johannes Caspar, de commissaris voor informatiebescherming in het Duitse Hamburg.

De tool moet het proces automatiseren omdat Google voorziet dat het een leger aan medewerkers nodig heeft om toekomstige verzoeken af te handelen. Het Europese Hof stelde eerder deze week dat zoekmachines persoonlijke informatie van mensen niet meer mag tonen als het niet meer relevant is, of al te zeer de privacy schendt.

Tools worden verder uitgebreid

Het bedrijf heeft al enkele tools die mensen de mogelijkheid geeft bepaalde standaard info te laten uitfilteren, zoals handtekeningen, verzekerings- of paspoortnummers of bankgegevens. Die mogelijkheden worden nu uitgebreid en de tool wordt verder geautomatiseerd, schrijft de internationale newsservice van IDG, uitgever van Webwereld.

Google zegt in een e-mail dat het nog enkele weken gaat duren voordat het bedrijf helemaal de werking en logistiek eromheen op orde heeft. De Duitse databeschermingsorganisatie DPA pleit voor een Europabrede afstemming over de criteria van hetgeen onder het recht om te worden vergeten moet vallen.

Bron: Webwereld

CSI in de digitale polder

Net als bij een gewone bedrijfsvoering, maken ook criminelen gretig gebruik van ICT-middelen. Dat biedt kansen voor de politie. Als een moderne Sherlock Holmes gaat een recherchekundige tijdens het onderzoek op zoek naar digitale sporen die een verdachte heeft achtergelaten.

Om criminaliteit aan te pakken is, naast onder andere tactische en forensische expertise, tegenwoordig steeds vaker digitale deskundigheid nodig. Plaatselijke en regionale onderzoeksteams schakelen hiervoor rechercheurs in met ICT als specialisatie. Ze hebben een driejarige opleiding tot Recherchekundige Digitaal ('reku') gevolgd aan de Politieacademie in Apeldoorn, waar alleen kandidaten met een hbo-diploma op ICT-gebied worden toegelaten.

Een Recherchekundige Digitaal is niet zomaar een ICT'er - alle reku's krijgen behalve trainingen in digitale recherche ook opleidingen in het reguliere politiewerk, inclusief politie-uniform en uitrusting. Reku's zitten niet alleen op kantoor achter pc's, maar hebben geweld- en aanhoudingsbevoegdheid. Behalve een scherp analytisch en conceptueel vermogen, zelfinzicht en integriteit, wordt van hen ook een ijzersterke conditie verwacht - niet alleen om opgewassen te zijn tegen fysiek veldwerk, maar ook omdat het werk emotioneel zwaar kan zijn.

Schimmige wereld

Een van de plaatsen waar de reku's na hun opleiding kunnen worden ingezet is het Team High Tech Crime (THTC), dat zich richt op geavanceerde cybercriminaliteit met een grote maatschappelijke impact of onderzoeken waar meerdere verdachten bij betrokken zijn. THTC staat internationaal in hoog aanzien en werkt samen met opsporingsinstanties in andere landen. Ze ontvangen en dienen ook zelf rechtshulpverzoeken in. Dat kan ook niet anders. In de digitale wereld ben je immers zo de grens over.

Michiel Kok is tactisch coördinator bij THTC. Na tien jaar in de automatisering te hebben gewerkt en succesvol een HEAO-opleiding te hebben afgerond, hakte hij de knoop door en maakte de overstap naar de politie. Iets wat hij altijd al wilde doen.

"Ik kwam bij THTC terecht om een rol te vervullen bij een onderzoek rondom Robert M. (de beruchte Amsterdamse zedenzaak uit 2010 - red.)," vertelt hij ons. "Robert M. had veel connecties met andere verdachten, legde daar ook dingen over vast, maar het is een schimmige wereld, met valse namen, afgeschermde ip-adressen en websites vol kinderporno op het TOR-netwerk. Wij hebben intensief onderzoek gedaan om zijn medeplichtigen op te sporen. Er waren uiteraard wel eerder zedenzaken geweest, maar nog nooit op deze schaal. Daarin heeft THTC de politieteams ondersteund die het onderzoek waren gestart."

Kansrijke sporen

Een forensisch expert is tegenwoordig een vast onderdeel van een onderzoeksteam, maar een digitale expert zit er nog niet altijd bij. Toch wordt de Recherchekundige Digitaal wel steeds vaker ingezet bij onderzoeken. Michiel Kok: "Net als bij een normale bedrijfsvoering, gebruiken ook criminelen computertechnologie. Om hun communicatie af te schermen, of concurrenten in de gaten te houden bijvoorbeeld. Het begint met een laptop, dan een netwerk en dat willen ze natuurlijk afschermen tegen hackers.

"ICT is voor criminelen belangrijk en dat biedt belangrijke kansen voor de politie. Wat wij op digitaal gebied kunnen doen is zeer uiteenlopend. Zoals systemen die zijn gehackt of door een verdachte zijn gebruikt in beslag nemen, een image van een server maken, of het veiligstellen van logfiles."

Samen met de beheerders van een provider of datacenter doet een recherchekundige er alles aan om informatie te achterhalen die een onderzoek verder kan helpen. Michiel: "Een hacker kan op een bepaald systeem bestanden hebben achtergelaten, of er zijn sporen te vinden in logfiles. Een verdachte kan bewijsmateriaal hebben vernietigd, maar ook dan zijn er nog kansen. Een gedegen kennis van ICT en een goed contact met de beheerders is daarom van essentieel belang om dan alsnog kansrijke sporen te vinden."

Hopen op fouten

Tijdens een opsporingsonderzoek is het zaak om net zo lang na te denken en te zoeken, tot foutjes worden gevonden die de verdachte heeft gemaakt. Michiel Kok: "Daar valt of staat alles mee. Met het vinden of uitlokken van fouten. We zijn al sporen volgend wel eens digitaal de halve wereld over gereisd, tot Korea aan toe, waarna de hacker in Barendrecht bleek te wonen en daar kon worden aangehouden."

Een recherchekundige moet een helikopterview hebben en herkennen welke digitale mogelijkheden zich in een onderzoek voordoen. Weten waar mogelijk sporen zijn achtergebleven. Zoals in camera's, telefoons, de apps die op het toestel staan, of geografische data in foto's.

"Digitale data is vaak vluchtig," vertelt Michiel. "Een verdachte heeft misschien ergens met zijn telefoon rondgelopen. Dan moet de data uit die zendmasten snel bevroren worden. Want ook al heeft een verdachte niet gebeld, de zendmast is dan wel aangestraald. Een recherchekundige moet goed zicht hebben op hoe de infrastructuur er in de snel veranderende digitale wereld uitziet. Hij moet ook weten welke waarde hij aan sporen moet hechten. In tegenstelling tot DNA is data niet uniek, dus iemand kan ten onrechte verdacht worden gemaakt door data te reproduceren."

Tactische operatie

Zodra de verdachte is opgespoord en er tot aanhouding kan worden overgegaan, breekt een spannend moment aan. "Je weet niet wat je aantreft als je bij de verdachte naar binnen gaat," vertelt Michiel Kok. "Hoe gedraagt hij zich, hoe reageert de omgeving, zijn er meer mensen in huis. Natuurlijk zoeken wij van te voren zo veel mogelijk uit en iedereen in het team is erop getraind. We hebben een blindelings vertrouwen in elkaar en het kameraadschap is hoog. Samen naar binnen, de verdachte aanhouden, de apparatuur in beslag nemen en hopen dat die open wordt aangetroffen, dus niet encrypted."

"De aanhouding is een tactische operatie. Een Recherchekundige Digitaal gaat mee, heeft dan ook een volwaardige politieopleiding gevolgd en praktijkervaring opgedaan. Toch is het vooral een kantoorbaan, al wordt er ook gereisd om sporen veilig te stellen. Er is altijd een team oproepbaar en we draaien piket. Als we vanavond een verdachte mogen aanhouden, staan we allemaal klaar. Die flexibiliteit is er, net als de gedrevenheid om het goede te willen doen."

Nooit hetzelfde

Het onderzoeksveld van een recherchekundige verandert continu. "Je weet nooit alles van internet of software," vertelt Michiel Kok tot besluit. "Technieken en methoden veranderen snel. Je moet daarom leren anticiperen. Je weet grofweg hoe de wereld in elkaar steekt, maar komt tijdens opsporingsonderzoeken steeds weer andere manieren tegen hoe er gehackt is, nieuwe malware-varianten of phishingtechnieken. Daar kun je op anticiperen dankzij de kennis en ervaring die je al hebt opgedaan. Wat dat betreft variëren de onderzoeksmogelijkheden per maand. Berichten op Whatsapp waren bijvoorbeeld goed inzichtelijk te krijgen, maar die data is nu encrypted. De digitale wereld is steeds weer anders en dat is heel erg gaaf. We blijven maar bezig, het gaat keihard."

Dit artikel is tot stand gekomen in samenwerking met de Landelijke Eenheid van de Nationale Politie.

Bron: Webwereld ContentWorks IDG

Snapshots:

Waarschuwing voor phishingmail Justitieel Incassobureau

Het Nationaal Cyber Security Center waarschuwt internetgebruikers voor phishingmails die zogenaamd van Rijksoverheidspartijen zoals de Belastingdienst en het Centraal Justitieel Incassobureau (CJIB) afkomstig lijken en ontvangers tot het betalen van een boete proberen te verleiden.

De phishingmail die van het CJIB afkomstig zou zijn heeft als onderwerp "Betaalverzoek inzake CJIB uw referentie 730116882" en stelt dat de ontvanger een schikking en vervolgens twee keer een aanmaning heeft ontvangen wegens een verkeersovertreding. De boete zou echter nog niet zijn betaald. "Daarom zullen wij de bank opdracht gegeven uw rekening te blokkeren per maandag 12 mei 2014", aldus de tekst in de e-mail, waarin de nodige typefouten zijn te vinden. "Het blokkeren van rekening betekent dat de toegang tot uw rekening geblokkkeerd is met ingang 12-05-2014 voor een periode van vier werken", laat de tekst verder weten.

Vervolgens krijgt de ontvanger instructies om het openstaande boetebedrag van 100,99 euro via Ukash te betalen. Wordt dit niet gedaan, dan wordt er ook met een registratie bij het BKR gedreigd. Ukash prepaid creditkaarten zijn bij allerlei benzinestations en winkels verkrijgbaar. De phishingmail die nu rondgaat bevat een link naar een website waar de code die op de Ukash prepaidkaart staat kan worden ingevuld.

Verdachten van phishingaanval op Raboklanten opgepakt

Een speciaal onderzoeksteam van de Haagse politie heeft drie mensen aangehouden wegens het uitvoeren van phishingaanvallen op Rabobankklanten en fraude met internetbankieren. Het gaat om een omvangrijke zaak waar zeker 70 bankklanten het slachtoffer van oplichting werden.

Een vrouw die zich voordeed als medewerkster van de Rabobank ontfutselde op slinkse wijze inlog- en signeercodes van internetbankieren. Zodra de internetcriminelen over de codes beschikten maakten zij geld over naar onder andere juweliers die veelal kostbare horloges verkochten via internet. De juweliers waren voor die tijd al benaderd met het verzoek of bepaalde dure horloges nog op voorraad waren.

Vervolgens vond telefonisch overleg plaats tussen de juwelier en - naar later zou blijken - de fraudeur met de vraag of het geld overgemaakt kon worden op een bankrekening, of werd medegedeeld dat het geld zojuist was overgemaakt. Naast dure horloges verlegden de verdachten hun terrein steeds meer naar dure auto’s. De auto's werden aangekocht bij autobedrijven en werden ook hier door de zogeheten katvangers opgehaald.

Het geld werd rechtstreeks overgeboekt van de rekening van het slachtoffer, van wie even daarvoor de inlog- en signeercodes waren ontfutseld. Met de juwelier of met het autobedrijf werd afgesproken dat een familielid de horloges of auto zou komen ophalen. Deze persoon, een zogenoemde katvanger, meldde zich vervolgens in de winkel of bij de dealer en ging er met de bestelling vandoor. Dit ging overigens niet altijd goed.

Soms kon de Rabobank op tijd ingrijpen en de juwelier of autodealer meldden dat er sprake was van een frauduleuze overschrijving, of roken zij zelf al onraad. Door snelle interventie werd voorkomen dat voor tenminste 400.000 euro aan frauduleuze overschrijvingen plaatsvonden. In een aantal gevallen kwam de waarschuwing echter te laat en wisten de katvangers er met de horloges of auto’s vandoor te gaan. Toen de zaak vorig jaar aan het licht kwam bleek er al voor 200.000 euro te zijn gestolen.

Marktplaats vol ‘fake’ accounts en oplichting

Wat Marktplaats ook doet om oplichting tegen te gaan, het werkt nog niet echt. Dat schrijft de website OHLN dat na onderzoek concludeert dat nog dagelijks tientallen mensen worden opgelicht. Enerzijds worden dagelijks ‘tal van accounts’ aangemaakt voor ‘foutieve doeleinden’, anderzijds bieden nepgebruikers ‘op honderden, misschien wel duizenden’ producten. Marktplaats zegt foute accounts binnen 24 uur te kunnen onderscheppen. Maar dat is nog lang niet genoeg, aldus het bericht: ‘deze aanpak komt vaak te laat’. Een relatief nieuw probleem is de handel in inactieve accounts. Daarbij worden gebruikers die lange tijd niks gekocht/aangeboden hebben, door oplichters benaderd om het account te verkopen.

Europol gaat cybercriminelen voortaan 'dwarszitten'

Omdat vervolging van cybercriminelen weinig oplevert, gaat Europol deze groep vaker dwarszitten dan oppakken. Volgens Troels Oerting, hoofd van de cybercime-afdeling van Europol, wordt het steeds moeilijker om de identiteit van cybercriminelen te achterhalen. Door het toenemende gebruik van tornetwerken lukt het ze steeds vaker om identiteit en locatie te verbergen. Als dat wel lukt, zijn het in driekwart van gevallen Russen. 'Die zijn buiten ons bereik'. Omdat er geen uitleveringsverdrag is met Rusland, is lokale vervolging 'het beste waar we op kunnen hopen'. Oerting sprak op het Infosec congres in Londen. Hij stelde dat het effectiever is cybercriminelen te hinderen. Dat kan als banken en winkels beter met elkaar en met de politie samenwerken door meer informatie uit te wisselen.

Wet id-fraude in werking

Per 1 mei 2014 is het mogelijk om alle vormen van identiteitsfraude aan te pakken. Met de nieuwe wet, die fraude met reisdocumenten, rijbewijzen, vreemdelingendocumenten en identiteitsbewijzen verbiedt, kan justitie ook optreden tegen mensen die fraude plegen met de persoonsgegevens van een ander. Daarbij het gaat het om naam, adres en telefoonnummer, maar ook om accountnamen en aliassen of nicknames op internet. Wie zich schuldig maakt aan identiteitsfraude, kan maximaal vijf jaar celstraf krijgen.

Een soort Laatjewietthuisbezorgen punt nl

'Met het businessmodel van Bol.com of Thuisbezorgd.nl' proberen coffeeshophouders het advertentieverbod te omzeilen. Zeven coffeeshops in negen steden hebben zich verenigd in Coffeeshopbon.nl, een website die stelt geen coffeeshop te zijn maar alleen tussenpersoon. Klanten kopen er bonnen, bestellen bij een aangesloten coffeeshop en krigen binnen 24 uur hun bestelling – voorgedraaide joints, van Nederlandse biowiet of tropische Thaiwiet – thuisbezorgd, schreef NRC vorige week al. Dat internet oprukt in de drugshandel was al lang bekend, maar dat betreft vooral hard drugs. Omdat zo'n 90% van de wiethandel via coffeeshops verloopt, was de rol van internet op de cannabismarkt lange tijd 'verwaarloosbaar klein'. De mensen achter de nieuwe site denken uiteindelijk een kwart van de cannabismarkt te kunnen bedienen met hun online initiatief. 'Niet iedereen wil voor cannabisproducten naar een coffeeshop gaan', stelt Alexander; alleen met voornaam in de krant omdat nog onduidelijk is of justitie tegen zijn site optreedt. 'Wij verkopen alleen tegoedbonnen', via iDeal ook nog eens. 'En er wordt gewoon belasting betaald'. Volgens burgemeester Paul Depla van Heerlen kan het initiatief een oplossing zijn voor overlast op straat maar niet voor 'de criminaliteit aan de achterdeur'. Ook het Trimbosinstituut is wantrouwend. 'Coffeeshops leveren kwalitatief goede en betaalbare drugs. Bestel je via internet, dan moet je maar afwachten wat je krijgt'. Een woordvoerder van Justitie meldt dat de handel via internet 'niet in het gedoogbeleid past'. Maar volgens de krant is het nog maar de vraag of justitie de internethandel – alleen al vanuit Nederland opereren zo'n 25 illegale sites – kan stoppen. Justitie heeft volgens een woordvoerder van het Trimbosinstituut nauwelijks middelen om die sites te sluiten. 'De mensen achter die sites hebben in principe weinig te duchten.'

Plaats delict: Social Media

Voor wie Vrij Nederland gemist heeft, met dat fraaie verhaal over hoe de politie op internet actief is, is er natuurlijk de website.

Klik HIER voor het artikel

Cops in cyberspace Blog

Door een simpele tweet van een burger wist de politie binnen een uur een verdachte aan te houden die een aanrijding had veroorzaakt in Dieren. De man had een lantaarnpaal omver gereden maar was doorgereden. Een getuige zag het gebeuren en twitterde de politie, die met deze informatie de man wist op te sporen. De man wordt ook verdacht van rijden onder invloed.

Onderwijsassistent Raymond van G. (27, uit Veenendaal) is door de rechtbank veroordeeld tot twee jaar celstraf, waarvan tien maanden voorwaardelijk, nadat bij hem 7200 kinderpornofoto's en 2300 -films waren gevonden. De man, trainer bij het korfbal en organisator van kindervakantieweken, haalde zijn collectie binnen via tor-netwerken. Hij liep tegen de lamp tijdens een Russisch onderzoek waarbij zijn ip-adres gevonden werd. De man had alle bestanden versleuteld en werkte volgens het OM niet actief mee aan het politieonderzoek.

In niet meer dan dertig seconden kun je op Instagram drugs vinden. Maar het duurt niet veel langer voordat je de verkoper ontmaskerd hebt. De gemiddelde instagram-dealer lijkt niet al te slim: een op de drie heeft bij zijn profiel een herkenbare foto, aldus DrugAbuse.com. De site deed onderzoek naar het fenomeen en merkte vooral dat verkopers zich onaantastbaar wanen: ze adverteren openlijk, met telefoonnummers en accountnamen erbij, ze gebruiken traceerbare rekeningen bij PayPal en GreenDot, en UPS en FedEx voor het verzenden. Meer dan de helft maakte foto's van het geld dat ze met hun handeltjes verdienden. 'Brilliant drug lords they are not', stelt DrugsAbuse dan ook. De politie vindt de dealertjes dus eenvoudig, de foto's worden als bewijs gebruikt. En door rechters geaccepteerd, blijkt uit de zaak van een grote Mexicaanse drugsdealer die begin dit jaar op Schiphol werd opgepakt. Eind 2013 scoorde de NYPD de 'biggest gun bust ever' : één fotootje op Instagram leidde uiteindelijk tot honderden arrestaties.

De rechtbank in Rotterdam heeft twee mannen (uit Zetten en Arnhem) die drugs verkochten via internet, veroordeeld tot celstraffen van vier en vijf jaar. De mannen handelden onder de naam XTC Express en boden vooral synthetische drugs aan op Silk Road. De pillen hadden 'een levensgevaarlijke concentratie' mdma. Daarmee stelden ze hun klanten (in onder meer de VS, Canada en Australië) 'willens en wetens' bloot aan ernstige gezondheidsrisico's, aldus het vonnis. Het dealerduo werd oktober 2013 op heterdaad betrapt bij de fabricage van drugs. Ze hadden ruim een ton cash, meer dan 325 bitcoins en andere dure spullen in bezit. Het OM had zes jaar geëist. In de VS loopt op dit moment de rechtszaak tegen Maikel S. (23, uit Woerden) die voor miljoenen euro's aan drugs verhandelde via Silk Road.

De landelijke eenheid van de politie heeft 'verhoogde aandacht' voor de handel in drugs (en wapens) op websites die via het TOR-netwerk toegankelijk zijn en waar met bitcoins betaald wordt. Sinds de FBI eind 2013 Silk Road oprolde, doken vergelijkbare sites op, waar drugs, medicijnen, wapens, valse paspoorten en creditcards en zelfs huurmoordenaars kon worden besteld. Het NRC inventariseerde dat op 'Silk Road 2.0' en 31 andere TOR-sites duizenden advertenties waarin drugs werden aangeboden maar ook een pillenpers en diverse fabricagehandleidingen. De politie zegt in een reactie 'niet te kunnen toelaten dat via moeilijk te achterhalen websites verboden wapens en drugs wordt verhandeld'. Volgens een woordvoerder lopen er 'verschillende onderzoeken' tegen internethandelaren en zijn er onlangs ook websites offline gehaald.

Burgers die elkaar op de hoogte houden van verdachte gebeurtenissen en diefstallen – het is nu ook in Heemskerk mogelijk. Een man uit die plaats nam het initiatief tot de pagina Heemskerk Meldt nadat de aanhanger van een vriend van hem was gestolen. 'In de wijk waar ik woon doet de wijkagent niet aan sociale media', verklaart hij zijn actie. En 'omdat meldingen die bij de politie worden gedaan, niet bekend zijn onder inwoners'. De pagina is bedoeld voor diefstallen, inbraken 'en andere misdaden in de gemeente'. Volgens de maker (die anoniem wil blijven) zijn dat vaak zaken die niet door de politie wordt opgepakt. 'Vaak voel je je machteloos en kan de politie niks voor je betekenen'.

Dankzij een volg-app op een gestolen smartphone heeft de politie een man (57, uit Oss) weten aan te houden die een woninginbraak had gepleegd. De man werd getraceerd met de app en kon daardoor relatief snel gevonden worden. Bij zijn aanhouding had hij de gestolen smartphone op zak. De man is aangehouden. Een politieman deed aangifte tegen de verdachte nadat deze de agent, en zijn familie, met de dood had bedreigd.