Secure Computing Magazine

Met de CTRL toets + het scrolwieltje van uw muis , kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen.

INDEX

AKTUEEL

MQTT-protocol: IoT-communicatie van kernreactors en gevangenissen publiek toegankelijk

————————————————————

Een enorm aantal IoT-sensors in bijvoorbeeld auto’s en vliegtuigen communiceert via het telemetrieprotocol MQTT met de bijbehorende servers. Dat gebeurt standaard zonder gebruik te maken van versleuteling of wachtwoorden. Hackers kunnen de communicatie hierdoor niet alleen meelezen, maar de verstuurde gegevens ook simpel manipuleren.

MQTT werd rond de millenniumwisseling ontwikkeld om telemetriegegevens tussen sensors en servers over onbetrouwbare dataverbindingen te kunnen versturen. Voordat Facebook zijn Messenger op XMPP baseerde, maakte de chatsoftware eveneens gebruik van MQTT. Het protocol is verder alleen bij ingewijden enigszins bekend, maar lijkt dankzij het Internet of Things weer wat populairder te worden.

De onbeschermd via internet communicerende sensors bevinden zich in auto’s, kernreactors, fitnesstrackers, aardbevingssensors, gevangenissen, geldautomaten, klimaatregelingen, lampen, medische apparatuur, pipelines, tv-zenders en zelfs vliegtuigen.

Afhankelijk van de toepassing lekken ze informatie als bitcoindata, druk, fitness-info, login-tokens, gebruikersnamen/wachtwoorden, locatie (lengte- en breedte), positionering van het stuur of rempedaal, stralingsgegevens, temperatuur of snelheid, toestandsmeldingen (deur open/dicht in gevangenissen) en nog veel meer..

Rubrieken:

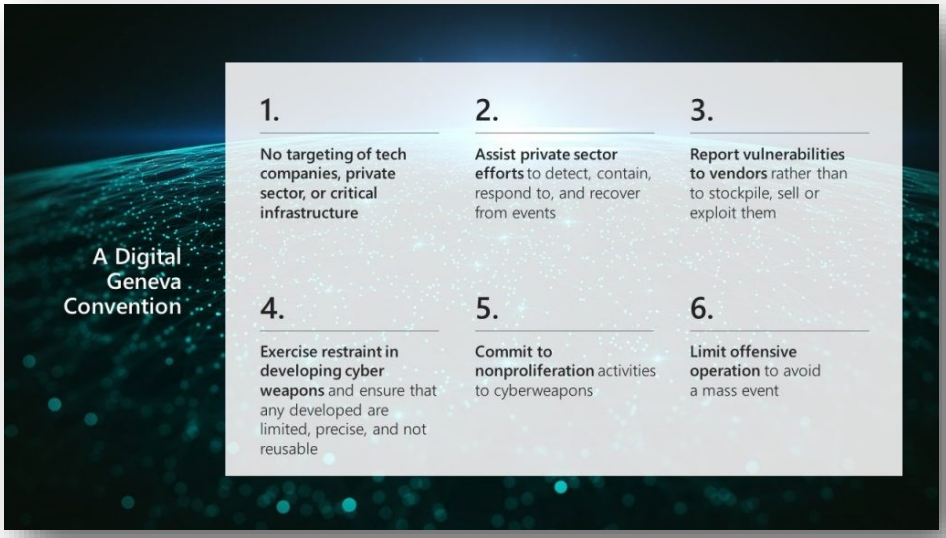
- Verder op Facebook / de website
- Cops in Cyberspace
- Rechtspraak
- Verschijningsvorm cybercrime
- Wetsartikel
- Video
- Handig

Microsoft wil Geneefse Conventie voor internet

Microsoft wil dat er een Geneefse Conventie voor internet komt die burgers, techbedrijven, vitale infrastructuur en private sector tegen cyberaanvallen van overheden beschermt. Ook moeten kwetsbaarheden in software bij de leverancier worden gemeld, in plaats van worden verzameld en aangevallen.

Dat heeft de softwaregigant vandaag tijdens de RSA Conferentie in San Francisco bekendgemaakt. Volgens Microsoft-topman Brad Smith is het aantal cyberaanvallen door landen het afgelopen jaar flink toegenomen. Dat heeft volgens Smith gevolgen voor het internet en daarom moeten er internationale regels komen om het internetgebruik door burgers te beschermen.

"Net zoals de Geneefse Conventie burgers in oorlogstijd beschermt, hebben we nu een Digitale Geneefse Conventie nodig die ervoor zorgt dat overheden burgers in vredestijd tegen staatsaanvallen beschermen", aldus Smith. "En net zoals de Geneefse Conventie stelt dat de bescherming van burgers directe betrokkenheid van het Rode Kruis vereist, vereist bescherming tegen cyberaanvallen door landen de actieve hulp van techbedrijven."



De Microsoft-topman stelt dat techbedrijven een unieke rol als "first responders" voor het internet kunnen vervullen. Daarbij moeten de techbedrijven als een "neutraal Digitaal Zwitserland" fungeren die klanten overal ter wereld helpen en door iedereen als betrouwbaar worden gezien. Smith vindt dan ook dat techbedrijven niet het doelwit van cyberaanvallen door landen mogen worden, net als de vitale infrastructuur. Als voorbeeld noemt Smith de aanval op Sony in 2014, die volgens de Microsoft-topman door Noord-Korea was uitgevoerd, en aanvallen op het 'democratische proces', waarbij hij doelt op de aanval op de Amerikaanse Democratische Partij.

"Conflicten tussen landen zijn niet langer beperkt tot de grond, zee en lucht, nu cyberspace een potentieel nieuw slagveld is geworden." Het grote verschil met de andere terreinen is dat cyberspace vooral door private bedrijven wordt gemaakt en beheerd. Smith roept overheden dan ook op om meer te doen en internationale cybersecurity-afspraken te maken. "Samengevat, het is de hoogste tijd dat overheden een Digitale Geneefse Conventie sluiten om burgers op het internet te beschermen."

Bron: Microsoft

De nieuwe afluistermogelijkheden van de AIVD

De nieuwe Wet op Inlichtingen- en Veiligheidsdiensten is door de Tweede Kamer geloodst, ondanks felle protesten van experts, hoogleraren en actiegroepen. Als de WIV ook door de Eerste Kamer komt, betekent dat dat de Nederlandse inlichtingendiensten verregaande bevoegdheden krijgen om grote sleepnetten uit te voeren. Het debat dat eerder in de Tweede Kamer werd gehouden werd onder de volgers ook wel het 'sleepnetdebat' genoemd. Dat is namelijk wat de inlichtingendiensten zoals de AIVD en de MIVD mogen doen als de wet is doorgevoerd: een 'sleepnet' uitgooien over een grote groep Nederlanders, om vervolgens te kijken of daar mogelijk iets verdachts tussen zit.

Kabelcommunicatie

Het gaat niet om een nieuwe wet, maar om een aanpassing van de bestaande Wet op Inlichtingen- en Veiligheidsdiensten. Die stamt nog uit 2002, en is dus grotendeels achterhaald. Een belangrijke term in de wet is 'aftappen van de kabel', een term die telkens terugkomt in discussies over het onderwerp. Er bestaat, kort door de bocht, twee soorten communicatie waar de AIVD inzicht in wil krijgen: Kabelgebonden communicatie, en niet-kabelgerichte communicatie. Als je belt met een mobiele telefoon, maakt die eerst via de ether verbinding met een zendmast. Dat is niet-kabelgerichte communicatie. Je kunt daarbij overigens ook denken aan satelliettelefonie (als je belt over langere afstanden) of radioverkeer. Vanaf de zendmast gaat de communicatie via de kabel. Daar valt daarnaast ook vaste verbindingen in huizen onder.

In de oude WiV mochten inlichtingendiensten (met name de AIVD en de MIVD) alleen de kabel aftappen met gerichte taps, dus specifiek op een verdachte. Dat is volgens minister Plasterk (Binnenlandse Zaken) niet genoeg. De communicatie moet in sommige gevallen namelijk ook ongericht worden onderschept. Daarbij kun je denken aan alle gebruikers van één specifieke app in een bepaalde wijk. De inlichtingendiensten willen vervolgens big-data-analyses loslaten op zulke communicatie, zodat er binnen die tap gezocht wordt op bijvoorbeeld sleutelwoorden of verdachte patronen (bijvoorbeeld herhaaldelijk contact met Syrische nummers). Omdat het niet gaat om een specifieke zoektocht naar één verdachte maar om een grote tap in de hoop verdachte patronen te vinden, noemen critici dat ook wel een sleepnet. Zoveel mogelijk uitgooien in de hoop iets te vangen tornt volgens hen aan het onschuldbeginsel omdat iedereen zo potentieel verdacht is én er geen echte reden is om een individu in de gaten te houden. Praktijkvoorbeelden

In de Memorie van Toelichting van de wet worden een aantal voorbeelden genoemd waarop de wet van toepassing kan zijn. Plasterk noemt het aftappen 'onderzoeksgerichte interceptie', en dat is volgens de minister de kern van de wet. Inlichtingendiensten mogen niet 'zomaar' iedereen afluisteren - daar moet wel een goede reden voor zijn.

Maar vorig jaar onthulde de NOS al een ander beeld. In een vertrouwelijke memo schreef Plaster dat het bijvoorbeeld mogelijk moet zijn 'om alle 400.000 inwoners van een [fictieve] stad te volgen als zij communiceren met een specifieke chatdienst'. Tijdens het debat van deze week noemde Plasterk het voorbeeld dat 'alle communicatie tussen Nederlandse en Syrische nummers' kan worden onderschept.

De AIVD en MIVD krijgen daarnaast nog meer bevoegdheden. Zo moeten straks 'providers van allerlei soorten communicatiediensten' verplicht meewerken aan dataverzoeken, waar dat vroeger nog 'openbare telecomnetwerken' waren. Nog een controversiële beslissing is dat de inlichtingendiensten straks 'via-via' mogen hacken. Dat betekent dat niet persé de verdachte kan worden gehackt, maar ook andere personen die verbonden zijn aan een verdachte om zo toegang tot het verdachte systeem te krijgen. Ook kan het gaan om het hacken van een router om zo in een computer van een verdachte te komen.

Tot slot mag de AIVD onder de nieuwe wet makkelijker gegevens uitwisselen met buitenlandse diensten, maar alleen 'als die rechtmatig zijn verkregen'. Daarvoor worden twee toezichtscommissies opgezet.

Nederlandse banken voeren dit jaar naam/ nummercontrole in tegen fraude

Rabobank heeft een systeem ontwikkeld dat bij een overboeking controleert of de ingevulde naam overeenkomt met de daadwerkelijke rekeninghouder. De bank voert de controle in het voorjaar in en andere banken volgen daarna.

Rabobank noemt het systeem IBAN-Naam Check en implementeert de functionaliteit in zijn app en website vanaf dit voorjaar. Klanten worden geïnformeerd als de naamcheck actief is. De bank gaat het systeem beschikbaar stellen aan andere Nederlandse banken, maar wanneer die het invoeren is nog niet bekend.

Als een klant bij een overschrijving een naam en rekeningnummer invult, wordt gecontroleerd of de ingevulde naam overeenkomt met de naam die bij de bank bekend is. Wijkt de naam een klein beetje af, dan wordt er een suggestie voor de juiste naam weergegeven. Als de ingevulde naam duidelijk anders is, of als een rekeningnummer bijvoorbeeld aan een persoon toebehoort, terwijl de klant een naam van een instantie invult, dan komt er een waarschuwing in beeld. Het systeem werkt alleen bij Nederlandse ibans. Bij overboekingen naar buitenlandse ibans komt er een melding in beeld dat de naam niet gecontroleerd kan worden.

ING had in het verleden al een vergelijkbare functionaliteit, waarbij gebruikers bij een overschrijving de naam van de begunstigde te zien kregen, als die bekend was bij de bank. Na de invoering van iban verdween die functionaliteit.

Tros Opgelicht en de Consumentenbond zetten sinds vorig jaar druk op de banken en de politiek om een naamcheck in te voeren om fraude tegen te gaan. Een petitie leverde in september bijna 40.000 handtekeningen op. Herhaaldelijk vertelde de Betaalvereniging Nederland in uitzendingen van Opgelicht dat de invoering van zo'n systeem ingewikkeld zou zijn en veel geld zou kosten. In de uitzending van dinsdagavond vertelt de woordvoerder dat het systeem er nu toch komt, dankzij een eigen 'innovatieprogramma' van Rabobank.

Bron: Banken.nl

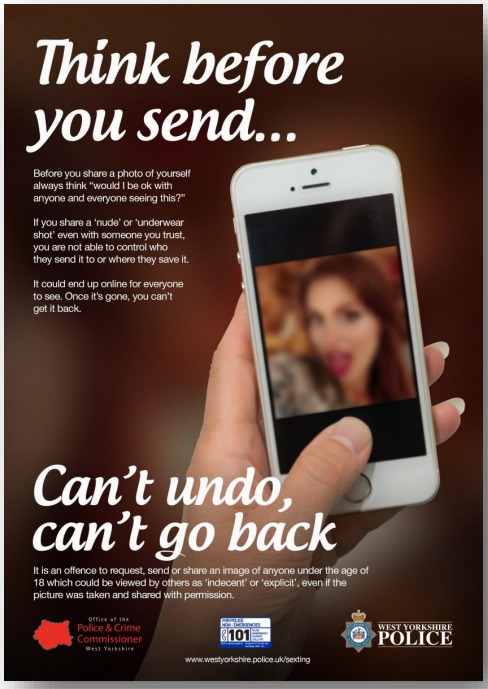
Marktplaats “lijkt wel een vrijplaats voor dieven, helers en andere kruimelaars”

‘Marktplaats weet wie de dief is, de politie weet wie de dief is, de ING weet wie de dief is, maar kennelijk heeft niemand de puf om de dief te vangen en tot de orde te roepen’, schrijft columnist Max Pam in De Volkskrant, naar aanleiding van een gevalletje oplichting van zijn zoon.

Die kocht op Marktplaats een dure trui, betaalde 250 euro aan ene ‘Ricardo de Vries’, maar kreeg natuurlijk geen trui. Aangifte bij politie én Marktplaats leverde niks op. Behalve een mail van Marktplaats-medewerker ‘Hannah’ die zoonlief ‘ondanks deze nare ervaring toch een fijne avond toewenste’.

Toen later bleek dat de account van die Ricardo niet eens geblokkeerd werd, kreeg Pam weer een mail: Marktplaats had besloten Ricardo ‘een tweede kans’ te geven. Wat bij Pam het vermoeden versterkte dat Marktplaats feitelijk een ‘vrijplaats is voor dieven, helers en andere kruimelaars’. Hoe moeilijk kan het zijn om die Ricardo op te sporen, vraagt hij in de column, als iedereen weet wie hij is. ‘Er is een banknummer waarnaar mijn zoon het geld heeft overgemaakt’. Maar ja, privacy he.

1 op de 15 jongeren online uit de kleren



Met sexting op zich is niet veel mis, maar met het delen van die foto’s natuurlijk wel.

Nieuw onderzoek van Bureau Jeugd en Media leert dat één op de vijftien jongeren (12-17 jaar) wel eens een pikante foto van zichzelf naar iemand anders heeft gestuurd. Een kwart van de jongeren zegt wel eens iemands blootfoto te hebben gekregen. Van de 16-17 jarigen kreeg 40% wel eens de vraag of zo’n foto van zichzelf te maken; een op de zeven deed dat ook.

Meisjes doen het vaker dan jongens, waar ‘dick pics’ overigens ook veel voorkomen. ‘Regelmatig’ worden de foto’s ook gestuurd naar onbekenden, vaak met vervelende gevolgen. ‘Binnen no time gaat zo’n foto door de hele school heen’, zegt Justine Pardoen van Bureau Jeugd & Media. Volgens Pardoen delen veel jongeren de foto’s zonder na te denken over de gevolgen.

Ze pleit voor meer voorlichting: vertel jongeren over de gevolgen. Snapchat en Whatsapp zijn de populairste apps om foto’s te delen.

Bron:

Politie start opsporing verdachten met gezichtsherkenning

De politie is begonnen met het opsporen van verdachten door gezichtsherkenning. Gezichten van verdachten kunnen worden vergeleken met die van bekenden van de politie.

Wanneer rechercheurs een verdachte op een foto of filmpje willen identificeren, kunnen ze de foto door grote databases met gezichten halen. Is de persoon op die foto aanwezig in de database, dan wordt er alarm geslagen.

Op dit moment staan er ruim 800.000 gezichten in die databanken: veroordeelde misdadigers, maar ook verdachten die nog niet zijn veroordeeld. "Je komt erin terecht als je wordt gearresteerd voor een misdrijf waar minimaal een jaar cel op staat", zegt John Riemen van de politie, die het project leidt. Bij arrestatie wordt dan een foto gemaakt.

Verdachten die onschuldig blijken, moeten uit de database worden verwijderd. Hoe snel dat gebeurt, is onduidelijk. De politie ligt al jarenlang onder vuur omdat ze niet zorgvuldig omgaat met opgeslagen gegevens. Foto's van veroordeelden blijven veel langer staan: 20 tot 80 jaar, afhankelijk van het soort misdrijf.

Toestemming OM
Gezichten van verdachten kunnen ook worden vergeleken met die van asielzoekers, uitgeprocedeerden en aanvragers van een Nederlands visum. Daaronder zijn mensen die niets op hun kerfstok hebben; om foto's met deze 'vreemdelingendatabase' te vergelijken, is dan ook toestemming van het Openbaar Ministerie. De herkenningssoftware - door de politie 'Catch' genoemd - kan bijvoorbeeld worden gebruikt om mensen op beelden van beveiligingscamera's te herkennen. Ook als iemand bijvoorbeeld een mishandeling filmt en die beelden aanlevert aan de politie, kunnen die beelden worden gebruikt. Maar ook beelden van bodycams, waarmee agenten in toenemende mate worden uitgerust, zijn geschikt.

Perfect Forward Secrecy

Je hoort de laatste tijd steeds vaker over perfect forward secrecy. Dat is begrijpelijk, want het is een belangrijk wapen tegen massasurveillance. Gelukkig wordt deze manier van versleutelen door steeds meer websites ondersteund en gebruikt door chat-apps zoals Signal. Hoe werkt perfect forward secrecy eigenlijk en waarom is het zo belangrijk?

Encryptie zonder perfect forward secrecy

Als twee computers versleuteld met elkaar gegevens willen uitwisselen, hebben ze een encryptiesleutel nodig. De verzender gebruikt de encryptiesleutel om data te versleutelen en verstuurt die dan naar de ontvanger. De ontvanger gebruikt vervolgens dezelfde encryptiesleutel om die data weer te ontsleutelen.

Als je een website via een beveiligde HTTPS-verbinding bezoekt, wordt de communicatie tussen je browser en de webserver op dezelfde manier versleuteld. Je browser genereert een encryptiesleutel, die vervolgens door je browser en de webserver gebruikt worden.

De vraag is nu: hoe kan je browser die encryptiesleutel op een veilige manier naar de webserver sturen, zonder dat derden die encryptiesleutel bij het versturen kunnen onderscheppen?

Lees hier verder.....

“Buitenlandse hackers jagen op geheime regeringsstukken”

Volgens AIVD-directer Rob Bertholee zijn (vooral) Russische cybercriminelen druk bezig overheidssites te hacken, op zoek naar ‘verslagen uit de boezem van de regering’.

Bertholee zegt tegen EenVandaag dat er alleen al in het eerste halfjaar van 2016 ‘honderden keren’ is geprobeerd een Nederlandse website te hacken. Hij noemt het een gevaar voor de democratie ‘dat zij beïnvloeden hoe ons parlement zou kunnen werken, of hoe onze overheid beslissingen neemt’.

De aanvallen komen behalve uit Rusland ook uit China en Iran, maar het is zinloos om stappen te ondernemen tegen deze landen. ‘Het heeft weinig zin om in de richting van China of Rusland te zeggen dat je hebt gezien dat ze een aanval hebben gepleegd, want dat wordt ontkend en daarna is het verhaal afgelopen’.

Beelden dashcam steeds vaker als bewijsmidel gebruikt

Was het niet gefilmd, dat van die wegpiraat op de A2 die een andere automobilist de weg afsnijdt, dan had de politie veel meer moeite gehad om die wegpiraat te vinden.

Niet verwonderlijk is dat dashcam-beelden steeds vaker als bewijs gebruikt worden, schrijft het ED. Maar mogen al die beelden – alleen al bij YouTube zijn er 3,5 miljoen filmpjes met zoekterm dashcam – wel online?

Volgens een woordvoerster van het parket Centrale Verwerking Openbaar Ministerie kunnen deze camerabeelden ‘alleen dienen als ondersteunend bewijs’ en mogen alleen politie en OM de beelden vertonen. ‘Je mag dus geen eigen rechter spelen door ze zomaar op sociale media te zetten’, waarschuwt ze.

Maar ja, wat als dat filmpje op facebook naar duizenden anderen gaat? Volgens de wet is dat een inbreuk op de privacy. Privacywaakhond Privacy First pleit daarom voor slimme software in de camera’s waarmee kentekens en gezichten automatisch geblurd worden. ‘Zet er een beveiligingssleutel op. Heb je een aanrijding, dan kunnen verzekeraar, politie of jijzelf met die sleutel de kentekens altijd weer leesbaar maken’.

Bron: AVD / OM

Australische geheime dienst: Blokkeer Flash en advertenties

De Australische geheime dienst heeft internetgebruikers en organisaties die zich tegen malware en andere aanvallen willen beschermen opgeroepen om Adobe Flash Player, Java, macro's en advertenties te blokkeren. Al jaren geeft de Australian Signals Directorate's (ASD) beveiligingstips.

Daarbij werden er altijd vier essentiële beveiligingstips gegeven, namelijk het installeren van beveiligingsupdates voor besturingssystemen, het patchen van applicaties, het beperken van beheerdersrechten en het whitelisten van applicaties. Deze "Top 4 mitigation strategies" zijn nu met vier aanvullende tips uitgebreid, wat de "Essential Eight" beveiligingstips oplevert. Er wordt een onderscheid gemaakt in tips voor het voorkomen van malware en adviezen om incidenten te beperken en data te herstellen. Zo wordt aangeraden dagelijks back-ups van belangrijke data te maken en tweefactorauthenticatie in te schakelen.

Verder moeten macro's in Microsoft Office worden geblokkeerd, alsmede Adobe Flash Player, Oracle Java en advertenties in de browser. "Flash, Java en advertenties zijn al lange tijd populaire manieren om computers met malware te infecteren", zo verklaart de ASD. Volgens de geheime dienst is het voordeel van het gegeven beveiligingsadvies dat het voor elke organisatie kan worden aangepast, afhankelijk van het risicoprofiel en de dreiging waar men zich zorgen om maakt. Voordat organisaties de beveiligingsadviezen implementeren wordt dan ook aangeraden om eerst een "risk assessment" uit te laten voeren.

10 procent jongeren slachtoffer cybercrime

Van de jongeren is één op de tien weleens slachtoffer geweest van cybercrime en 52 procent durft dit niet met zekerheid te ontkennen. Dit blijkt uit onderzoek van colocatie-specialist BIT uit Ede. Daarnaast komt naar voren dat maar liefst 46 procent van de jongeren niet weet hoe zij hun privacy kunnen waarborgen op internet. Voor het onderzoek zijn 248 mensen tussen de 18 en 34 jaar met een kantoorbaan ondervraagd.

Daarnaast blijkt dat jonge werknemers in groten getale e-mails (67 procent) en bestanden (41 procent) van onbekende afzenders openen. Jongeren gaan er dan ook van uit dat zij een malafide e-mail direct herkennen (90 procent).

Tijd als excuus

Bij webwinkels is zo'n 40 procent van de jongeren bereid informatie te verstrekken die niet nodig is voor de verzending van artikelen. De reden hiervoor is dat zij geen tijd en zin hebben om de producten opnieuw te zoeken op een andere website. Tijd blijkt sowieso een issue te zijn voor jongeren. Zo voert 37 procent van hen alleen updates van het besturingssysteem uit wanneer daar tijd voor is en update 22 procent de virusscanner alleen als het uitkomt.

Ook op het gebied van wachtwoorden zijn jongeren laks, zo stelt BIT. Bijna de helft (45 procent) deelt hun wachtwoorden met een ander. Het merendeel (63 procent) gebruikt slechts één wachtwoord voor meerdere logins. Zo nu en dan worden er kleine variaties toegepast, als hoofdletters en cijfers (52 procent). Meer dan de helft van de jongeren verandert het wachtwoord minder dan één keer per jaar, waarvan 12 procent dit zelfs nooit doet.

Bron: ASD / BIT

De 5 tekenen van malware: zo ontdek je of je de dupe bent

Wie last heeft van malware op zijn pc is niet blij. Het kan de snelheid en functionaliteit van je computer ernstig belemmeren en voor een hoop problemen zorgen. Maar hoe ontdek je eigenlijk dat je last hebt van malware, zonder meteen een hele systeemscan uit te voeren?

De beste manier om te ontdekken of je malware hebt, is natuurlijk wel degelijk het uitvoeren van een systeembrede scan. Als het goed is doe je dat automatisch al, maar stel nu dat dat niet zo is, wat zijn dan de signalen die op malware wijzen?

Trage pc

Als je computer zomaar van de ene dag op de andere traag wordt, kan dit een teken zijn dat er malware op staat. Met name wanneer eenvoudige apps zoals bijvoorbeeld de rekenmachine plotseling heel langzaam geopend worden.

Malware kan namelijk op de achtergrond een heleboel rekenkracht opeisen, waardoor je computer geen systeembronnen meer over heeft voor jouw eigen taken.

Browser omgeleid

Je browser gaat er op de meest vreemde momenten vandoor naar een andere website. Bijvoorbeeld, je opent Google en je komt terecht op een site die je niet kent met een of andere onbekende zoekmachine met allerlei reclame. Ook dan weet je dat je last hebt van malware.

Wanneer er voortdurend pop-ups in beeld verschijnen, zélfs wanneer je geen enkele browsers open hebt staan, dan mag je ervanuit gaan dat je malware (of in ieder geval crapware) op je pc hebt staan. Ook hier is het de bedoeling om geld te verdienen doordat mensen op deze pop-ups klikken en naar websites gestuurd worden.

Onbekende software en processen

Er verschijnen voortdurend pop-ups met dreigende meldingen van beveiligingssoftware die je niet kent. Software die je vooral aanspoort om nu actie te ondernemen (want anders...). Angst is altijd een goede trigger om mensen minder na te laten denken. Voer zo snel mogelijk een scan uit als je last hebt van dit soort meldingen.

Als je in het taakbeheer van je besturingssysteem processen tegenkomt die je niet kent en die er normaal gesproken niet staan, kan dit een teken van malware zijn. Zoek op internet naar de naam van een dergelijk proces om te zien of het inderdaad om iets ongewensts gaat.

Tevens draaien dergelijk processen vaak constant, ook wanneer je zelf je computer niet gebruikt. Als je schijfactiviteit en dergelijke opmerkt terwijl er geen back-up of onderhoudsprocessen aan de gang zijn, is het een goed idee om op malware te controleren.

Vreemde posts op social media

Er verschijnen plotseling berichten op Twitter en Facebook vanuit jouw naam, die je helemaal niet hebt geplaatst. Dat er iets aan de hand is, dat is zeker en het is zaak om er zo snel mogelijk iets aan te doen, want vaak zorgen die berichten ervoor dat je anderen infecteert. Overigens hoeft het niet per definitie zo te zijn dat je malware op je pc hebt, het kan ook zijn dat je social media-account 'gewoon' gehackt is.

Hetzelfde geldt voor e-mailberichten en andere communicatietools. Krijgen mensen opeens vreemde mailtjes of berichtjes uit jouw naam? Het kan zijn dat je gehackt bent, of je hebt te maken met malware.

Bepaalde tools werken niet meer

Sommige malware zorgt ervoor dat je antivirusprogramma niet meer werkt, of dat bepaalde systeemtools niet geladen kunnen worden, zodat de malware lastiger te detecteren en te verwijderen is. Als je merkt dat dergelijke programma's niet naar behoren draaien kun je het beste op zoek gaan naar een alternatieve scanner om te kijken of je inderdaad met malware te maken hebt.

Hoe een digibeet uitgroeide tot een van de grootste online drugsverkopers

De Volkskrant volgt de rechtszaak tegen hoofdverdachte Jan P. (57, uit IJmuiden), een digibeet die met zijn internethandeltje in drugs begon toen zijn vrouw ziek werd. Een beetje googelen over dark web, tor-netwerken, encryptie, een mailaccount bij TorMail en een bij Silk Road – 'en hop, daar ging-ie'.

Verbluffend simpel was het. De pillen gingen eerst gewoon in een envelop, later in pakketjes. Twee jaar later was P. een van de grootste Nederlandse drugsverkopers op het dark web. Zijn webwinkel HollandOnline floreerde, net als de sites van twee medeverdachten die hem de drugs leverden: AlbertHeijn, AmsterdamUnited en TheHeineken.

Eind 2014 heeft P. pech: een agent ziet toevallig op de parking van Ikea dat plastic tassen uit een BMW in een Mercedes verdwijnen. De Mercedes wordt aangehouden, met een kofferbak vol xtc, amfetamine en lsd. P. bekent de drugshandel, bij zoeking wordt een plastic tas met vier ton in euro's in zijn woning gevonden.

Lees het hele verhaal hier. Marktplaats van de drugs

Signal introduceert versleutelde videogesprekken

De versleutelde chat-app Signal heeft een nieuwe feature toegevoegd waardoor gebruikers ook versleutelde videogesprekken kunnen houden. "Dit is een geheel nieuwe gespreksinfrastructuur voor Signal en zou ook de gesprekskwaliteit moeten verbeteren", zegt Moxie Marlinspike, de man achter Open Whisper Systems, de ontwikkelaar van Signal.

Volgens Marlinspike gaat het om een grote verbetering voor de chat-app, maar zal het in fases worden uitgerold om feedback van gebruikers met verschillende apparaten te verzamelen, voordat het standaard wordt ingeschakeld. Gebruikers die de functie willen testen moeten die eerst inschakelen voordat ze er gebruik van kunnen maken. Verder is aan de nieuwste iOS-versie van Signal een functie toegevoegd genaamd CallKit waarmee gesprekken met één tap direct vanaf een vergrendeld scherm kunnen worden beantwoord. De nieuwe Signal-versies zijn via de App Store en Google Play te downloaden.

Bron: De Volkskrant / Security.nl

Fortuinen gebouwd op schaamte

Waar hoofdstad Lagos in Nigeria al jarenlang het wereldwijde centrum is van alle 419-fraude, advanced fee fraud of hoe het ook heten mag, lijkt het Marokkaanse stadje Oued Zem dat te zijn voor afpersers die Skype en facebook inzetten voor sextortion.

De BBC omschrijft Oued Zem als 'de hoofdstad van de sextortion industrie'. Dagelijks zijn daar 'honderden' jonge mannen aan het werk. Met facebook, Skype en gejatte filmpjes van masturberende vrouwen.

De BBC verhaalt over 'Samir', een jonge Palestijn die wordt meegesleurd nadat hij via facebook bevriend was door een mooi jong meisje. Geen idee wie het precies is, maar Samir accepteert het verzoek. Met als gevolg dat hij een tijdje later de webcam aanzet om zijn piemel te laten zien en zelfs masturbeert voor het meisje. Niet verwonderlijk is even later het dreigement dat zijn filmpje op YouTube wordt gezet, en aan familie en vrienden wordt toegestuurd, als hij niet vijf mille in euro's betaalt.

Links naar de film verschijnen op Whatsapp – Samir vreest voor het ergste, maar bedenkt zich: niemand opent tegenwoordig nog een bestand dat door een vreemde gestuurd wordt. Bovendien, weet hij: wie betaalt, moet volgende week nog eens betalen. Hij schakelt daarom YouTube in en weet het filmpje offline te krijgen. De BBC vond later dat het '23-jarige meisje uit Libanon' waarmee Samir dacht te skypen, een jongen uit Oued Zem is. Eentje die, samen met vele anderen, dagenlang facebook afschuimt op zoek naar slachtoffers.

Als er één toehapt, een video call beantwoordt, wordt een filmpje van een masturberend meisje, volop te vinden op het net natuurlijk, afgespeeld. De jongens zijn zo bekend met de filmpjes dat ze op elk moment de juiste chatboodschappen kunnen intikken.

Een van de oplichters, de BBC noemt hem Omar, noemt het bij de opnames cruciaal dat zowel hoofd als genitaliën in beeld komen. Daarna is het simpel. 'Als we de opname hebben, zetten we die op YouTube en sturen we het slachtoffer een privémail. Dan begint de bedreiging'. Alles bij elkaar duurt het een uurtje, aldus Omar. 'We chatten twintig minuten, filmen twintig minuten en het bedreigen duurt ook twintig minuten'. En ze betalen bijna allemaal, verzekert hij.

Vooral slachtoffers uit Arabisch-sprekende landen, waar seks en schaamte dicht bij elkaar liggen. Dagopbrengst? Gemiddeld zo'n vijfhonderd dollar, een bedrag dat wordt bevestigd door de lokale exploitant van Western Union. Die zegt dat er soms wel tienduizend dollar op een dag door zijn handen gaat. Maar ook voor wie door het stadje (werkloosheid officieel 60%) loopt, is het duidelijk: Duitse auto's, Japanse motoren en veel café's waarachter tientallen mannen zitten te facebooken.

Huis kwijt door internet-truc

Vraag niet hoe het kan, maar zo'n twintig jaar na de eerste nep-mailtjes over gewonnen loterijen en erfenissen van onbekenden, is een echtpaar uit Duiven hun huis kwijtgeraakt aan Nigeriaanse oplichters.

Eduard (57) en zijn vrouw Kitty kregen februari 2015 zo'n mailtje. Over een 'ver familielid' die maar liefst 10,4 miljoen dollar voor hen had achtergelaten. Het (goed)gelovige stel betaalde direct 58 mille aan 'advocaatkosten' en leende uiteindelijk zelfs geld bij vrienden en familie. 'Van die tien miljoen kan ik iedereen met rente ruim terugbetalen', dacht Eduard nog. Tot ze eind 2016 hun huis moesten verkopen.

Ze vonden via de kerk onderdak in een woongemeenschap maar ook van daaruit bleef het stel er in geloven. 'Afgelopen week heb ik 10.400 euro betaald, ze beloofden me dat het de allerlaatste keer was'. Tja. In totaal raakte het echtpaar 137.897 euro kwijt. Het slachtoffer heeft samen met de pastoor inmiddels aangifte gedaan, de politie Limburg zegt de zaak te onderzoeken.

Maatschappij niet klaar voor digitale samenleving

De overheid, het bedrijfsleven en de maatschappelijke spelers zijn onvoldoende toegerust om onze fundamentele rechten te beschermen in de huidige gedigitaliseerde samenleving. Dat is de conclusie van een onderzoek van het Rathenau Instituut.

De onderzoekers stellen in het rapport 'Opwaarderen - Borgen van publieke waarden in de digitale samenleving' dat we onze apps, onze software en onze technologie wel regelmatig opgewaardeerd hebben, maar zijn vergeten om de maatschappij te updaten.

Het wordt volgens het Rathenau Instituut tijd om de invloed te onderkennen van digitalisering op de samenleving. Data en software beïnvloeden beslissingen en gedrag.

Nepnieuws speelt een rol bij verkiezingen. Platformen zoals Airbnb, Facebook en Uber verzamelen informatie over ons en beïnvloeden onze keuzes. Slimme speelgoedpoppen en smart-tv's luisteren met ons mee. Robots in de zorg roepen de vraag op of we recht hebben op menselijk contact. De virtuele en fysieke wereld raken volledig met elkaar verweven.

De verregaande digitalisering vraagt volgens het Rathenau Instituut om discussie over verantwoordelijkheden van overheid, bedrijven en maatschappelijke organisaties. Nu is het maatschappelijk debat nog vooral gericht op privacy en veiligheid. Er is veel minder aandacht voor andere publieke waarden die door digitalisering evengoed onder druk staan zoals gelijke behandeling, menselijke waardigheid en ongelijke machtsverhoudingen. Lees hier de samenvatting van het rapport.

Tweetrapsverificatie WhatsApp nu voor alle gebruikers

WhatsApp maakt tweetrapsauthenticatie mogelijk bij alle gebruikers. Het gaat om een opt-in die gebruikers moeten inschakelen via de instellingen, bij de optie Account.

Gebruikers hoeven alleen de code in te voeren als zij hun nummer verifiëren, bijvoorbeeld als zij een nieuwe telefoon in gebruik nemen.

De functie leunt op het instellen van een zelfgekozen code van zes cijfers in de instellingen. Vervolgens vraagt WhatsApp om de code als iemand probeert een account aan te maken of in te loggen met het telefoonnummer van die gebruiker, zegt WhatsApp.

De functie komt in de komende tijd geleidelijk aan beschikbaar voor alle 1,2 miljard gebruikers.

Om de passcode te kunnen resetten moeten gebruikers een e-mailadres opgeven; de dienst kan hier de resetcode naartoe sturen. Als de gebruiker de code is vergeten en geen e-mailadres heeft ingevoerd, kan hij een week lang niet meer inloggen bij WhatsApp. Daarna is dat wel mogelijk, maar maakt de dienst een nieuw account aan, zonder bijvoorbeeld toegang tot back-ups.

De functie zit al sinds vorig jaar in testversies van de chatapp.

Ruim 70% ouders bezorgd over online veiligheid kinderen

Uit recent onderzoek blijkt dat de meeste Nederlandse ouders zorgen maken over de veiligheid van hun kinderen op het internet. Bijna driekwart van de Nederlandse ouders (73 procent) maakt zich zorgen over de veiligheid van hun kinderen op het internet. Meer dan de helft is bezorgd dat hun kinderen mogelijk worden gepest of geïntimideerd (57 procent) of worden meegelokt door een vreemde (60 procent).

Blijkens de resultaten van de enquête, die is gehouden onder bijna 21.000 consumenten wereldwijd, denkt bijna de helft (48 procent) van de ouders dat hun kinderen tegenwoordig eerder online worden gepest dan op het schoolplein. Ook geeft driekwart van de ouders aan dat kinderen nu veel meer worden blootgesteld aan online gevaren dan vijf jaar geleden.

Naast cyberpesten maken ouders zich voornamelijk zorgen dat hun kinderen mogelijk:
• Schadelijke programma's of apps downloaden (43 procent)
• Te veel persoonlijke informatie aan vreemden geven (38 procent)
• Iets plaatsen wat in de toekomst van negatieve invloed kan zijn op banen of een studie (33 procent)

Verkiezingsuitslag eenvoudig te hacken

We gebruiken al jaren het rode potlood, maar achter de schermen worden alle stemmen geteld door software. En dat systeem is zo lek als een mandje, waardoor hackers de uitslag van de verkiezingen kunnen manipuleren. Dat stellen beveiligingsexperts en een hoogleraar tegen RTL Nieuws.

Toch wordt de uitslag van de Nederlandse verkiezingen sinds 2009 op deze kwetsbare software gebaseerd.

Als je in Nederland stemt dan worden stemmen met de hand geteld in het stembureau. De resultaten worden dan op een onbeveiligde usb-stick gezet en vanaf het gemeentelijk stembureau naar het hoofdkantoor van één van de twintig kiesringen gebracht. Vanuit daar komen alle usb-sticks uiteindelijk terecht bij het centraal stembureau.

"De Chinezen en Russen kunnen eenvoudig met de uitslag rommelen", zegt hacker Rop Gonggrijp, wiens onderzoek er tien jaar geleden voor zorgde dat de stemcomputer weer werd vervangen door het rode potlood. Volgens hem is de stemcomputer ingeruild voor een computer die stemmen telt.

Verouderd
De software is volgens beveiligingsonderzoeker Sijmen Ruwhof, die als ethisch hacker wordt ingehuurd door grote banken en overheidsinstanties om hun online beveiliging te testen, sterk verouderd en op allerlei punten lek.

"De gemiddelde iPad is beter beveiligd dan het Nederlandse verkiezingssysteem", aldus Ruwhof, die de software op verzoek van RTL Nieuws heeft onderzocht. Ruwhofs bevindingen zijn gecheckt door beveiligingsonderzoeker Ger Schinkel.

Herbert Bos, hoogleraar Systems & Network Security aan de Vrije Universiteit Amsterdam, is ook geschokt: "Als een student dit programma bij mij inlevert, krijg hij een hele dikke onvoldoende. Het is dramatisch."

Bron: Norton / RTL

Website toont 'verborgen' Facebook-gegevens

De site vraagt de gebruiker een Facebook-profiel in te voeren, waarna via verschillende links foto's, berichten en andere media van de persoon in kwestie op te zoeken zijn. Ook is te vinden wat het deze allemaal heeft 'geliket'.

Dat kan ook als deze eigenlijk niet direct voor de gebruiker bedoeld zijn. Hiervoor maakt StalkScan gebruik van de zoekmogelijkheden van Facebook, waarmee alle openbare of voor vrienden bedoelde content te vinden is.

De site is gemaakt door de Belgische ethische hacker Inti De Ceukelaire. Hij benadrukt dat de site geen beveiliging omzeilt, maar enkel al doorzoekbare berichten en media vindt. Het doel is volgens hem dan ook om aan te tonen dat veel mensen heel veel persoonlijke informatie online te grabbel gooien, ook als ze denken dat het in besloten kring blijft. Zo is een 'besloten' groep op Facebook ook te doorzoeken. Wie de deksel op de pot wil houden, moet een 'geheime' groep aanmaken.

FBI zoekt wereldwijd 123 vermeende cybercriminelen

De FBI zoekt wereldwijd 123 mensen die worden verdacht van het plegen van cybercrime. Dat maakte de Amerikaanse opsporingsdienst deze week tijdens de RSA Conferentie in San Francisco bekend. "Toen ik een week geleden keek waren het 123 individuen", aldus Steven Kelly, hoofd van de FBI-eenheid die de internationale bestrijding van cybercrime coördineert.

"Het is een gigantisch aantal. Het gaat om veel mensen die nog niet voor de rechter zijn gebracht omdat ze zich over de hele wereld bevinden. Ze bevinden zich in locaties waarmee we geen uitleveringsverdrag hebben en dat is een probleem", aldus Kelly. Hij waarschuwde dat het lastig wordt om huidige en toekomstige cybercriminelen af te schrikken als gezochte personen voortvluchtig weten te blijven.

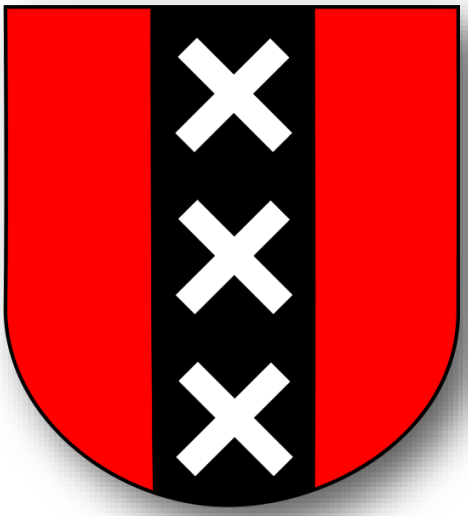
"Als we een aantal jaren aan een zaak werken en het voor de rechter weten te krijgen, maar de man of vrouw niet te pakken weten te krijgen, zal dat cybercrime niet afschrikken." Cybercriminelen blijven zodoende hun activiteiten in schuilhavens voortzetten. Met name op dit gebied probeert de FBI volgens Kelly zich te richten en de situatie te verbeteren, zo meldt IT News.

Bron: Facebook / FBI

Amsterdam pakt radicalisering online aan

Voorjaar 2017 wordt in Amsterdam een speciale app gelanceerd waarmee ambtenaren, professionals en 'sleutelfiguren uit de moslimwereld' informatie kunnen uitwisselen.

Hoewel de gemeente benadrukt 'geen rol [te hebben] bij online opsporing of inlichtingen heeft', gaat Amsterdam veel meer doen online: er komt een team dat kennis heeft van polarisatie, extremisme en radicalisering, "ambassadeurs' moeten online radicalisering gaan signaleren en jongeren aansporen 'kritisch na te denken' over extremistische boodschappen, er komt een stel vloggers die gematigde boodschappen moeten laten horen, en mogelijk een onlinehelpdesk voor jongeren die worstelen met radicalisering.



Verheerlijken terreur straks ook strafbaar

Het Europees Parlement heeft een 'antiterreurpakket' goedgekeurd waarin onder meer de strafbaarheid van het verheerlijken van terreur is opgenomen.

Lidstaten kunnen daarmee terreurgroepen of individuen aanpakken die boodschappen of beelden verspreiden om steun te werven voor de terroristische zaak. Wie terroristisch geweld verheerlijkt, bijvoorbeeld op sociale media, kan straks dus vervolgd worden.

Bron: Gemeente Amsterdam / EU

...verder op de website oa .....

- MINISTER WIL BEVEILIGDE VERBINDINGEN VERPLICHTEN VOOR OVERHEID
- CYBERPESTEN GESPREKSHANDLEIDING
- SIGNAL INTRODUCEERT VERSLEUTELDE VIDEOGESPREKKEN
- SYSTEEMBEHEERDERS DOELWIT GETROJANISEERDE BEHEERSOFTWARE
- MAAK WINDOWS 10 GEBRUIKSVRIENDELIJKER
- HOE PERFECT FORWARD SECRECY JOUW COMMUNICATIE VEILIG HOUDT !
- INTEL LANCEERT DASHBOARD MET INFORMATIE OVER CYBERDREIGINGEN

.... en meer .....

...verder op de Facebook pagina oa .....

- Los problemen met je harde schijf op met chkdsk
- Welke mobiele browser is de snelste?
- Het verschil tussen alle USB-types en -standaarden uitgelegd
- Herstel Windows met een usb-stick als live-medium
- Zo gebruik je de privémodus van je browser
- Optimaliseer de zoekfunctie van Windows 10
- Hoe start je Windows 10 op in veilige modus?
- 8 tips om je wifi te beveiligen
- Windows-problemen met professionele tools oplossen

.... en meer .....

Cops in cyberspace

Bij de politie Limburg is een agent op staande voet ontslagen omdat hij, tijdens het werk en in uniform, webcamseks had. De zaak werd geopenbaard door Peter R. de Vries die de beelden in handen kreeg en uiteindelijk de politie inlichtte. De agent had de webcamseks, via Skype, met een vrouw die hij op een datingsite had ontmoet. De vrouw, meerderjarig, zou op een gegeven moment tegen de man gezegd hebben dat ze 17 was, 'om te kijken wat hij zou doen'. Na verloop van tijd werden de chats seksueel; de agent masturbeerde in uniform op een politietoilet. Politiechef Gery Veldhuis spreekt van 'schandelijk gedrag'. Onduidelijk blijft waarom de vrouw zei dat ze minderjarig was.

———————————————————-

Met 'een geniale inval' heeft een Belgische agent een ontvoering in Australië weten op te lossen. In die zaak ging het om de vermiste Vlaamse vrouw Davine (24, uit Heule) die gegijzeld werd door een Australiër. Davine, dierenverzorgster, had zich op een lokale website aangeboden voor vakantiewerk. Eenmaal op de fruitplukkerij werd ze overmeester, opgesloten en verkracht. De vrouw wist echter vanaf een (kennelijk aanwezige) computer een privéberichtje via facebook te versturen naar een vriendin in België. Een lokale agent bedacht daarop om Davine een zogeheten silent message te sturen – een berichtje dat door de ontvanger niet gezien wordt. Maar het berichtje leverde wel het ip-adres op van de computer in de fruitplukkerij waar Davine werd vastgehouden. Dat leidde weer naar de gps-coördinaten, enfin, voldoende voor de Australische politie om de ontvoerder 'te klissen'.

————————————————————

De politie heeft een man (21, uit Epe) opgepakt die op het dark web een vuurwapen en handgranaten probeerde te kopen. De man had een wapenvergunning maar deze is direct ingenomen. In de woning van de verdachte werden onder meer gasdrukwapens, een airsoftwapen, munitie, een verzameling messen, ploertendoders en meerdere computers in beslag genomen. De aanhouding is volgens de landelijke eenheid het bewijs 'dat criminelen op het dark web niet zo anoniem zijn als ze mogelijk denken'. De verdachte is na verhoor vrijgelaten in afwachting van een beslissing van het OM.

———————————————————-

'Mijn zaken van deze week: verkrachting, verkrachting, inbraak, geweld, afpersing, geweld tegen politie, bedreigingen, drugs, inbraak, poging tot moord, verkrachting. De verdachten? Ali, Mohamed, Mahmod, Mohammed, Mohammed Ali, etcetera. Afkomstig uit? Irak, Irak, Turkije, Syrië, Somalië, Syrië, onbekend, onbekend, Zweden, Syrië, Irak'. Een Zweedse politieman, Peter Springare, schreef op facebook over de frustaties op zijn werk. 'Ik ben zo fucking moe. Wat ik hier zal schrijven, is niet politiek correct. Maar het kan me niet schelen'. Springare, 47 dienstjaren, liep (vlak voor zijn pensioen) helemaal leeg en zorgde voor veel opschudding toen hij schreef over criminaliteit en immigranten. Hij werd niet alleen beschuldigd van racisme maar ook gesteund door vele mensen, waaronder collega's van hem, die het wel stoer vonden dat 'eindelijk eens iemand de waarheid schreef'. Het bericht werd tienduizenden keren gedeeld en geliket en op Springares politiebureau in Örebro werden zestig boeketten bloemen bezorgd. Korpschef Dan Eliasson verklaarde dat het belangrijk is onderscheid te maken tussen wat een politiemens ín zijn werk doet en daarbuiten. 'Als hij in zijn vrije tijd wil praten over de problemen van immigranten, heeft hij recht van meningsuiting, zoals iedereen'. Springare is nuchter: 'als je dit probleem niet kunt bespreken zonder dat het over racisme gaat, hebben we een probleem'.

————————————————————

Een opmerkelijke vraag van de politie Enschede op facebook, als een vrouw is opgepakt die een jas heeft gestolen. 'Wat vinden jullie? Wat voor straf moet ze hiervoor krijgen. Gevangenisstraf, taakstraf of een geldboete?' Chef basisteam Arjan Derksen zegt hiervoor geen toestemming aan het OM gevraagd te hebben. 'Maar we hebben ook geen signalen ontvangen dat er bezwaren tegen zouden bestaan'. Van de (bijna 15 duizend) facebookvrienden reageerden er enkele honderden. De reacties, van boete tot stokslagen, waren nog redelijk genuanceerd. Opvallend is dat niemand pleit voor de maximale straf (vier jaar celstraf) bij dit soort delicten. Volgens Derksen was de achtergrond van deze 'volksraadpleging' de wens om burgers mee te nemen in de praktijk van het politiewerk. 'De vraagstelling was misschien wat scherp, maar dat hoort naar onze mening ook een beetje bij social media, toch?' Bovendien, schrijft Derksen, 'kunnen én willen we niet op de stoel van een Officier van Justitie of rechter [gaan] zitten'.

————————————————————

Op een speciale facebookpagina van de politie Limburg wil de eenheid meer aandacht geven aan cold cases. 'We proberen in deze tijd op zo veel mogelijk manieren mensen te bereiken voor deze zaken', zegt een woordvoerster. 'Daarom zoeken we naar nieuwe wegen om cold case-zaken opnieuw onder de aandacht van de bevolking te brengen'. De eerste zaak op de pagina is van Henri Nieboer, een man die in 2005 dood in zijn tuin werd aangetroffen.

————————————————————

Om af te rekenen met het 'asociale gedrag in het verkeer' moeten 'radicale maatregelen' genomen worden: alle auto's moeten worden uitgerust met ademslot, snelheidsbegrenzer én apparatuur die appen of mailen onder het rijden onmogelijk maakt. Volgens politiecommissaris Egbert-Jan van Hasselt, landelijk projectleider infrastructuur is 'alleen handhaven niet meer voldoende'. Van Hasselt wil 'gedrag aan de voorkant beïnvloeden', zei hij in het NOS Radio 1 Journaal. Hij vindt een medestander in landelijk verkeersofficier Achilles Damen. 'Alle technische hulpmiddelen die het veiliger kunnen maken en die helpen het aantal slachtoffers terug te dringen vind ik de moeite waard'.

————————————————————

Rechtspraak

Vermoedelijk de oudste persoon die in Nederland ooit terechtstond in een zaak waarin facebook een rol speelt, is de man (72, uit Nieuwegein) die deze week door de rechtbank in Arnhem werd veroordeeld tot vijf jaar celstraf voor poging tot moord op een ex-vriendin (ook 72). Die had hem kort daarvoor verlaten maar ze schreven elkaar nog wel berichtjes via facebook. Over een zo'n bericht werd de man zo kwaad dat hij niet kon slapen en, toen hij een mes zag, midden in de nacht naar die vrouw toe reed en haar probeerde te steken. De vrouw wist het mes af te pakken maar raakte licht gewond aan hoofd, lichaam en hand. Hoewel de man verklaarde zijn ex alleen maar bang te willen maken, vond de rechtbank voorbedachte rade bewezen. De verdachte, tegen wie het OM zes jaar had geëist, kreeg verder een contact- en locatieverbod en moet zijn ex een schadevergoeding betalen.

———————————————————-

De rechtbank Oost-Brabant heeft deze week een man (56, uit Someren) veroordeeld tot honderd uur taakstraf (de helft voorwaardelijk) voor het stalken van een (destijds) 13-jarig meisje. De man dacht dat het meisje in hem geïnteresseerd was en begon haar te filmen, vanuit zijn woning, als ze voorbij liep of fietste. Op internet zocht de man welke locaties en evenementen ze bezocht, hing kadootjes aan haar fiets, bezocht haar voetbalwedstrijden etcetera. Vanaf september 2013 Whatsappte hij zelfs een vriendinnetje van het meisje. De rechtbank vindt dat de man 'met zijn gedrag de grenzen van het maatschappelijk betamelijke in aanzienlijke mate' heeft overschreden, ook al stopte hij in 2014 met de belaging. Een bijzondere voorwaarde bij de straf is een contactverbod met het meisje.

———————————————————-

De rechtbank in Almelo heeft een man (26) tot 42 maanden celstraf plus
tbs veroordeeld voor verkrachting, aanranding en ontucht met minderjarige meisjes. De verdachte benaderde de meisjes, tussen 12 en 16 jaar, via internet waar hij zogenaamd Spaans was en 17 jaar. Tijdens afspraakjes met de meisjes had hij seks met ze, soms onder dwang. De verdachte, die tijdens de zitting de feiten bekende, werd in het verleden al eens tot vier jaar celstraf veroordeeld voor soortgelijke feiten. Hij zat nog in zijn proeftijd toen hij in deze zaak in de fout ging.

———————————————————-

Honderden politiecamera's die in Washington DC zouden worden gebruikt bij de inauguratie van Donald Trump hebben geen beelden kunnen doorzenden omdat ze besmet waren met ransomware. Hackers hadden 123 van de 187 beschikbare netwerkvideorecorders geïnfecteerd die werden gebruikt voor het opslaan van beelden. De gemeente Washington weigerde te betalen. Alle software werd opnieuw geïnstalleerd waarna het systeem weer geactiveerd werd. Ransomware leidde in ander deel van de VS tot verlies van bewijsmateriaal. Het Cockrell Hill Police Department verloor documenten, bodycambeelden, foto's, surveillancevideo's en vanuit de auto genomen beelden toen een server besmet raakte toen een agent een besmette bijlage opende. Ook hier werd niet betaald. Wel werd de hele server gewist waardoor bewijs verloren ging – de backups waren gemaakt ná de infectie.

———————————————————-

De rechtbank in Den Haag heeft een man (61, uit Zoetermeer) veroordeeld tot anderhalf jaar celstraf (een half jaar voorwaardelijk) voor bezit en verspreiding van kinderporno. De straf is conform de eis van het OM dat sprak van een 'buitengewoon schokkende' collectie, met onder meer babyfoto's. De advocaat van de verdachte had een werkstraf gevraagd maar de rechtbank 'had geen genade' met de verdachte. Die bleek drie jaar lang materiaal uitgewisseld te hebben. Via Skype en in chatrooms had hij zijn medegluurders gevonden 'en van het een kwam het ander', aldus de verdachte in een verklaring. De rechter sprak van 'het ergste wat er is' en nam de eis van de officier over.

———————————————————-

De politierechter in Almelo heeft een man (35, uit Rotterdam) 750 euro boete opgelegd voor een facebookbericht waarin de man bedreigingen uitte richting burgemeester Onno Veldhuizen van de gemeente Enschede. 'Hier staat maar 1 straf op. De Kogel', schreef de man bij een foto van de viering van 400 jaar betrekkingen tussen Nederland en Turkije waar Veldhuizen aanwezig was. 'In 1945 stonden al die landverraders tegen de muur', schreef de verdachte verder. Volgens de man was dat een impulsieve daad en heeft hij spijt. De rechter noemde de uitlatingen echter onaanvaardbaar. Wel kreeg de man een lagere straf dan in vergelijkbare zaken. Zo kreeg de man die D66-leider Pechtold bedreigde onlangs een week onvoorwaardelijk en werden in andere zaken vaak werkstraffen (zestig uur) opgelegd.

———————————————————-

Een moeder (48, uit Bleskensgraaf) is tot twee jaar celstraf (acht maanden voorwaardelijk) veroordeeld voor het misbruik van haar eigen zoon ten gerieve van haar chatvriend. De vrouw maakte opnames van de seks om chatvriend 'Faam' te behagen. Deze onbekend gebleven man (?) gaf haar online opdrachten. Bij de rechtbank verklaarde de vrouw dat ze van 'Faam' eerst seks met haar puberdochter moest hebben, maar die 'gooide gewoon de deur voor me dicht'. Bij haar zoontje, nog niet tegen zijn moeder opgewassen, ging het beter – de jongen noemde 'Faam' zelfs 'zijn vriend'. De politie kwam op het spoor van de ontucht toen een vriendinnetje van de dochter per ongeluk de beelden zag. Dat vriendinnetje lichtte haar moeder in die de politie inschakelde. De twee kinderen van de verdachte vrouw zijn uit huis geplaatst, de moeder krijgt steun via haar dominee en moet van de rechtbank verplicht in therapie. Chatvriend 'Faam' is nooit gevonden …

———————————————————-

Verschijningsvorm cybercrime	138ab *lid 1*	138ab *lid 2*	138ab *lid 3*	138b	139c *lid 1*	139d	139e	161 *sexies*	161 *septies*	350a *lid 1*	350a *lid 2*	350a *lid 3*	350b *lid1*	350b *lid2*
● Malware														
Malware maken en/of verspreiden	X					X		X	X	X	X	X	X	X
Malware (Trojaanse paarden) gebruiken	X	X			X			X	X	X	X	X	X	
● Computerinbraak														
Computerinbraak (hacking)	X		X								X			
Computerinbraak vervolg-handelingen		X	X		X	X	X	X	X	X	X	X		
Portscan						X								
Spoofing/cache poisoning	X	X		X	X	X	X	X		X	X			
Sniffing					X	X	X			X				
Draadloze netwerken hacken/ misbruiken	X	X	X	X	X		X	X		X	X			
Password guessing	X			X		X								
● Website aanvallen														
Veroorzaken open relay									X				X	
Wederrechtelijk open relay gebruiken	X							X		X				
Defacing/vernielen website	X							X	X	X			X	
Defacing/doorleiden internet-verkeer	X							X	X	X				
Cross-site scripting	X	X			X	X	X	X		X			X	
SQL-injecties	X	X						X		X				
● Botnets														
Botnet bouwen en beheren	X	X	X		X					X		X		
● Denial of Service														
DDoS-aanval				X				X		X			X	
● Social Engineering														
Phishing		X			X		X							
Vishing/Smishing		X			X									
● E-mail gerelateerd														
Wederrechtelijk open mail relay gebruiken	X							X	X	X				
Spamming (met DoS tot gevolg)				X				X	X				X	

Bron: Overheid.nl

Wetsartikel

Art. 138ab, lid 1 Sr Hacken: opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk

Art. 138ab, lid 2 Sr Hacken: overnemen, aftappen of opnemen van gegevens uit een geautomatiseerd werk na binnendringen daarvan

Art. 138ab, lid 3 Sr Hacken door tussenkomst van een openbaar telecommunicatienetwerk

Art. 138b Sr Het belemmeren van toegang tot of gebruik van een geautomatiseerd werk

Art. 139c Sr Het aftappen of opnemen van gegevens (afluisteren)

Art. 139d, lid 1 Sr Plaatsen van opname-, aftap- of afluisterapparatuur; voorbereidingshandelingen

Art. 139d, lid 2 Sr Het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen of toegangscodes bedoeld om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen

Art. 139d, lid 3 Sr Zoals in art. 139d, lid 2 Sr, maar met oogmerk gericht op art. 138ab, lid 2 en 3 Sr

Art. 139e Sr Het bezit en verspreiden van gegevens of een voorwerp waarop gegevens staan die door wederrechtelijk aftappen of opnemen zijn verkregen

Art. 161sexies Sr Opzettelijk vernielen etc. van een geautomatiseerd werk of werk voor telecommunicatie; voorbereidingshandelingen

Art. 161septies Sr Vernieling etc. van een geautomatiseerd werk of werk voor telecommunicatie door schuld

Art. 231b Sr Identiteitsfraude

Art. 232 Sr Opzettelijk valselijk opmaken, vervalsen, gebruiken, etc. van betaalpas, waardekaart e.d.

Art. 240b Sr Kinderpornografie

Art. 248e Sr Grooming

Art. 273, lid 2 Sr Bekendmaking bedrijfsgeheimen; heling computergegevens ondernemingen

Art. 273d Sr Schending telecommunicatiegeheim

Art. 317, lid 2 Sr Afpersing door de bedreiging dat gegevens opgeslagen door een geautomatiseerd werk onbruikbaar, ontoegankelijk of gewist worden

Art. 326c Sr Het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen

Art. 350a, lid 1 Sr Opzettelijke vernieling van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350a, lid 2 Sr Het feit gepleegd in lid 1 met tussenkomst van een openbaar telecommunicatienetwerk

Art. 350a, lid 3 Sr Opzettelijk gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Art. 350b, lid 1 Sr Vernieling door schuld van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350b, lid 2 Sr Door schuld gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Video

Tek Tok Late Night:

1. Privacy
2. Internetvrijheid
3. Digitale veiligheid
4. High Tech Crime
5. Data in onderwijs
6. Cybersurveillance
7. Techtrends in onderwijs
8. Veilig internetten
9. MKB cyber secure
10. Cyberellende bij Tek Tok
11. Standaarden en keurmerken
12. Operation Hijg Tech Crime
13. Kraak van de Maand

You Tube:

Doe jij het veilig online
Malware
WiFi ontvangst verbeteren
Internetfraude via de telefoon
Documentaire: Veiligheid en privacy
Herken een nep-hotspot
Gebruik wachtzinnen
Drive-by-downloads voorkomen
Hoe herken je een phishing mail
Beveiligd internetbankieren
Privacy—ik heb toch niets te verbergen
Webinar Computercriminaliteit
Mousejack
Gegijzeld door Ransomware. Wat nu?
Telefonische phishing

Help wanted:

Grooming
Sexting
Webcammisbruik
Bedreigd/gechanteerd
Kinderporno
Nepprofiel

Handig

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

Tips voor veilig handelen op Marktplaats

Internetoplichting: controleer vooraf de (bank)gegevens van de verkoper via

www.mijnpolitie.nl/miocheck

Komt de verkoper voor op de website Opgelet op internet ?

Malware ID website met info omtrent verwijderen van infecties

PCrisk verwijderingsrichtlijnen voor spyware en virussen

Cookie Verwijderen kennisdatabase voor het verwijderen van adware, hijackers, ransomware, toolbars en pop-ups

Computer woordenboek

Secure Computing Naslag

Veel meer handige tips vindt u op de Secure Computing website.