



Augustus 2015

JAARGANG 4

Secure

Computing

Meer en meer wordt er gebruik gemaakt van Twitter. Nog geen Twitter account? In dit nummer leest u hoe dit te realiseren. Kunt u tijdens uw vakantie 'uw volgers' op de hoogte houden.

In bijna elk artikel zijn hyperlinks opgenomen. Klik erop en u ziet meer informatie!



Veel lees(r)plezier

(NB: met Ctrl+ scrolwielje kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen.)



W. Bosgra Taakaccenthouder Digitale Criminaliteit Basisteam Enschede



Snel index

Klik op een link voor snelle toegang tot het artikel.

Om terug te keren naar de snelindex klikt u onderaan de pagina op Index

Bronnen:

Security.nl, PCMweb, ZDnet, Webwereld, Comptable, Bits of Freedom, Cops in Cyberspace, De Digitale Revolutie, PCwereld, PCpro, Klikx, Peppermunt.net, PrivacyNieuws, HackInfo, HardwareInfo, Bright, Computerworld

[Virtuele diefstal](#)

[Heling van computergegevens](#)

[Mag politie aangifte van ransomware weigeren?](#)

[Organisatie luidt noodklok over malware-video's op YouTube](#)

[Hoe veilig is internetbankieren?](#)

[Valse Windows 10-upgrade bevat cryptovirus](#)

[Malware opsporen in opstartitems en processen](#)

[Zo voorkom en verwijder je virussen op Android met AVG](#)

[Cyberspionagegroep Morpho nooit weggeweest](#)

[Google: politieagent van het internet?](#)

[Continu emails checken slecht voor werk](#)

[Medisch dossier voor cybercrimineel interessant](#)

[Schatkist](#)

[Snapshots](#)

[Cops in Cyberspace](#)

[Handig](#)

[Wetsartikelen](#)

Miljoenen mensen over de hele wereld bewegen zich tegenwoordig (ook) in een virtuele wereld. Een virtuele wereld is een 'plaats' op internet waar mensen samen kunnen komen.



Virtuele diefstal

Voorbeelden zijn World of Warcraft, waar spelers missies moeten volbrengen en hun karakter moeten ontwikkelen, en Habbo Hotel waarin vooral jongeren elkaar kunnen ontmoeten en een eigen hotelkamer kunnen inrichten.

In veel van die werelden kan met echt geld virtueel geld of virtuele spullen worden aangeschaft, zoals Dragon Coins in het spelletje Dragon Fable, virtuele meubels in Habbo Hotel of maskers en amuletten in het spel Runescape. De diefstal van dergelijke virtuele objecten is strafbaar.

Bij virtuele diefstal is gewoon sprake van diefstal, strafbaar gesteld in [artikel 310 Sr](#).

Indien de verdachte zich toegang heeft verschaft tot het account van het slachtoffer door het onbevoegd gebruiken van diens wachtwoord, is er sprake van een bijzondere vorm van diefstal, namelijk diefstal waarbij de schuldige het weg te nemen goed onder zijn bereik heeft gebracht middels een valse sleutel. (onbevoegd gebruik van wachtwoord is valse sleutel) Hierop staat op grond van [artikel 311 lid 1 onder 5 Sr](#) een zwaardere straf dan 'eenvoudige' diefstal.

Strafbaarstelling voorbereidingshandelingen

Om virtuele diefstal te kunnen plegen heeft iemand zich zonder toestemming toegang moeten verschaffen tot het account van het slachtoffer. In dat geval is in ieder geval sprake van hacken. Dit is strafbaar gesteld in artikel 138ab Sr. Ook voorbereidingshandelingen voor hacken zijn strafbaar.

Bewijsmiddelen

Indien er sprake is van een complexe zaak, neem dan contact op met een digitaal expert uit je eenheid. Daarnaast kan de aangever in ieder geval proberen de volgende informatie aan te leveren:

Gebruikersnaam (bijvoorbeeld de Habbo Hotel-accountnaam).

Datum/tijdstip laatste keer waarop virtuele goederen zichtbaar aanwezig waren.

Datum/tijdstip eerste keer waarop virtuele goederen niet meer zichtbaar aanwezig waren.

Welke virtuele goederen zijn onvreemd (globaal) en wat was de geschatte vertegenwoordigde waarde van deze virtuele goederen?

Welke internetpagina's zijn bezocht rondom de periode dat de virtuele goederen voor de laatste keer zichtbaar waren? Kijk bijvoorbeeld in de internetgeschiedenis.

Is het slachtoffer geadviseerd/gevraagd om naar een bepaalde internetpagina te surfen of een programma te downloaden? Zo ja,

Welke internetpagina's/programma's waren dat?

Door wie werd dit geadviseerd/gevraagd?

IP-adres waar normaliter vandaan wordt ingelogd om in de virtuele wereld te gaan spelen. Dit IP-adres is op te vragen door vanaf de computer van de aangever te surfen naar het webadres www.watismijnip.nl (eventueel later aanvullen, daar aangever dit mogelijk thuis nog moet uitzoeken).

Wat betreft het vastleggen van digitaal bewijs, is het van belang om, indien de dader en het slachtoffer met elkaar gecommuniceerd hebben, zoveel mogelijk van de communicatie vast te leggen. De veelvoorkomende manieren van communicatie via internet/ict zijn:

Chatten

E-mailen

Forums

Sms

VoIP (internetbellen)

Skypen

Zie www.internetsporen.nl voor het vastleggen van sporen. Het kan ook zijn dat de dader een website heeft, of dat er informatie over de dader op een website staat. Leg ook deze informatie vast.



Heling is het verwerven, voorhanden hebben of overdragen van een goed dat verkregen is door een misdrijf, dan wel het vestigen of overdragen van een persoonlijk recht ten aanzien van een dergelijk goed, terwijl de dader weet of redelijkerwijs moet vermoeden dat het om een door misdrijf verkregen goed gaat.



Heling van computergegevens (139e Sr)

Iemand die via een verkoopsite een product koopt voor een onrealistisch lage prijs kan zich – afhankelijk van de omstandigheden - bijvoorbeeld schuldig maken aan opzet- of schuldheling.

[Art. 416 Sr](#) stelt opzetheling strafbaar. In dit geval wist de dader dat het om een door misdrijf verkregen goed ging. [Art. 417bis Sr](#) stelt schuldheling strafbaar. De dader moet in dit geval redelijkerwijs hebben vermoed dat het om een door misdrijf verkregen goed ging. Ten slotte stelt art. 417 Sr. gewoonteheling strafbaar. In dat geval heeft de dader een gewoonte gemaakt van het plegen van opzetheling. Naast de helingsbepalingen kunnen ook de witwasbepalingen van toepassing zijn. Witwassen is strafbaar gesteld in art. 417bis Sr, schuldwitwassen in [art. 420quater Sr](#) en gewoontewitwassen in [art. 420ter Sr](#).

Heling van (computer)gegevens
De toepassing van de helings- en witwasbepalingen bij de online heling van goederen verschilt in beginsel niet van de toepassing bij offline heling. Indien sprake is van de heling van (computer)gegevens kunnen zich echter problemen voordoen.

De helingsbepalingen hebben namelijk alleen betrekking op door misdrijf verkregen 'goederen', de witwasbepalingen op uit misdrijf afkomstige 'voorwerpen'. In het geval sprake is van de heling van een door misdrijf verkregen gegevensdrager, zoals bijvoorbeeld een cd-rom of de harde schijf van een computer, is er niets aan de hand. Een gegevensdrager vormt zowel een goed in de zin van de helingsbepalingen als een voorwerp in de zin van de witwasbepalingen. Indien echter sprake is van de heling

van door misdrijf verkregen 'losse' computergegevens, zijn de helings- en witwasbepalingen niet van toepassing. Je kan hierbij bijvoorbeeld denken aan de publicatie van – tijdens de hack van een computer gestolen – digitale foto's. (Computer)gegevens kunnen namelijk niet als goed of voorwerp aangemerkt worden.

Indien sprake is van de heling van (computer)gegevens is soms wel sprake van strafbaarheid op grond van [art. 139e Sr](#), [art. 273 Sr](#), [art. 273d Sr](#) of [art. 273e Sr](#).

Art. 139e kan van toepassing zijn bij de heling van zowel gegevens als gegevensdragers. Art. 139e Sr stelt enkele gedragingen strafbaar met betrekking tot gegevens waarvan de dader weet of redelijkerwijs moet vermoeden dat die door wederrechtelijk afluisteren, aftappen of opnemen zijn verkregen. Op de eerste plaats is het strafbaar om de beschikking te hebben over een voorwerp waarop dergelijke gegevens zijn vastgelegd (een gegevensdrager), of om een zodanig voorwerp opzettelijk ter beschikking te stellen van een ander (art. 139e onder 1^o en 3^o Sr). Onder laatstgenoemde gedraging wordt ook het aan een ander mededelen van de inhoud van het voorwerp begrepen. Op de tweede plaats is het strafbaar dergelijke gegevens opzettelijk aan een ander bekend te maken (art. 139e onder 2^o Sr). Hieronder wordt ook het ongericht openbaar maken begrepen. De strafbaarstelling is op twee belangrijke punten begrensd. Op de eerste plaats beperkt zij zich tot gegevens die afkomstig zijn uit bepaalde misdrijven (de gegevens moeten verkregen zijn door wederrechtelijk afluisteren, aftappen of opnemen). Op de tweede plaats

beperkt zij zich tot bepaalde handelingen (de beschikking hebben over een voorwerp met dergelijke gegevens of het opzettelijk ter beschikking stellen daarvan van een ander; het opzettelijk bekendmaken van dergelijke gegevens)

In het wetsvoorstel Computercriminaliteit III wordt het helen van computergegevens afzonderlijk strafbaar gesteld in het nieuw op te nemen artikel 139f Sr. In dit artikel wordt strafbaar gesteld degene die niet-openbare gegevens verwerft, voorhanden heeft, ter beschikking van een ander stelt, aan een ander bekend maakt of uit winstbejag voorhanden heeft of gebruikt, terwijl hij wist of redelijkerwijs had moeten vermoeden dat deze gegevens door misdrijf zijn verkregen. Niet strafbaar is degene die te goeder trouw heeft kunnen aannemen dat het algemeen belang belangbekendmaking van de gegevens vereiste.*

Strafbare vervolghandelingen
[Art. 273 lid 1 onder 2^o Sr](#) stelt een bijzondere vorm van heling strafbaar: het opzettelijk bekendmaken of uit winstbejag gebruiken van gegevens die door misdrijf zijn verkregen uit een geautomatiseerd werk van een onderneming van handel, nijverheid of dienstverlening en die betrekking hebben op deze onderneming. Er is alleen sprake van strafbaarheid indien de gegevens ten tijde van de bekendmaking of het gebruik niet algemeen bekend waren, en uit de bekendmaking of het gebruik enig nadeel kan ontstaan.

Op grond van art. 273 lid 2 is strafbaarheid uitgesloten indien de dader te goeder trouw heeft kunnen aannemen dat het algemeen belang de bekendmaking vereiste. Bovendien is op grond van art. 273

lid 3 sprake van een klachtdelict: geen vervolging heeft plaats dan op klacht van het bestuur van de onderneming.

Bijzondere strafbaarstelling
[Art. 273d Sr](#) en [art. 273e Sr](#) zijn kwaliteitsdelicten: zij zijn alleen gericht op personen die werkzaam zijn bij een aanbieder van een telecommunicatienetwerk of -dienst (art. 273d lid 1 en lid 2 Sr). Het kan hierbij zowel om openbare als om niet-openbare netwerken en diensten gaan. Bij een niet-openbaar netwerk kan bijvoorbeeld aan een bedrijfsnetwerk gedacht worden. Internet Service Providers bieden doorgaans openbare netwerken en diensten aan. Een dergelijke persoon is strafbaar indien:

hij de beschikking heeft over een voorwerp waaraan, naar hij weet of redelijkerwijs moet vermoeden, een gegeven kan worden ontleend dat verkregen is door wederrechtelijk overnemen, aftappen of opnemen van gegevens die door tussenkomst van het betreffende netwerk of de betreffende dienst zijn opgeslagen, worden verwerkt of overgedragen ([art. 273d lid 1 onder b.](#));

hij opzettelijk en wederrechtelijk de inhoud van zodanige gegevens aan een ander bekendmaakt (art. 273d lid 1 onder c.);

hij opzettelijk en wederrechtelijk een voorwerp waaraan een gegeven omtrent de inhoud van zodanige gegevens kan worden ontleend, ter beschikking stelt van een ander (art. 273d lid 1 onder d.);

hij opzettelijk toelaat dat een ander een van de drie hierboven genoemde feiten pleegt, of die ander daarbij als medeplechtige terzijde staat (art. 273e Sr).

Onlangs werd de computer van een kennis overgenomen door ransomware, wat een strafbaar feit is. Daar wilde ik bij de politie vervolgens aangifte van doen, maar de agent aan de balie wilde de aangifte niet opnemen. Is de politie niet verplicht om ook aangiftes van ransomware op te nemen?

Mag politie aangifte van ransomware weigeren?

Door Arnoud Engelfriet ICT jurist

Software zoals [Cryptolocker](#) wordt wel ransomware ("gijzelsoftware") genoemd. Dergelijke software wist geen gegevens maar versleutelt ze, zodat ze onbruikbaar zijn totdat de juiste sleutel wordt ingevoerd. De verspreider van deze software geeft de sleutel pas af nadat de eigenaar van de gegevens heeft betaald. Dit is strafbaar (art. 350a lid 1 Strafrecht), met maximaal 2 jaar cel.

Van strafbare feiten kun je aangifte doen. De politie is verplicht deze op te nemen ([art. 163 lid 6 Strafvordering](#)): "Tot het ontvangen van de aangiften bedoeld in de artikelen 160 en 161, zijn de opsporingsambtenaren, en tot het ontvangen van de aangiften bedoeld in artikel 162, de daarbij genoemde ambtenaren verplicht."

In de praktijk wordt het opnemen van aangiftes rond computercriminaliteit nogal eens geweigerd. De reden hiervoor lijkt te zijn dat men direct vermoedt dat de pakkans nul is, bij ransomware geen gekke gedachte. En waarom tijd verspillen aan een volstrekt kansloze aangifte?

Wie voet bij stuk houdt, kan het vaak wel voor elkaar krijgen dat de aangifte wordt opgenomen. De kans is alleen erg groot dat deze vervolgens direct wordt geseponeerd, oftewel terzijde gelegd en verder geen actie.

Wordt een aangifte geseponeerd, dan kun je in theorie via het gerechtshof ([een artikel 12-procedure](#)) afdwingen dat het OM er alsnog naar kijkt. Maar als er wordt geseponeerd wegens gebrek aan aanknopingspunten of bewijs, dan is de kans natuurlijk klein dat dat alsnog een heel succesvolle procedure wordt.

De praktijk leert mij dat het eigenlijk geen zin heeft om die kant op te gaan. Je kunt zelf vaak ook al redelijk aanvoelen dat opsporing hem niet gaat worden, en in dat geval zal de politie er ook weinig zin in hebben. Ik zou willen dat het anders was, maar ja.



De Amerikaanse organisatie Digital Citizens Alliance heeft de noodklok geluid over Remote Access Trojans (RATs) en het feit dat talloze instructievideo's voor het gebruik van dit soort malware op YouTube zijn te vinden. Iets waar zowel de makers als Google uiteindelijk van profiteren.

Organisatie luidt noodklok over malware-video's op YouTube

[Remote Access Trojans](#) bestaan al vele jaren en geven een aanvaller volledige controle over de computer van het slachtoffer. Om de RAT bij een slachtoffer te installeren wordt in veel gevallen gebruik gemaakt van social engineering, waarbij het slachtoffer wordt verleid om een bestand te openen en zo zijn eigen computer te infecteren. Het gaat dan bijvoorbeeld om e-mailbijlagen of bestanden die via Skype of social media worden uitgewisseld. Zodra het slachtoffer het bestand opent kan de aanvaller bijvoorbeeld met de webcam meekijken of toetsaanslagen opslaan.

Handel

Op internet zijn verschillende fora te vinden waarop computers die met een RAT zijn besmet worden verhandeld, of waar beelden zijn te zien van slachtoffers die via hun eigen webcam stiekem zijn gefilmd. Een praktijk waar al in 2008 voor werd gewaarschuwd. Software voor het maken van een RAT is eenvoudig via internet te vinden. Daarnaast staan er op YouTube tal van instructievideo's, aldus de [Digital Citizens Alliance](#). Video's waarmee zowel de makers als Google geld verdienen, omdat Google advertenties bij de video's toont. "Geen enkel bedrijf, met name één zo groot als Google, zou geen cent moeten verdienen aan video's die de gezichten van slachtoffers en hun IP-adressen laten zien", aldus de organisatie. Als het aan de Digital Citizens Alliance ligt worden YouTube-video's voortaan dan ook handmatig gecontroleerd.

Menselijke aard

Om de oproep kracht bij te zetten werd er een lijvig rapport over Remote Access Trojans gepubliceerd. Daarin wordt vooral de schijn gewekt dat consumenten niets tegen dit soort malware kunnen doen, in plaats van zich te richten op het voorkomen van een infectie via een RAT, namelijk door geen ongevraagde bijlagen, bestanden of links te openen.

Zo komt er een beveiligingsexpert aan het woord die juist stelt dat mensen er niets aan kunnen doen als ze besmet raken. "Links zijn bedoeld om te worden geopend. Veel mensen klikken op honderden links per week", aldus Megan Horner van [Blackfin Security](#). "Het gaat tegen de menselijke aard in. Het is lastig om niet doen, zelfs als je iets ziet waarmee je zou moeten wachten." In de conclusie van het rapport wordt echter in het kort opgeroepen tot bewustwordingscampagnes. Daarnaast wil de Digital Citizens Alliance dat opsporingsdiensten meer middelen krijgen om dit soort misdrijven aan te pakken en zouden "hackers" die de privacy van hun slachtoffers schenden moeten worden gestraft.

(klik op het oog voor meer.....)



Je kan overal waar je wil je geld beheren en uitgeven. Tenzij misschien op plaatsen waar er amper internet is. Hoe zit het tegenwoordig met de veiligheid van dat mobiel bankieren?

Hoe veilig is internetbankieren?

Niet iedereen is blij met de fantastische dienstverlening die internetbankieren heet. Onlangs nog verklaarde een van mijn burens (een man van rond de 30) dat hij nog liever door de regen met de fiets naar de bank in het centrum rijdt, dan dat hij online moet bankieren. De eerlijkheid gebiedt me wel om te zeggen dat die anekdote diende om een verhaal over hoe hard hij computers haat te illustreren, en niet zozeer over hoe hard hij internetbankieren haat. Toegegeven: ik vind internetbankieren ook vooral leuk om te kijken hoeveel geld er op mijn rekening staat, en minder om rekeningen te betalen. Maar ik betaal gewoon niet graag rekeningen.

Dat nakijken hoeveel geld je nog (of niet meer) hebt, kan tegenwoordig ook eender waar. Zowat alle banken hebben een degelijke app, waarmee je (bijna) alles kan doen wat je op je computer kan doen. In de meeste gevallen beperkt dat zich vooral tot het nakijken van je saldo, want om transacties te doen heb je vaak nog je kaartlezer nodig. Dat is vervelend als je op de trein even snel wat geld wilt overschrijven, maar het zorgt ook voor een stevige beveiliging. Hoe mobieler internetbankieren wordt, hoe belangrijker immers de beveiliging.

Two-factor authentication



Enkele jaren geleden kon ik nog overal op internet aankopen doen met mijn kredietkaart, zonder dat ik me op een of andere manier moest legitimeren. Dat was ontzettend handig en goed

(of slecht, afhankelijk van hoe je het bekijkt) om impulsaankopen te doen. Op een gegeven moment moest ik op steeds meer websites mijn identiteit bevestigen door mijn kredietkaart in het 'kaske' van de bank te steken en een procedure met codes te volgen.

In het begin was dat erg frustrerend, want je

hebt niet zomaar altijd die kaartlezer bij de hand. Maar gaandeweg raakte ik aan dat extra stukje veiligheid gewend, en tegenwoordig zal je niet snel nog een site vinden waar je zomaar kan betalen door enkel en alleen je kredietkaartgegevens in te voeren.

Je zal zo goed als altijd te maken krijgen met wat men two-factor authentication noemt, of een tweeledige verificatiemethode: je hebt je inloggegevens voor je mobiele bankaccount nodig, en daarnaast nog een extra stukje hardware. Enkel met die combinatie kan je dan aan je rekeningen, wat het voor mensen van slechte wil een pak moeilijker maakt om ze te plunderen. Bij de ene bank heb je je bankkaart en een kaartlezer nodig, terwijl de andere bank bijvoorbeeld een sms naar je gsm-nummer stuurt.

Met of zonder vinger

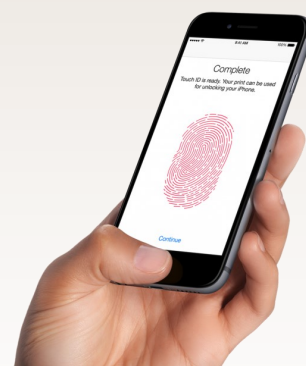
In november vorig jaar voerde ING als eerste bank in België [biometrie](#) toe aan die vergelijking. Biometrie betekent dat er biologische eigenschappen gebruikt worden om een gebruiker te herkennen. Dat kan stemherkenning zijn, een oogscanner, of – zoals in dit geval – een vingerafdruks scanner. Wie een iPhone met zo'n vingerafdruks scanner heeft (de 5S, 6 of 6 Plus) kan met dus zijn vinger inloggen in de app van ING, in plaats van een pincode te moeten intikken. Zo ben je zeker dat jij en jij alleen in de app kan. Tenzij iemand je vinger steelt. In dat geval ben je natuurlijk slechter af dan wanneer iemand enkel je pincode nodig heeft.

Met de lancering van de iPhone 5S en zijn vingerafdruks scanner kwam er trouwens een hele discussie op gang over de veiligheid van biometrisch inloggen. Is het nu een veel betere of veel slechtere beveiliging? Het is erg veilig in die zin dat jouw vingerafdruk uniek is, en moeilijk om na te maken. Een pincode kan je raden, een vingerafdruk niet. Aan de andere kant kan het frustraties meebrengen als je vinger niet met-

een herkend wordt, als je bijvoorbeeld net een vettige pizza gegeten hebt of vergeten bent dat

je handschoenen aan hebt. En, belangrijker: een pincode kan je veranderen, een vingerafdruk niet.

Om je vingerafdruk te herkennen, moet die in een of andere vorm opge-



slagen worden op het toestel waarmee je hem gebruikt. Dat betekent per definitie dat die gegevens ook gestolen kunnen worden. En zodra iemand jouw vingerafdruk in zijn bezit heeft, kan hij meteen ook inloggen op andere toestellen waar je je vinger gebruikt als beveiliging. Je kan wel snel van pincode veranderen, maar niet zo snel van vingerafdruk. De beveiliging van je vingerafdrukgegevens is dus cruciaal. Is dit alles een reden om geen biometrische veiligheid te gebruiken? Nee. Banken zullen biometrie pas gebruiken als ze zelf zeker genoeg zijn dat de beveiliging sterk genoeg is, en het zal altijd moeilijker blijven om dat soort gegevens te stelen dan om de geboortedatum van je kat te raden.



Extra veiligheidsmaatregelen

De meeste apps om online te bankieren bevatten trouwens meer veiligheidsmaatregelen dan je op het eerste zicht zou denken. Zo kunnen ze gebruik maken van de gps-module in je smartphone, om na te gaan of je je op een "logische" plaats bevindt wanneer je mobiel je geld wil beheren. Check je meestal je saldo in de trein tussen Mechelen en Brussel (al is die kans klein aangezien je op de trein zelden een stabiele mobiele verbinding hebt), dan zal de app achterdochtig worden als je ineens vanuit hartje Rusland je rekeningen willen bekijken.

Natuurlijk kan je zelf ook veel doen aan de veiligheid van je bankierapp(s), net zoals dat met online bankieren in je browser het geval is. Zorg bijvoorbeeld dat je jezelf uitlogt wanneer je klaar bent met de app. De meeste apps zullen dat ook in jouw plaats doen, maar dikwijls duurt dat wel een paar minuten. Als je telefoon net dan gestolen wordt, hebben de dieven toegang tot jouw rekening. Een ramp is dat meestal niet, dankzij die two-factor authentication waar ik het eerder over had. Zolang de dieven jouw code, kaart en kaartlezer of vinger(afdruk) niet hebben, zullen ze weinig kunnen uitvoeren.

Checken op de [smartwatch](#)



Wie tegenwoordig helemaal hip wil zijn, checkt zijn saldo trouwens niet meer op zijn smartphone maar op zijn horloge. Dat voorrecht is voorlopig nog voorbehouden voor Belfius-klanten die de Belfius Direct Mobile app

draaien op een smartphone met Android 4.3 of hoger, en een Android Wear-smartwatch hebben. Denk bijvoorbeeld aan de Motorola Moto 360, de Samsung Gear Live of de LG G Watch.

Wereldschokkende dingen moet je er niet van verwachten: je krijgt enkel een zogenaamde saldometer te zien, een balkje dat van rood naar groen gaat en een driehoekje dat aangeeft waar op het balkje je huidige saldo zich bevindt. De app werkt dan ook alleen als je eerst een minimum- en een maximum-bedrag hebt ingesteld. Cijfers toont de app niet, om de discretie te waarborgen. Een leuke gimmick, maar niet meer dan dat. Toch verwacht ik dat de combinatie van verschillende toestellen in de toekomst een rol zal spelen in de nooit aflatende beveiligingsrevolutie.

Betalen zonder kaart

Een leuk voorbeeld is [de app van Bancontact](#), waarmee je makkelijk geld kan uitwisselen met vrienden, familie of totale onbekenden. Je moet een keer een bankkaart activeren in de app met je

kaartlezer, en daarna kan je de app gebruiken. De interface is erg eenvoudig: je moet aangeven of je geld wil ontvangen, of moet betalen. In het eerste geval moet je aangeven om hoeveel geld het gaat en kan je eventueel een boodschap toevoegen.

Onderaan zie je steeds door welke bank de transactie zal uitgevoerd worden. Daarna genereert de app een QR-code. Moet je betalen, dan opent de app een QR-scanner waarmee je de code van de ontvanger moet scannen. Je krijgt dan de details van de transactie te zien en kan kiezen om te betalen. Een fluitje van een cent en bijna onmogelijk te vervalsen, want de code wordt ter plekke gegenereerd en moet je ook ter plekke inscannen. Het enige risico is dat je vriend een malafide app heeft geïnstalleerd om de code te genereren, maar de kans dat zo'n vervalsing tot in de officiële App Store of Google Play Store geraakt, is klein.

Sommige banken willen de app van Bancontact integreren in hun eigen app, maar op dit moment zijn we zover nog niet.

Phishing en co

Een gewaarschuwd man is er twee waard.

En daarmee zijn we, alle technologische vernieuwing ten spijt, aanbeland bij wat nog steeds een van de grootste veiligheidslekken van online bankieren is: phishing. Als trouwe lezer van Clickx



herken je zo'n vals aas ongetwijfeld van ver, maar ik heb het afgelopen jaar toch enkele héél overtuigende phishingmails zien binnenrollen. Het gebrekkige taalgebruik blijft in de die gevallen achterwege en de mails zien er ook heel echt uit. De twee belangrijkste weggevers zijn het e-mailadres van de afzender, en de website waar je naartoe gestuurd wordt. Een mailadres kan nog vervalst worden, een url niet.

De echte url van jouw bank is normaal gezien <https://www.denaamvanjouwbank.be> (let op de https in plaats van http), een valse url zal er dikwijls uitzien als <http://ietswillekeurigs.com/denaamvanjouwbank.be> of zelfs gewoon helemaal nonsens zijn. Ben je toch op de site belandt,

klik dan eens op andere links in het menu.

Phishers doen zelden de moeite om de hele website na te maken, en dan zie je al snel waar je belandt. In de adresbalk van je browser moet een slot-icoontje verschijnen. Klik daarop om het veiligheidscertificaat na te kijken, daar moet altijd de juiste url van je bank getoond worden met de melding dat de identiteit geverifieerd is.

Daarnaast zijn er nog een aantal makkelijke tips voor de wat meer goedgelovige mensen in je familie of vriendenkring: je bank zal nooit ofte nimmer naar persoonlijke gegevens vragen in een mail, of het nu gaat om je adres, geboortedatum of kredietkaartnummer. Ben je toch al dieper in het proces beland en vraagt de website om in te loggen met je kaartlezer, dan is het goed om te weten dat je enkel kan inloggen met de M1-knop van die kaartlezer. Om een transactie te verrichten moet je de M2-knop gebruiken. Vraagt de site dus om in te loggen door op M2 te drukken en een code in te geven, dan weet je dat er iets niet pluis is.



Ben je nog steeds ongeduldig aan het wachten op je Windows 10-upgrade? Laat je niet verleiden door e-mails met gratis Windows 10-software.

Valse Windows 10-upgrade bevat cryptovirus

Cybercriminelen proberen voordeel te halen uit de uitrol van Windows 10. Er zijn namelijk verschillende e-mails in de omloop waarin de ontvanger wordt aangemoedigd naar Windows 10 te upgraden met de bijgevoegde software. Velen zijn nog steeds ongeduldig aan het wachten op hun Windows 10-upgrade en zijn daarom geneigd de software via deze weg te downloaden.

Vanaf het moment dat je [de executabel](#) uitvoert sluit de val zich echter. Al je bestanden worden geëncrypteerd en op je bureaublad verschijnt een waarschuwingsbericht met timer. Indien je niet binnen de 96 uur

Windows 10 is familiar and easy to use. It includes an improved Start menu and is designed to startup and resume fast. Plus, it's packed with new innovations including Microsoft Edge, an all-new browser. Your personal files and apps you've installed will all be waiting for you. We've designed the upgrade to be easy and compatible with the hardware and software you already use.

Don't miss out as this free offer won't last forever. Upgrade today. Follow the attached installer and get started.

“Upgrading from Windows 7 or Windows 8? You will love Windows 10!”

betaalt aan de cybercrimineel zal al je data verloren zijn. In het verleden is echter al gebleken dat zelfs na het betalen van losgeld je bestanden voorgoed versleuteld zijn.

Hoe herken je de frauduleuze e-mail?

In de eerste plaats hoort er al een belletje te gaan rinkelen wanneer de Windows 10-upgrade via mail wordt aangeboden. De upgrade wordt namelijk door Microsoft automatisch uitgerold via Windows Updates. Voor wie nog steeds zit te wachten op de upgrade en geen geduld meer heeft, staan er enkele trucjes te lezen in dit artikel.

Cybercriminelen proberen je vertrouwen te winnen door de afzender van de e-mail 'update@microsoft.com' te maken. Wanneer je echter naar de [hoofding van de mail](#) kijkt, kan je zien dat het IP-adres van de afzender van Thailand afkomstig is.

Het kleurenschema van de mail is bewust soortgelijk gekozen aan het kleurenschema van Windows 10. De achtergrond heeft namelijk de typische blauw kleur die we kennen van Windows 10.

In de tekst van de e-mail staat te lezen waarom we voor Windows 10 moeten kiezen. Dit lijkt opnieuw erg hard op de manier waarop Microsoft reclame maakt voor zijn nieuwste operating system. In de tekst, welke overigens in het Engels is, zijn er echter verschillende karakters foutief weergegeven. Dit wijst erop dat de karakterset waarin de mail is getypt niet overeen komt met jouw karakterset, een typisch probleem voor exotische talen.

Onderaan staat er dezelfde disclaimer te lezen die ook onder officiële e-mails van Microsoft zou staan. In deze tekst zijn er echter wederom enkele karakters foutief weergegeven.

Als laatste probeert men je nog eens extra te overtuigen dat de inhoud van de e-mail veilig is door onderaan te schrijven dat de inhoud gescand is door een antivirusscanner. Volgens deze tekst zouden er geen virussen zijn gevonden. In het bericht wordt gelinkt naar een bestaande open-source e-mailfilter, waardoor veel mensen in de val trappen.



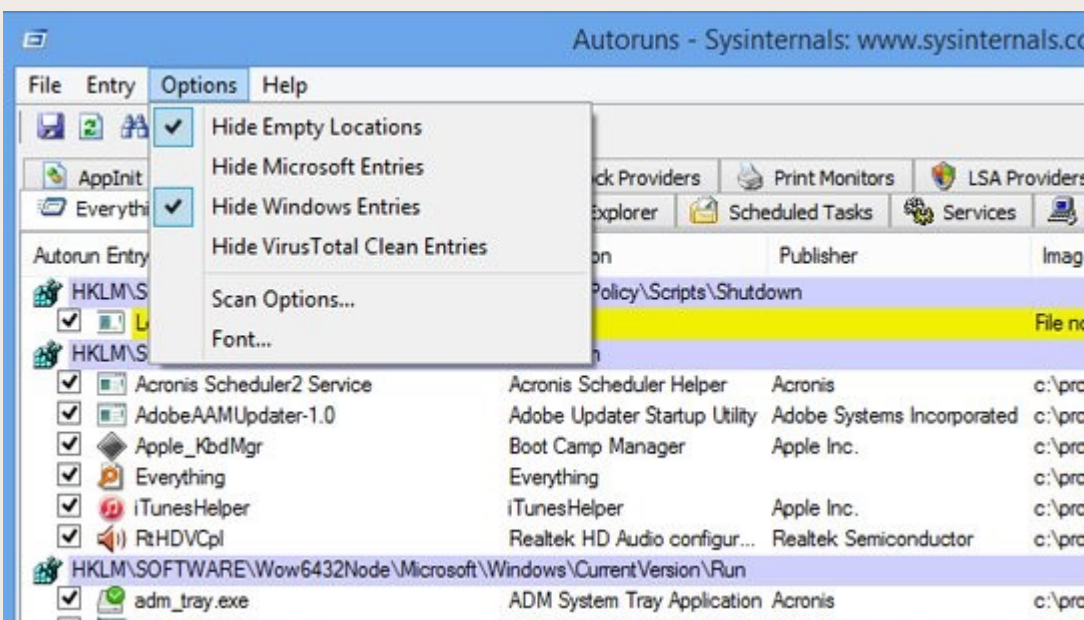
Bij het opstarten van je pc worden op de achtergrond heel wat items mee in gang gezwaaid. Met Process Explorer en Autoruns scan je al die items pijlsnel op malware.

Malware opsporen in opstartitems en processen

Onder de noemer [Sysinternals](#) vind je een aantal handige systeem- en diagnosetools voor Windows. Hoewel ze voornamelijk bedoeld zijn voor professionals en programmeurs, kan je er als thuisgebruiker ook tot op zekere hoogte je voordeel mee doen. Twee van die tools zijn Process Explorer en Autoruns. Samen kan je ze zien als een uitgebreide versie van het taakbeheer in Windows. Net als Process Explorer kreeg Autoruns onlangs een extra functie: de bekende [online virusscanner Virus Total](#), die je bestanden door de motoren van meer dan 50 verschillende scanners jaagt.

Je kan Autoruns [hier downloaden](#). Het is een zip-bestand dat je naar een-der welke map kan uitpakken. Dubbelklik op autoruns.exe om het programma te starten. Je kan ook autorunsc.exe gebruiken, dat is de zogenaamde command line interface. Het DOS-venster, zeg maar. Daar doe ik niet aan mee. De eerste keer dat je Autoruns start moet je de gebruiksvoorwaarden accepteren met een druk op 'Agree'. Daarna komt er een interface te zien met een hele hoop tabbladen. Het geopende tabblad wordt meteen gevuld met alle informatie die het programma tijdens het scannen van je systeem vindt.

In dat tabblad, 'Everything', zie je alle opstartitems staan. Dat zijn niet alleen de programma's die samen met je computer opgestart worden, maar ook alle registeritems die ingeladen worden. Alle items die met Windows zelf te maken hebben, worden verborgen. Wil je die ook tonen, dan klik je in de menubalk bovenaan op 'Options' en vervolgens verwijder je het vinkje bij 'Hide Windows Entries'. Wil je integendeel ook alle items van Microsoft verbergen, dan ga je via 'Options' naar 'Hide Microsoft Entries'.



Sommige items zijn geel gemarkeerd, die bestanden werden niet gevonden. Je kan ze uit het autorunsysteem halen door er met je rechtermuisknop op te klikken en 'Delete' te kiezen. Dat zal niet altijd lukken, zelfs niet als je de actie herhaalt als administrator. Maar echt belangrijk is dat ook niet. Het belangrijkste is dat je alle items door VirusTotal kan laten

scannen, zodat je in een oogopslag ziet of er verdachte dingen gebeuren tijdens het opstarten van je computer. Dat doe je door bij 'Options' op 'Scan Options' te klikken en vervolgens een vinkje te zetten bij 'Check VirusTotal.com' en 'Submit Unknown Images' en op 'Rescan' te drukken.

De eerste keer dat je zo'n scan wil starten, moet je de gebruiksvoorwaarden van VirusTotal accepteren. Die gebruiksvoorwaarden worden geopend in je browser, maar je kan in het programma gewoon op 'Ja' drukken. In Autoruns zie je in de kolom VirusTotal nu overall Hash submitted staan. Dat betekent dat het bestand door VirusTotal gecontroleerd wordt. Na een tijdje verandert die tekst in een link met cijfers als 0/57. Dat betekent dat van de 57 gebruikte malware- en virusscanners er geen enkele een probleem heeft gevonden. Staat er iets anders dan 0/57, dan zal de link rood kleuren om aan te geven dat sommige scanners wél een probleem hebben gevonden. Door op de link te klikken, zie je welke scanners een probleem vonden en wat dat probleem is. Op basis daarvan kan je dan zelf inschatten of het echt om een probleembestand gaat of niet. Sommige gratis tools waarmee je bijvoorbeeld netwerken kan afspeuren worden ook als schadelijk aanzien, omdat je er ook malafide dingen mee kan doen. Als dat soort false positives bekend zijn, zal de fabrikant dat op zijn website normaal gezien wel vermelden.

Process Explorer kan je [hier downloaden](#). Het is eveneens een zip-bestand dat je eender waar kan uitpakken. Je start het programma met een dubbelklik op procexp.exe. Process Explorer ziet er zo mogelijk nog ingewikkelder uit dan Autoruns. Je krijgt een overzicht van alle lopende processen, maar uitleggen waar alles voor staat zou ons veel te ver leiden. Voor een leek als mezelf is het handigste onderdeel het vakje boven-

aan met de bewegende groene lijn. Die geeft aan hoe hard de processor aan het werk is. Hoe lager het lijntje staat, hoe minder werk hij heeft. Staat het lijntje continu te pieken, dan loopt je processor tegen zijn limieten aan en zal je computer wellicht traag reageren. Door op het vakje te klikken krijg je een detailweergave te zien. Hetzelfde vakje zie je ook in het systeemvak van Windows.

Net zoals Autoruns heeft ook Process Explorer VirusTotal geïntegreerd. Je kan alle processen laten scannen via Options, VirusTotal.com, Check VirusTotal.com. In de kolom VirusTotal verschijnen na een tijdje dan weer (hopelijk) de meldingen à la 0/57. Elke keer je Process Explorer of Autoruns opnieuw opstart, zullen ze alle bestanden opnieuw laten controleren door VirusTotal.

Zo kan je af en toe snel nog eens controleren of alles nog in orde is. Je kan uiteraard ook losse bestanden door VirusTotal laten scannen. Daarvoor surf je naar [www.virustotal.com](#), waar je een bestand kan uploaden of een url kan invullen om die te laten controleren.

Als je applicaties buiten de Play Store van Google om installeert, kan het voorkomen dat je Android-toestel besmet raakt met malware. Wil je toch veilig zijn buiten de applicatiewinkel van Google, dan kan Antivirus Gratis van AVG je helpen je toestel schoon te houden.

Zo voorkom en verwijder je virussen op Android met AVG

Installeer je eigenlijk alleen apps uit de Google Play-applicatiewinkel, dan heb je weinig aan antivirusapplicaties. Google scant de applicatiewinkel zelf op malware. Een kritische blik op de machtigingen die apps vragen is voldoende, een antivirus-app is alleen maar zonde van je systeemcapaciteit. Installeer je echter zelf apps uit apk-bestanden die je van internet downloadt, dan heb je de bescherming uit de Play Store niet meer en is het risico op malwarebesmetting veel groter.

Na het installeren van [AntiVirus Gratis](#) van AVG wordt gevraagd om een scan uit te voeren. De app gaat direct op zoek naar besmette programma's en apps die op je Android-apparaat geïnstalleerd staan. Je bestanden, instellingen, postvakjes en apps worden gecontroleerd op mogelijke virussen en malware. Het uitvoeren van een scan duurt ongeveer tien minuten, tenzij je hele smartphone volstaat met applicaties.

Verwijderen van troep

Als AntiVirus Gratis van AVG geïnfecteerde programma's vindt, dan krijg je na de scan direct een melding te zien van het aantal besmette programma's. Als je klikt op problemen oplossen dan krijg je een overzicht van de infecties te zien. Klik hier eerste een van de categorieën aan, en klik vervolgens op het geïnfecteerde programma. Je kunt deze dan direct via de AVG virusscanner verwijderen. Als je merkt dat je na het downloaden van een app minder goede prestaties hebt van je smartphone of tablet, dan kun je de scan uitvoeren om problemen op te sporen.

Bonusfuncties

In de app kun je direct aan de icoontjes zien hoe goed je smartphone beveiligd is. Volledig groene cirkels geven aan dat alles perfect is, waarbij oranje een gevarenzone betekent. Bij cirkels die niet af zijn moeten nog gegevens aangevuld worden om je smartphone of tablet optimaal te beveiligen. Je weet dus precies hoe goed je apparaat beveiligd is tegen inbraken en besmette programma's.



Symantec heeft een cyberspionagegroep ontdekt die al sinds maart 2012 actief is in Europa en Noord-Amerika. De groep, die door Symantec Morpho wordt genoemd, leek na 2012 te zijn verdwenen, maar volgens Symantec is de groep nog altijd actief.



Cyberspionagegroep Morpho nooit weggeweest

[Morpho](#) richt zich op het stelen van informatie om deze vervolgens te verkopen. Tot nu toe blijkt de groep 49 organisaties in twintig landen tot slachtoffer te hebben gemaakt. Details over mogelijke aanvallen op Nederlandse bedrijven zijn niet bekend bij Symantec.

Begin 2013 werd de cyberspionagegroep opgemerkt omdat techgiganten zoals Twitter, Facebook, Apple en Microsoft publiek aangaven aangevallen te zijn. De hackersgroep wordt door Symantec Morpho genoemd, maar de groep staat ook onder de namen Wild Neutron en Jripbet bekend. Hoewel de groep pas in 2013 publiciteit kreeg en daarna in de vergetelheid verdween, zijn ze volgens Symantec al sinds maart 2012 actief.

De hackers richten zich specifiek op grote organisaties om informatie te stelen en zijn volgens Symantec een stuk geavanceerder dan de gemiddelde hacker. De manier waarop de hackers te werk gaan is via zogenaamde stepping stones, oftewel door kleinere organisaties aan te vallen en deze infectie vervolgens te gebruiken om Amerikaanse en Europese hoofdkantoren te bereiken.

Voor deze aanvallen gebruikt de groep verschillende, intern ontwikkelde malware tools. Ze zetten voornamelijk twee typen Trojans in: OSX.Pintsize voor Mac OS X computers en Backdoor.Jiripbot voor Windows computers. Daarnaast wordt onder andere de hacking-tool Hacktool.Securetunnel ingezet om een command & control (c&c)-serveradres en -poort door te geven aan een besmette computer.

De hackers richten hun aanvallen binnen de grote organisatie op Microsoft Exchange of Lotus Domino email servers, op enterprise content management systemen en op specialist systemen.

Mogelijk Amerikaanse wortels

De technologiebedrijven die door Morpho zijn aangevallen, zijn voornamelijk gevestigd in Amerika. In Europa zijn voornamelijk grote farmaceutische bedrijven aangevallen door Morpho. Daarnaast denkt Symantec ook dat de hackers zelf in Amerika zijn gevestigd, omdat de c&c-serveractiviteit het hoogst is tijdens de Amerikaanse werktijden. Hoewel dit er ook op kan wijzen dat de meeste slachtoffers in Amerika zijn gevestigd. Daarnaast is de malware in vloeiend Engels gedocumenteerd. Ook zijn de hackers volgens Symantec bekend met de Engelssprekende popcultuur, omdat zij de term AYBABTU (All your base are belong to us) gebruiken als encryptiekey in hun Windows-Trojan.

Verdienmodel Morpho

Symantec heeft een idee van het soort informatie dat is gestolen, zoals financiële gegevens, product beschrijvingen en juridische documenten. Echter wat er precies met deze documenten gebeurt, is niet bekend. Wel meent Symantec dat de hackersgroep geld verdient doordat zij bijvoorbeeld zijn ingehuurd door bedrijven om informatie van andere organisaties te stelen. Ook kunnen de hackers geld verdienen aan de gestolen data door deze te verkopen aan de hoogste bidder. Tot slot kan de informatie gebruikt worden voor interne verhandel-doeleinden.

Maatregelen

Volgens Symantec kunnen organisaties zichzelf het beste tegen deze hackergroepering beschermen door een combinatie van de volgende beveiligingstechnologieën te gebruiken:

Gebruik de bestaande antimalware-oplossing volledig. Hiermee wordt bedoeld dat alle functionaliteiten moeten worden aanzet.

Gebruik nieuwe [Advanced Threat Protection](#) (ATP)-technologieën

Gebruik Cyber Security Services zodanig dat een gespecialiseerd bedrijf je omgeving monitort



Google is niet alleen de populairste zoekmachine, de internetgigant ontpopt zich ook steeds vaker als online politie-agent. Nadat Google eerder al honderdduizenden verzoeken om 'vergeten te worden' behandelde, zet het bedrijf zich nu in om wraakporno te bestrijden.



Google: politieagent van het internet?

Over enkele weken kunnen slachtoffers van 'revenge porn' online een formulier invullen om hun pikante foto's en filmpjes (in ieder geval) uit de zoekresultaten van Google te verwijderen.

Van wraakporno spreken we als iemand na een verbroken relatie pikante opnames online zet van de ex-partner, puur om hem of haar te raken. Google kan niet voorkomen dat beelden online worden gezet, het bedrijf bepaalt immers niet de inhoud van websites, maar het kan wel voorkomen dat de beelden met de zoekmachine makkelijk te vinden zijn. Volgens Google-topman Amit Singhai zijn die foto's en filmpjes 'vernederend en uitsluitend bedoeld om de slachtoffers, vooral vrouwen, te beschadigen'.

De anti-wraakporno-actie van Google is voor zover bekend een initiatief van het bedrijf zelf. Het 'recht om vergeten te worden' werd anderhalf jaar geleden door het Europese Hof opgelegd, overigens niet alleen aan Google, maar aan alle grote zoekmachines. Ook in die kwestie moeten gebruikers die zich gekwetst voelen of ten onrechte gelinkt aan bijvoorbeeld misdrijven een formulier invullen. De eerste resultaten daarvan laten zien dat Google in nog niet in de helft van de gevallen de link ook daadwerkelijk verwijdt. Het laat zich raden dat ook in de wraakporno niet alle verzoeken gehonoreerd zullen worden.

Wraakporno is niet bepaald een kwestie die alleen bij Google speelt: amper een week geleden stond misdaadverslaggever Peter R. de Vries voor de rechter om de firma Facebook te dwingen de gegevens van de internetpester van een 21-jarig meisje te onthullen. Volgens Facebook zijn die gegevens inmiddels gewist, niettemin volgt op 25 juni een uitspraak van de rechter. Die uitspraak kan misschien een belangrijk precedent worden en ook Facebook dwingen iets aan het probleem te doen.

Toch blijft het opvallend: beslissingen over onze privacy en onze gegevens worden blijkbaar niet meer genomen door de instantie die wij daarvoor benoemd hebben, of de regering, maar door wereldwijd opererende concerns en dan ook nog met een zekere willekeur en zonder de plicht zich achteraf te verantwoorden. Een beter bewijs dat internet de wereld voorgoed heeft veranderd lijkt er niet te zijn.



Het probleem is gekend: e-mails zuigen veel van uw dagelijkse werktijd op en zijn enorm afleidend. Er is nu ook een wetenschappelijke verklaring hoe dat precies zit.



Continu emails checken slecht voor werk

E-mails lezen maakt uw hersenen duizelig. Althans, dat is de conclusie van een onderzoek gedaan aan de Canadese McGill Universiteit in Montréal. Het geeft een wetenschappelijke verklaring waarom continu uw e-mails checken funest is voor uw productiviteit.

Tussen positief en negatief

Professors Levitin en Menon, uitvoerders van de studie, stellen dat mensen constant wisselen tussen twee bewustzijnstoestanden: taak-positief (dus geconcentreerd op een opdracht) of taak-negatief (dagdromen of afdwalen). Wanneer u te vaak en te vlug wisselt tussen die twee toestanden, zijn uw hersenen in de war en niet in staat om zich op een van beide bewustzijnssituaties te richten. Als u frequent uw mails doorneemt, op sociale media zit of op het net surft, zit u nu precies in die tussentoestand.

Om uw productiviteit te optimaliseren is het dus de boodschap om dat aan banden te leggen of te beperken. Levitin verwoordt het zo: “Een e-mail waarvan je weet dat die is aangekomen, en die ongelezen in je inbox wacht, kan je aandacht opzuigen als je brein erover blijft denken en je afleidt van wat je aan het doen bent. Wat staat er in? Van wie is het? Is het goed of slecht nieuws? Het is beter om je mailprogramma af te zetten dan om de constante waarschuwingen te horen en te weten dat je berichten negeert.”

Mailproject

De professoren bevelen dan ook aan om het lezen van uw mails als een individuele taak of project te behandelen en er een bepaalde tijdsperiode voor uit te trekken tijdens je werkdag. Het afzetten van notificaties op je pc of smartphone helpt al, en als u het radicaler wil aanpakken dan kan u ook gewoon uw mailprogramma niet openen tot het tijdstip waarop u het hebt ingepland.



Medische data en dossiers zijn voor een doorsnee cybercrimineel interessanter dan kredietkaarten. De medische sector zou hierdoor wel eens een belangrijk doelwit worden de komende jaren.



Medisch dossier voor cybercrimineel interessant

Het zogenaamde 9/11'-moment voor de ziekenhuisindustrie viel eerder dit jaar. Toen gaf de Amerikaanse ziekteverzekeraar Anthem schoorvoetend toe dat 37,5 miljoen medische dossiers in verkeerde handen waren gevallen. Hackers waren ermee aan de haal.

Achterpoortjes

Het voorval had voor de medische industrie evenveel impact als de aanval op de Amerikaanse winkelketen Target die vorig jaar de cyberbeveiliging opnieuw tot een prioriteit van de retailsector had gemaakt.

Ook al werd er niet zo erg veel aandacht aan besteed, de impact was er wel. Bovendien was het geen alleenstaand geval. Eerder hadden verzekeringsfirma's als CareFirst en Premiera Blue Cross aangegeven dat ze af te rekenen hadden met digitale achterpoortjes die door hackers werden gebruikt.

Vijf keer meer waard

Toeval zijn deze inbreuken niet. Specialisten stellen dan ook dat persoonlijke medische informatie een grote waarde heeft.

Volgens sommigen is persoonlijke medische informatie op internet zelfs meer waard dan financiële gegevens. "Medische informatie weerspiegelt het hele levensverhaal van het individu," oppert Caroline Rivett, directeur cyberbeveiliging bij consulent KPMG, in The Financial Times.

Volgens analisten van cyberstrategie-specialist Stroz Friedberg wordt, zo haalt nieuwssite Express aan, op de illegale markt voor gestolen medische gegevens inmiddels vijf keer meer betaald dan voor kredietkaart-informatie.

Redenen

Er zijn diverse elementen die de hoge waarde van medische informatie kunnen verklaren. Enerzijds is er de reikwijdte. Deze informatie omvat gegevens over de woonplaats, beroep, leeftijd, opleiding en gezondheid. Allemaal data die kunnen helpen om op internet een valse identiteit in te vullen.

Anderzijds zijn medische data erg interessant in functie van afpersing of onthullingen. Denk maar aan politici of film- of televisiesternen, die mogelijk een gezondheidsprobleem voor de buitenwereld verborgen zouden willen houden.

Bewust

Volgens experts zijn gezondheidsorganisaties – zoals ziekenhuizen, verzekeraars of overheidsinstellingen – zich tot nu toe niet echt bewust zijn geweest van de bedreiging. Al zijn er uiteraard ook die hier echt over nadenken.

Een organisatie als Kind en Gezin zette de meeste data in de cloud. Maar voor medische dossiers gaat het om een private cloud waar de bestanden geëncrypteerd worden. Minder gevoelige informatie, zoals personeelsplanning, zit in de public cloud.

Hoe dan ook, het zal er voor de gezondheidssector op aankomen om beveiliging nog meer (en hoger) op de agenda te zetten. En dan liefst vooraleer ze zelf het slachtoffer zijn geweest van inbreuken, zoals bij Anthem, CareFirst en Premiera Blue Cross het geval is geweest.



Na avonturen met open versus gesloten standaarden, het aan de kaak stellen van de onveilige OV-chipkaart en een actie tegen informatielekkende websites (Lektober), richt onderzoeksjournalist en tech-nerd Brenno zijn blik nu op digitaal Nederland en de politiek.

Brenno de Winter over digitaal Nederland

Nederland loopt toch voorop met digitalisering en de overheid streeft naar de positie van kennisland?

"Wij lopen wel voorop met digitalisering, we doen veel dingen best goed. Alleen gaan we ook in de minder goede ontwikkelingen wat harder dan andere landen. Kijk maar naar wat het Openbaar Ministerie wil en doet in de strijd tegen cybercrime. Daar wordt geen openlijk debat over gevoerd."

Ben je bang voor geheime en ondoorgrondelijke waarschuwingsrichtlijnen (bijvoorbeeld no-flylijsten) tegen bepaalde personen? Zoals jij zelf vorig jaar bij overheidsorganisaties op een 'zwarte lijst' bent gekomen?

"Ja, hoewel dat laatste wel één van de meest extreme voorbeelden is. Maar kijk ook simpel naar Wob-verzoeken [Wet openbaarheid bestuur - red.]; het is onvoorstelbaar hoeveel moeite burgers moeten doen om gewoon de wettelijk verplichte openheid van onze eigen overheid te krijgen."

Wat is hierbij volgens jou het grondprobleem?

"Mijn grote zorg is dat bij herhaling is gebleken dat de Tweede Kamer niet bij machte is om sturing te geven aan 'digitaal Nederland', aan onze informatiesamenleving."

Wie is dan wel bij machte om te sturen?

"Nou, deels de commercie, waarbij de politiek dan een ondergeschikte rol speelt. Zie bijvoorbeeld handelsverdragen zoals TTIP en eerder al het uiteindelijk tegengehouden ACTA. Daar spelen commerciële belangen de boventoon en komen die verdragen boven onze eigen regels te staan." [TTIP staat voor Transatlantic Trade & Investment Partnership, het is een handelsovereenkomst tussen de EU en de VS, ACTA staat voor Anti-Counterfeiting Trade Agreement en is een handelsovereenkomst ter bestrijding van namaak - red.]

"Bovendien wordt de rol van de Tweede Kamer gemarginaliseerd. Bevoegdheden gaan deels naar gemeenten en deels naar Brussel."

Is dat dan een verkeerde zaak? Meer lokale macht betekent toch ook meer lokale invloed? En Brussel maakt zich toch ook hard voor de



informatiemaatschappij? Dáár is immers de omstreden bewaarplicht laatst gesneuveld.

"Ja, de Europese rechter heeft de bewaarplicht afgewezen. Maar vergeet niet dat de dataretentie eerst vanuit Brussel is gekomen. Vervolgens is het wel realiteit geworden en toen na jaren van aanvechten pas door de rechtbank illegaal verklaard. Het had eigenlijk niet eens zo ver mogen komen."

"Los daarvan zorgt de marginalisering van de Tweede Kamer ervoor dat veel regie op nationaal niveau en daarmee Nederlandse identiteit verloren gaan. Alles wordt veel minder centraal geregeld. En dat raakt dus alles! Want digitalisering is de kern van deze samenleving. Je moet dan wel bestuurders hebben die daar goed mee om kunnen gaan. Maar als het digitaal wordt, is onze overheid niet goed onderlegd."

Daar wordt toch aan gewerkt? Zie onder meer de onderzoekscommissie onder leiding van Ton Elias die het mislopen van ICT-projecten bij de overheid heeft doorgelicht.

"Juist dat onderzoek toont aan dat de Tweede Kamer niet serieus acteert. De belangrijkste conclusie uit dat onderzoek heeft Elias wel gezien, maar daar is verder helemaal niets mee gedaan. Namelijk dat de overheid de eigen informatievoorziening niet op orde heeft, waardoor het mislopen van ICT-projecten heel slecht zichtbaar is. Daar is de commissie zelf ook tegen aangelo-

pen."

"Vervolgens moeten er na die belangrijkste conclusie de aanbevelingen komen. Maar die zijn er niet. Helemaal niets! Men vertrouwt erop dat het wel goed komt. Ook de CIO [Chief Information Officer - red.] van de Nederlandse overheid. Het probleem wordt aan alle kanten geconstateerd en ook erkend. Maar er wordt niets concreets aan gedaan."

Waarom dan niet?

"De Tweede Kamer zegt zelf in het rapport Elias dat het ze niet interesseert en dat ze er niet deskundig in zijn. De Tweede Kamer is dysfunctioneel wat betreft het digitale. Het is als een asbestprobleem: iedereen denkt dat er niks aan de hand is, tot het te laat is."

Maar de informatiemaatschappij en Nederland-kennisland zijn toch politieke speerpunten? Of hebben we het hier over het verschil tussen woorden en daden?

"Ja. Het zijn holle frases. De politiek weet het niet en wil het ook niet weten. Ondertussen leven we met z'n allen al in een informatiesamenleving en daar moeten we wat mee. Want deze tijd gaat later wel beoordeeld worden. We weten nu dat het niet goed zit, met privacy, security en informatievoorziening. Voor je het weet zit je met zoekgeraakte bonnetjes van miljoenendeals met grote criminelen."

Is Brenno de Winter omgeturnd van tech-journalist tot politiek dier?

"Als je wat voor de maatschappij wilt bereiken, heb je ook met politiek te maken. Dáár komt technologie en de maatschappij bij elkaar. Ik ben geen politiek activist; ik ben agnostisch voor partijen. Het thema is echter wel een politiek thema. Er is bijna geen activiteit meer in de fy-



sieke wereld die geen digitale poot heeft."

"Alleen lijdt de overheid wel aan technooptimisme. Nee, dat is niet de overtuiging hebben dat technologie ons veel voordelen kan brengen. Dat kan het ook. Ik bedoel met technooptimisme het geen oog hebben - geen oog willen hebben - voor de mogelijk negatieve kanten. Zoals de boodschap van professor Bart Jacobs, die door de Tweede Kamer is gevraagd om zijn professionele blik te geven op technologische projecten zoals de OV-chipkaart. Zijn boodschap was onwelgevallig en zijn advies is vervolgens genegeerd."

"Erger nog is dat er geen zelfcorrigerend mechanisme is. Daar is dan enorme druk van buiten voor nodig. En als er al eens iets gecorrigeerd wordt, dan schiet de overheid gelijk weer door: dan gaat alles op slot. Daarmee is de burger dan weer buitengesloten."

Ben je pessimistisch over de digitale toekomst van Nederland?

"Nee, ik ben ook wel optimistisch. We zijn nu echter wel op een punt in onze geschiedenis dat we iets moeten doen. Als we nu niks doen, wordt het steeds moeilijker. Dan wordt het argument steeds sterker dat 'we nu al zo ver zijn met X dat we niet terug kunnen'. We worden onderuit geschoffeld, door de grootdatabe-zitters. Die hebben straks de macht."

Geef eens een voorbeeld van zo'n X. Iets waar we nú op moeten sturen of bijsturen.

"[Big Data](#) is onvermijdelijk, daar zijn we het wel over eens. Zoals het er nu voor staat, is de con-

sument daarbij vogelvrij verklaard. Ik mag als persoon niet meer weten hoe welke informatie over mij is vergaard en hoe dat wordt gecombineerd. De consument is ondergeschikt gemaakt aan het systeem, waarbij het systeem niet meer door ons is gemaakt. De grootste belanghebbende staat buitenspel."

"La Place geeft je een gratis kopje koffie, in ruil

voor je persoonlijke informatie die misschien wel 10 euro waard is. Wat gebeurt er met die informatie als V&D failliet gaat? Een zorgverzekeraar kan best interesse hebben in die gegevens. Een curator hoeft de data ook niet slechts één keer te verkopen. Hij moet immers de maximale waarde uit een failliete boedel zien te halen, voor de schuldeisers."

"En waarom wil de mobiele app van een pakketbezorger op constante basis mijn locatie weten? Als het servicegericht gaat om het afleveren van mijn pakketje, dan moet de vraag zijn waar ik het morgen afgeleverd wil hebben. Maar dit is datahonger: het hebben van alsmáar meer data is belangrijker dan servicegericht zijn. Ondertussen is een PostNL wel bezig om de klantenbestanden van Bol.com en vele andere winkels in kaart te brengen. Een webwinkel moet hier heel nerveus van worden."

We kunnen toch stemmen? Als klanten met onze portemonnee en als burgers minstens één keer in de vier jaar?

"Ja, maar in verkiezingsprogramma's staan dit soort zaken niet op de agenda. Bovendien werkt de overheid steeds meer aan publiek-private samenwerkingen, waarbij openheid niet van toepassing is en waar sturing heel lastig blijkt. Daar is betere governance nodig."

"De overheid is een heel slechte aandeelhouder in dat soort samenwerkingen. Kijk bijvoorbeeld naar ProRail, die heeft maar één aandeelhouder: de overheid. Toch blijkt het haast onmogelijk om daar lijn in te kunnen brengen."

Het gaat je niet alleen om grip op technologie.

Je maakt je ook zorgen om zaken als function creep: het geleidelijk aan inzetten van zaken voor andere doeleinden. Leg eens uit?

"Een goed voorbeeld is het Syri-systeem en de nieuwe SUWI-wet [structuur uitvoeringsorganisatie werk en inkomen - red.] die zonder een minuut openbaar overleg is geaccepteerd. Als zogeheten hamerstuk aangenomen; met slechts één hamerslag in de Kamer. Die wet is oorspronkelijk bedoeld om terrorisme te bestrijden. Tegenwoordig dient het echter ook om fraudeurs op te sporen. Daarvoor mogen overheidsinstanties allerlei gegevens en databases aan elkaar koppelen. Alle burgers worden dus grondig doorgelicht."

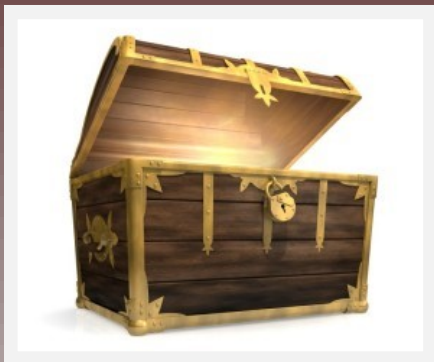
Een bekende reactie daarop is: 'Je hebt toch niks te verbergen?'

"Ik lust geen zuurkool, antwoord ik daar tegenwoordig op. Ja, dat is een irrelevant antwoord. Net zoals het irrelevant is of je wel of niet iets te verbergen hebt. We hebben simpelweg grondrechten, zoals vrijheid van godsdienst, vrijheid van meningsuiting en recht op een persoonlijke levenssfeer. Dat zijn zaken die allang geregeld zijn, waar goed over is nagedacht. Hier is het Europese Verdrag voor de Rechten van de Mens, daar staat het allemaal in. Het privacyrecht geldt niet alleen verticaal: van jou naar de overheid toe. Het geldt ook horizontaal: tussen jou en de rest van de wereld."

"De informatiesamenleving gaat over én ICT-beveiliging én basale burgerrechten én de economie. Er wordt tot op heden te veel op het eerste en het laatste gestuurd. Terwijl de economie juist op termijn veel baat heeft bij het goed borgen van beveiliging plus burgerrechten, inclusief privacy. Er valt zo veel te winnen als je dát als land goed geborgd hebt. Ik geloof echt dat er een gouden eeuw op ons ligt te wachten!"

Kom eens met wat concretere adviezen: hoe moeten we omgaan met technologie?

"Als je de vraag zo stelt dan is het antwoord ook: voer het debat eerlijk en stuur niet op het doordrukken. Erken de beperkingen. Wees er niet blind voor, zoals in het begin is gedaan bij de OV-chipkaart. Moedig mensen en organisaties aan om die beperkingen tegemoet te treden. Het is net zoals de zwaartekracht: dat is ook een beperking. Eentje waar we elke dag mee opstaan. Toch is vliegen een goede, nuttige en efficiënte bezigheid die ook nog eens commercieel aantrekkelijk is. Technologie kan dat ook zijn, meer dan het nu is."



Software schatkist

De kist is gevuld met fraaie software en naslag.

Nieuwsgierig?

Open de kist middels de sleutel en ontdek.....



(Enkelen onder jullie weten dat ik regelmatig remixen maak van trance– en dancemuziek onder de naam DoubleYouAB.

Omdat de vakantietijd is aangebroken kunnen jullie via de schatkist mijn nieuwe TrancePhonic 2015 mix downloaden (in de traditie van Sensation white) . Lekker voor in de auto af aan het strand.....!! . Try it out!)



Het College bescherming persoonsgegevens (CBP) is zeer kritisch over het wetsvoorstel dat burgers en bedrijven toestaat om beelden van misdrijven online te zetten. Het is onduidelijk waarom dit noodzakelijk is, er is zeer de vraag of de veiligheid hierdoor wordt verhoogd en de inbreuken op de privacy staan niet in verhouding tot het doel van het wetsvoorstel. Het wetsvoorstel van minister Ard van der Steur regelt dat én hoe particulieren en bedrijven camerabeelden van verdachten mogen publiceren op internet, overigens nadat er aangifte is gedaan en de beelden ter beschikking zijn gesteld aan de politie. Het college wijst ook op het feit dat onschuldige burgers ten onrechte als verdachte kunnen worden aangemerkt.

Wie geflitst is op de snelweg, kan de foto daarvan sinds deze week terugzien bij het [Digitaal Loket](#) van het CJIB. Ook andere verkeersboetes zijn daar te vinden, net als een mogelijkheid om online te betalen (DigiD vereist) of beroep aan te tekenen. In een testfase van vier maanden is het loket al veertigduizend keer bezocht.

AIVD en MIVD krijgen meer mogelijkheden om telefoongesprekken en e-mailverkeer af te tappen. Met de nieuwe Wet voor de Inlichtingendiensten moeten terroristen en potentiële Syrië-gangers beter kunnen worden opgespoord. De twee diensten kunnen straks grote hoeveelheden data onderscheppen van mobieltjes, apps, sociale media en e-mail, en deze gegevens bovendien drie jaar bewaren. Volgens minister Ronald Plasterk is de privacy van burgers niettemin gewaarborgd. Hij verwacht dat de wet nog deze kabinetsperiode van kracht wordt.

De familie Graansma uit Drachten heeft de gestolen Audi A4 weer terug, na een succesvolle facebookactie. De Graansma's werden slachtoffer van een oplichterstruc 'die de politie Noord-Nederland nog niet eerder bij de kop had', schreven lokale kranten. 'Uitgekookt, geraffineerd en hondsbrutaal'. Toen de auto op internet te koop werd gezet, reageerde een stel uit de Achterhoek. Er werd een prijs afgesproken en een datum. Het stel zou de auto komen bekijken maar ze verschenen pas enkele uren later. Iets met hun zoontje ... Doorgewinterde internetters ruiken dan al onraad maar dit keer niet. De aanstaande kopers, 'Robert en Mireille' wilden de zaak snel regelen

en dat kon wel online, op de MacBook van de verkopers natuurlijk. Natuurlijk moest er nog even naar de bank gebeld worden maar ja, achter dat nummer zat natuurlijk een handlanger. Enfin. De auto was betaald, de sleutels werden overhandigd. Er werd nog een foto gemaakt. Maar Graansma ontdekte al snel dat hij besodemieterd was – e-mails werd niet beantwoord, het 06-nummer bleek van een 15-jarig meisje, het bedrijf waar Robert zei te werken kende hem niet. Graansma deed aangifte maar zette zijn verhaal ook op facebook. Daar regende het tips, het bericht werd in een dag tijd tweeduizend keer gedeeld. De auto werd al teruggevonden. 'Nu deze jongeman nog even'.

Kinderlokkers anno 2015 – geen lange jas, geen snoepjes, maar volledig digitaal. Volgens Remco Pijpers van Mijn Kind Online zijn digitale kinderlokkers, groomers, vaak op zoek naar kwetsbare, onzekere meisjes. Ze benaderen, bijvoorbeeld via facebook, honderden meisjes in de hoop dat er eentje instinkt – de man die nu wordt verdacht van ontucht met Lisa had maar liefst 2733 jonge meisjes in zijn vriendenlijst. In vrijwel alle gevallen doen ze zich voor als leeftijdsgenoot en zoeken ze interactie, nog niet eens seks, maar wel macht. Pijpers spreekt, in Trouw, van 'kampioenen in sociale manipulatie' die stap voor stap hebben geleerd hun slachtoffers steeds verder te manipuleren. 'Als je de hele dag gesprekken voert, leer je precies wat je wel en niet kunt zeggen'. Bij de politie beaamt Walter van Kleef, landelijk coördinator zedenzaken, dat manipuleren in fases gaat. 'Als ze hun slachtoffer hebben uitgekozen, geven ze hun het gevoel dat ze speciaal zijn. Daarna begint het inpalmen door geheimpjes te delen en te zeggen dat seksuele handelingen heel normaal zijn. Vervolgens isoleren ze een meisje door het tegen haar ouders op te zetten'. Soms komt daar chantage bij, bijvoorbeeld als het meisje een pikante foto heeft gestuurd. Van Kleef noemt de moderne groomer gevaarlijker dan de kinderlokken-van-vroeger. 'Achter een computer kan iemand veel gesprekken met verschillende potentiële slachtoffers tegelijk voeren, tot hij een keer beet heeft. Het volume maakt het gevaarlijk. En het kan vanuit de luie stoel. Dat verlaagt de drempel'. Volgens alle deskundigen is het toeverwoord (voor ouders) om te (leren) praten over wat het kind op internet ziet. Als een groomer door heeft dat een tiener over hem praat met haar ouders, geeft hij het vaak op.

Het recht om vergeten te worden gaat veel te ver. Vindt Google. En daarom weigert het bedrijf om een Frans verzoek te honoreren om zoekresultaten wereldwijd te verwijderen. Zoals bekend geldt het vergeetrecht alleen voor Europese landen, als informatie op een website 'ontoereikend, irrelevant of buitensporig' is kan Google worden verplicht de link ernaartoe weg te halen. Maar alleen in het land waar het verzoek gedaan is. Frankrijk eiste recent dat bepaalde zoekresultaten uit alle edities van Google zouden verdwijnen maar dat gaat te ver, blogt het privacyhoofd van Google, Peter Fleisher. Wat legaal is in het ene land, is immers vaak verboden in een ander land. 'Thailand verbiedt kritiek op de koning, Turkije verbiedt kritiek op Atatürk en Rusland verbiedt homopropaganda', aldus Fleischer die wijst op een 'race naar beneden' als Frankrijk zijn zin krijgt. Internet wordt dan 'net zo vrij als de minst vrije plek op de wereld'. Fleischer vindt dat geen enkel land kan controleren wat mensen in een ander land kunnen zien.

Uit onderzoek van beveiliging Kaspersky blijkt dat een op de twaalf cyberaanvallen wereldwijd, wordt verstuurd vanuit Nederland. Iets meer dan de helft van alle aanvallen komt uit Rusland, 12% uit de VS. Opvallend in de top-10 is de vijfde plek voor de Maagdeneilanden (2,1%). Het gaat in het onderzoek alleen om de cyberaanvallen die werden geblokkeerd door de software van Kaspersky. Die software wist van april t/m juni 2015 zo'n 380 miljoen aanvallen af te weren. In opkomst is malware gericht tegen mobiele apparaten. In het tweede kwartaal werden drie keer zoveel nieuwe mobiele malwareprogramma's gelanceerd dan in het eerste kwartaal. Het aantal cyberaanvallen dat toegang probeert te krijgen tot bankrekeningen nam met achthonderdduizend af tot bijna zes miljoen.

De Kansspelautoriteit heeft twee buitenlandse gokbedrijven en twee directeuren daarvan een boete van 180 mille opgelegd. De bedrijven Total E Soft Ltd (geregistreerd in Groot-Brittannië) en XKL Limited (Costa Rica) boden via veertien verschillende websites gokspelletjes aan. De sites, waarop casinospelen, digitale gokkasten, pokerspelen en sportwedenschappen stonden, waren in het Nederlands en dus specifiek gericht op Nederlandse gebruikers.



Verslavingsinstelling Novadic-Kentron en het Trimbosinstituut waarschuwen weer eens voor de opkomst van designerdrugs in het uitgaansleven. Met name het gemak waarmee de drugs – van speed en xtc tot 4-mmc, 6-abp en 4-fa – via internet besteld kunnen worden, is zorgwekkend. Volgens experts worden deze designerdrugs niet gemaakt door traditionele criminele netwerken maar door ‘whizzkids die het op een zolderkamertje in elkaar knutselen’. De drugs worden extra gevaarlijk genoemd omdat niemand goed weet wat de schadelijke gevolgen zijn. Volgens de politie moeten ‘we niet de illusie hebben dat we dit kunnen tegenhouden: er is gewoon heel veel vraag naar’. Woordvoerder Erik Passchier van de politie wijst ook naar de ouders. ‘Die moeten zich afvragen hoe het kan dat drugs zo normaal zijn geworden’.

Om ‘dichter bij de mensen te zijn’ heeft de politie Zoetermeer sinds kort een eigen facebookpagina. Daarop geeft de politie ‘een kijkje achter de schermen’, oftewel een filmpje vanaf een politiemonitor, foto’s van agenten-aan-het-werk, opsporingsberichten en tips. Wijkagent Bart van Rijn noemt de pagina ‘een logisch vervolg op de twitterkanalen’. Hij vergelijkt twitter met de radio en facebook met de televisie. ‘Twitter is meer voor de korte, snelle berichten, terwijl je met facebook meer de ruimte hebt’. Volgens Van Rijn bereikt facebook ook een andere groep mensen. ‘Op twitter zijn onze volgers geografisch heel verspreid en zijn er veel liefhebbers die alle accounts van hulpverleners volgen. Met facebook denken wij wat meer in het zicht te komen en zijn we dicht bij de mensen’. De facebookpagina is overigens nog lang niet het ‘laatste digitale extraatje’, er komt nog een eigen youtubekanaal.

Een opvallend bericht komt van de

Fraudehulpdesk dat periodiek onderzoek doet naar internetfraude. Uit het onderzoek komt niet alleen dat sinds 2012 een op de vijf Nederlanders slachtoffer werd van internetoplichting maar ook dat 56% van de slachtoffers zo weinig vertrouwen in de politie heeft dat ze geen aangifte doen. Aangifte doen is zinloos, aldus veel slachtoffers. Wellicht net zo opvallend is dat driekwart van de respondenten vindt dat het wél een overheidstaak is om fraude te voorkomen en te bestrijden. Net iets meer dan de helft vindt dat het ook de eigen verantwoordelijkheid is om niet te worden opgelicht.

Binnenkort op vakantie? Dan heb je tijd genoeg om even uit te kijken naar de Meest Gezochte Cyberbandieten. Voor het geld hoeft je het niet te laten, want er staan behoorlijke bedragen op hun hoofden. Op de lijst van de FBI staan behalve namen en foto’s ook de strafbare feiten waar de mannen – er staat geen enkele vrouw op de lijst – van worden verdacht. De hoogste premie, drie miljoen dollar, staat op het hoofd van Evgeniy Mikhailovich Bogachev, aka Lucky12345 aka Slavik. Bogachev zou het grote brein achter het Zeus-virus zijn waarmee hij meer dan 100 miljoen dollar verdiende. Maar ook de nummers 15 en 16 op de lijst, Farhan ul Arshad en Noor Aziz Uddin, zijn nog altijd vijftig mille waard. Bij twee van de gezochten is een Nederlandse connectie. Zo wordt sinds 2012 gezocht naar de Nederlandse Vietnamees Viet Quoc Nguyen, die ruim een miljard e-mailadressen bijeen hackte. En naar de Let Peteris Sahurovs die gebruik maakte van Nederlandse servers. Sahurovs werd in 2011 opgepakt in Letland maar kennelijk nooit uitgeleverd aan de VS.

In 2010 kwamen de eerste wijkagenten op twitter, in 2015 is – in Amsterdam

althans – de helft van alle wijkagenten op dit medium actief. Het Parool bericht over hun successen en mislukkingen, hun pogingen om de burgers te bereiken en informatie te delen. De politie is tevreden, aldus het artikel. Het voornaamste doel, het vergroten van de zichtbaarheid van blauw op straat, is bereikt. Succesvol is vooral het bureau Oost/Zeeburg, met een facebookpagina, een fanatiek twitterende wijkagente en een teamchef ‘die open staat voor vernieuwingen’. Deze teamchef, Jaap van der Woude, vergelijkt sociale media met de vroegere balie in het politiebureau. ‘Mensen kwamen binnen om gewoon even iets door het bureau heen te roepen, of om een boodschap door te geven’. Deze berichtjes komen nu op de virtuele balie binnen, aldus Van der Woude: via sociale media. Een discussie is nog op welke media/platforms de politie aanwezig moet zijn. In principe op alle, maar het blijkt lastiger dan gedacht om zowel te instagrammen, te foresquaren, te periscopen, te twitteren, te facebooken en ook nog boeven te vangen. Voor Van der Woude is de basisvraag of het er veiliger van wordt. ‘Op sociale media hebben we contact met mensen, organiseren we bijeenkomsten, krijgen we getuigen aangedragen. Er komen aangiftes binnen en er is interactie’.

Het OM heeft laten weten geen vervolging in te stellen tegen de man die begin 2015 zogeheten Jodenzeep aanbood op Marktplaats. Het NFI onderzocht de zeep, waarin resten zouden zitten van Joodse mensen uit de Tweede Wereldoorlog, maar bewijs werd niet gevonden. Ook de tekst bij de advertentie is niet beledigend, aldus het OM. Een antifascistische organisatie had geklaagd over de advertentie van de man, een verkoper van oorlogsmemorabilia.

Phishing- / valse e-mails melden

ABN AMRO Bank: valse-email@nl.abnamro.com

ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

ICS- / ABN AMRO creditcards: valse-email@icscards.nl

Voor vragen over veilig internetbankieren bij uw eigen bank, kunt u op een van de onderstaande websites terecht.

Websites banken

[ABN AMRO](#)

[LeasePlan Bank](#)

[Argenta](#)

[Rabobank](#)

[Credit Europe Bank](#)

[SNS Bank](#)

[DeltaLloyd Bank](#)

[Staal Bankiers](#)

[DHB Bank](#)

[Triodos Bank](#)

[Friesland Bank](#)

[Van Lanschot Bank](#)

[ING Bank](#)

[ASN Bank](#)



MARKTPLAATS: "Wat moet ik doen als ik denk dat ik ben opgelicht?"

Antwoord

1. Wanneer u vooraf betaalt, maar de verkoper het product vervolgens niet levert, adviseren wij het volgende:

Neem eerst nogmaals contact op met de verkoper. Mogelijk is er sprake van een misverstand of wordt het product alsnog geleverd. Breng in geval van oplichting altijd de Politie op de hoogte (dit kunnen wij niet voor u doen). Zij hebben immers de kennis, expertise en opsporingsbevoegdheden om onderzoek te doen naar strafbare feiten. Wij adviseren u om aangifte te doen bij het Meldpunt Internetoplichting van de Politie via www.mijnpolitie.nl (formulier Melding Internetoplichting).

Wij adviseren u om het formulier zo accuraat en volledig mogelijk in te vullen.

Zorg dat u, wanneer u aangifte gaat doen, alle relevante gegevens bij de hand heeft zoals:

- Uw eigen (contact)gegevens, inclusief uw Burgerservicenummer (BSN).
- De (contact)gegevens van de partij met wie u heeft gehandeld (zoals naam en bankrekeningnummer).
- De gegevens van de transactie, zoals het advertentienummer en de onderlinge communicatie.

Meld oplichting ook altijd aan Marktplaats. Wij nemen dergelijke meldingen zeer serieus en nemen waar mogelijk gerichte maatregelen. Indien u aangifte doet via het formulier Melding Internetoplichting op www.mijnpolitie.nl wordt direct



Controleer vooraf de (bank)gegevens van de verkoper op
www.mijnpolitie.nl/miocheck

(ruime zin: algehele benamingen / enge zin: specifieke verschijningsvormen)

. Artikel 138a WvSr: het binnendringen in een geautomatiseerd werk.

. Artikel 161 septies WvSr: stoornis in de gang of in de werking in een geautomatiseerd werk of werk voor telecommunicatie door schuld.

. Artikel 350a WvSr: het opzettelijk onbruikbaar maken en veranderen van gegevens.

. Artikel 350b WvSr: het onbruikbaar maken en
veranderen van gegevens door schuld,

. Artikel 139c WvSr: het aftappen en/of opnemen van gegevens en

Artikel 139d WvSr: het plaatsen van opname-,
aftap- c.q. af luisterapparatuur.

Er zijn geen specifieke wetsartikelen om cybercrime in ruime zin aan te duiden. Voor de hoofddaad worden dezelfde wetsartikelen gebruikt als wanneer de criminele daad niet met ICT zou worden gepleegd.

'Het zaaien van haat of het (opzettelijk) beledigen of discrimineren van een groep mensenwegens hun ras, hun godsdienst of levensovertuiging, hun hetero- of homoseksuelegerichtheid of hun lichamelijke, psychische of verstandelijke handicap, zonder een bijdrage te leveren aan het publieke debat, waarbij ICT essentieel is voor de uitvoering'.

Haatzaaien staat niet als zodanig in het wetboek.

Aan de hand van de geformuleerde definitie kunnen echter de volgende wetsartikelen worden onderscheiden die delicten omschrijven welke vallen onder deze noemer:

- Artikel 147 WvSr: godslastering
- Artikel 90quater WvSr: discriminatie.
- Artikel 137d WvSr: aanzetting tot discriminatie van een bevolkingsgroep.

- . Artikel 137e WvSr: openbaarmaking discriminerende uitlatingen.
- . Artikel 137f WvSr: deelname of steunen van discriminatie.
- . Artikel 137g WvSr: discriminatie in ambt, beroep of bedrijf.
- . Artikel 131 WvSr: opruiing.

'Cyberstalking' is de verzamelnaam voor het stelselmatig lastigvallen van een persoon door provocerende uitspraken te doen en/of berichten te plaatsen via online forums, bulletin boards en chatrooms, of de ander als het ware via spyware te bespioneren dan wel voortdurend ongevraagd e-mail en spam te sturen. Er is sprake van een verregaande inbreuk op de privacy van het slachtoffer' .

Relevante wetsartikelen zijn:

Artikel 285b WvSr: belaging.

Artikel 138a WvSr: computervredebreuk.

Artikel 266 WvSr: belediging.

Grooming wordt door het particuliere Meldpunt Kinderpornografie op Internet (MKI) opgevat als het zich op internet anders voordoen (door een volwassene) met het doel om seksueel getinte contacten te leggen met kinderen. Deze contacten kunnen zowel virtueel (seksuele handelingen voor de webcam) als fysiek (een ontmoeting waarbij het kind daadwerkelijk seksueel misbruikt wordt) zijn. Op dit moment is grooming niet strafbaar.

Grooming is echter wel opgenomen in het door Nederland ondertekende, maar nog niet door Nederland geratificeerde EU-verdrag van Lanza-rote van 25 oktober 2007, artikel 23 ('Solicitation of children for sexual purposes'), waarin landen zich verplichten om grooming strafbaar te stellen. Grooming is dan het door een volwassene via ICT leggen van contacten met een jongere met de intentie deze te ontmoeten voor het verrichten van seksuele handelingen, gevolgd door het feitelijk geven van uitvoering aan het tot stand brengen van die ontmoeting. Dat is een aanzienlijk engere uitleg dan het MKI geeft, vooral omdat volgens het verdrag begonnen moet zijn met het realiseren van de ontmoeting ('material acts leading to such a

meeting').

Verschijningsvormen:

drugs, geneesmiddelen, vuurwapens en explosieven, mensenhandel- en smokkel, heling.

Kenmerkend bij deze vormen van cybercrime is dat de handel plaatsvindt op of middels ICT

(bijvoorbeeld marktplaats) en dat de betrokken partijen weten dat het gaat om illegale handel.

Relevante artikelen zijn:

Artikel 273a WvSr mensenhandel.

Artikel 416 WvSr opzetheling.

Artikel 417 WvSr opzetheling (gewoonte).

Artikel 274 WvSr slavenhandel.

Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



Cybercrime wetsartikelen (2)

Bij **piraterij** gaat het feitelijk om illegale handel van allerhande 'cd's, dvd's, films, software en andere producten waarvoor auteursrechten gelden'. De nadruk ligt volgens het [KLPD](#) veelal bij eindgebruikers, internetpiraten en vervalsters, en in mindere mate bij gebruikers van licenties (bijvoorbeeld bedrijven) en computerverkopers. In alle gevallen is piraterij echter strafbaar en valt het onder meer onder het Wetboek van Strafrecht, de Auteurswet en de Merkenwet.

Relevante artikelen uit het wetboek van strafrecht zijn:

- [Artikel 337 WvSr](#): handel goederen vervalste merken.
- [Artikel 328 WvSr](#): oneerlijke mededinging.
- [Artikel 441a WvSr](#): heling.
- [Artikel 1 AW](#): auteurswet
- [Artikel 31 AW](#): opzettelijk inbreuk op auteursrecht
- [Artikel 31a AW](#): voorwerp met daarop een inbreuk op auteursrecht
- [Artikel 31b AW](#): beroep maken van inbreuk op auteursrecht

Kinderpornografie.

Kinderpornografie is in Nederland strafbaar gesteld in artikel [240b Wetboek van Strafrecht](#).

Kinderpornografie is volgens dit artikel iedere afbeelding - of gegevensdrager die een afbeelding bevat - van een seksuele gedraging waarbij iemand, die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar betrokken is'. Zowel het verspreiden, tentoonstellen, vervaardigen, invoeren, doorvoeren, uitvoeren als in bezit hebben ervan is in Nederland strafbaar. In Nederland is het enkel kijken naar kinderpornografie niet strafbaar.

Illegale kansspelen.

'Volgens de Wet op de kansspelen (Wok) is er in Nederland een verbod op het aanbieden,

propageren en gebruikmaken van kansspelen waarvoor geen vergunning is verleend. Illegale

kansspelen en gokken op het internet (bijvoorbeeld het online casino) is één van de groeiindustriën

op internet'.

Relevante wetsartikelen zijn:

[Artikel 1 Wks](#): wet op de kansspelen

[Artikel 1a Wks](#): piramidespelen

E-fraude.

'De essentie van fraude is steeds dezelfde: mensen eigenen zich middels bedrog geld of vermogensbestanddelen toe waarop ze geen recht hebben en tasten daardoor de rechten van anderen aan. Er zijn verschillende

begrippen in omloop om de cybervorm van fraude te beschrijven, zoals fraude in e-commerce en internetfraude. 'Bij deze vorm van fraude wordt het internet gebruikt om op oneigenlijke wijze gelden, goederen en diensten te verkrijgen zonder daarvoor te betalen of tegenprestaties te leveren'.

Bij internetfraude wordt er al snel gedacht aan oplichtingen via verkoopsites op internet zoals marktplaats en e-bay. Wij gebruiken de term 'e-fraude' als overkoepelende term. E-fraude is bedrog met als oogmerk het behalen van financieel gewin waarbij ICT essentieel is voor de uitvoering. Fraude staat niet als zodanig in de wet genoemd. Relevante wetsartikelen uit het wetboek van strafrecht zijn:

[Artikel 326 WvSr](#): oplichting.

[Artikel 225 WvSr](#): valsheid in geschrifte.

[Artikel 231b WvSr](#): identiteitsfraude

[Artikel 310 WvSr](#): diefstal.

[Artikel 321 WvSr](#): verduistering.

[Artikel 416 WvSr](#): heling.

