Secure Computing

Februari 2016 JAARGANG 5

Veel lees(r)plezier

(NB: met Ctrl+ scrolwieltje kunt u de pagina vergroten en

W.Bosgra Taakaccenthouder Digitale Criminaliteit Basisteam Enschede

Secure Computing

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 oa:

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

Het kabinet wil cybercriminaliteit bestrijden. Zo moeten politie en justitie meer bevoegdheden krijgen om cybercrime aan te pakken en komen er hogere straffen voor cybercriminaliteit.

Cybercrime bestrijden

Meer bevoegdheden voor overheid bij aanpak cybercrime

De overheid krijgt meer bevoegdheden om cybercrime aan te pakken. Zo is er een wetsvoorstel voor de bestrijding van cybercrime van het ministerie van Veiligheid en Justitie in de maak dat politie en justitie de volgende mogelijkheden moet geven:

- helers van (digitale) gegevens arresteren;
- op afstand onderzoek laten doen in computers van criminelen of hierin binnendringen;

gegevens overnemen of ontoegankelijk maken (bijvoorbeeld kinderporno of e-mailberichten met informatie over misdrijven).

Hogere straffen voor cybercriminaliteit

Per 1 juli 2015 gelden hogere straffen voor cybercriminaliteit. Op die datum is de Wet voor de implementatie van een Europese richtlijn over aanvallen op informatiesystemen in werking getreden. Het gaat om de volgende straffen:

- Criminelen die computergegevens vernielen, kunnen een gevangenisstraf van maximaal 2 jaar krijgen. Dat was 1 jaar.
- Personen die computersystemen ontoegankelijk maken, kunnen ook een gevangenisstraf van maximaal 2 jaar krijgen. Bijvoorbeeld al zij aan

wachtwoorden sleutelen of computers bestoken met spam zodat de boel vastloopt.

- Computercriminelen die delicten plegen met behulp van een zogeheten botnet, kunnen maximaal 3 jaar gevangenisstraf krijgen.

Brengt een computerdelict ernstige schade toe of richt het zich tegen een vitale infrastructuur? Dan wordt de maximale gevangenisstraf 5 jaar. Voorbeelden van vitale infrastructuren zijn een overheidsnetwerk of energiecentrale.

Meldplicht bij ICT-inbreuken

Organisaties in de zogenaamde vitale sectoren moeten in de toekomst verplicht melding maken van digitale veiligheidsincidenten (ICT-inbreuken). Dit staat in een wetsvoorstel gegevensverwerking en meldplicht cybersecurity van het ministerie van Veiligheid en Justitie. Het gaat om organisaties in de volgende sectoren:

elektriciteit;

gas;

drinkwater;

telecom;

keren en beheren oppervlaktewater;

transport (mainports Rotterdam en Schiphol);

financiën;

(rijks)overheid.

De organisaties moeten ICT-inbreuken melden bij het NCSC. Dit moet alleen als door de inbreuk de beschikbaarheid of betrouwbaarheid van de producten of diensten in gevaar komt. Door de wettelijke meldplicht van ICT-inbreuken kan het NCSC de risico's voor de samenleving inschatten en hulp verlenen aan de getroffen organisatie. Daarnaast kan het NCSC hierdoor andere organisaties in de vitale sectoren zo nodig waarschuwen en adviseren.

Bron: Rijksoverheid

Index

Politie werkt nog met te oude systemen.

Politie moet nog steeds met oude ict-systemen werken

Ondanks herhaalde beloftes van minister Ard van der Steur van Justitie en Veiligheid werkt de politie nog steeds met oude ict-systemen, wat invloed op de opsporing van verdachten heeft. Dat meldt de Volkskrant. De ict-systemen zouden gelijktijdig met de reorganisatie van 26 korpsen tot één nationale politie worden vernieuwd. Ondanks toezeggingen worden de ict-vernieuwingen al twee jaar niet nagekomen.

Volgens de Volkskrant staan de huidige politiesystemen als verouderd en kwetsbaar te boek. In plaats van ze te vernieuwen worden ze steeds opgelapt, wat tegen de afspraken is. De vernieuwing van de systemen loopt inmiddels 30 procent achter op schema. Daardoor zouden wetsovertreders minder efficiënt worden opgespoord. Het gaat dan onder andere om de analyse van digitale data voor het vervolgen van cybercriminelen, maar ook op de grootschalige registratie van vreemdelingen zijn de systemen niet berekend. Het ministerie van Justitie laat weten dat de politie meer tijd nodig heeft om de ict-vernieuwing te realiseren.

Het Aanvalsprogramma Informatievoorziening Politie werd met veel bombarie gepresenteerd en moest de ICT-organisatie weer helemaal up-to-date brengen. Maar al een half jaar nadat het programma van start was gegaan, werden al de eerste knelpunten gesignaleerd door de toezichthoudende Review Board.

De bemerkingen van die onafhankelijke commissie van experts kostte toenmalige Politie CIO Ad Meijboom de kop. Hij nam ontslag nadat er grote kritiek was ontstaan op de aansturing van dat Aanvalsplan.

Inmiddels hebben de twee vervangers van Meijboom, de interim managers Pieter Cloo en Jo van den Hanenberg van bureau Boer & Croon, het Aanvalsplan bijgesteld. Temporiseren, is het sleutelwoord. Al te ambitieuze projecten worden uitgesteld of geschrapt. De nadruk ligt op het in de lucht houden van de ICT en vandaar uit verbeteringen aanbrengen. Het risicomanagement wordt verzwaard: ieder project krijgt een risicoparagraaf, risico's worden gemonitord en daarover wordt gerapporteerd aan de CIO's.

Een van de redenen om projecten uit te smeren over langere tijd, uit te stellen of geheel te schrappen is simpelweg het ontbreken van de mankracht om ze uit te voeren. Daarom is nu een prioriteitenlijstje gemaakt. Daarnaast wordt er in de politieorganisatie beter gekeken welke kennis en kunde beschikbaar is. Het project- en programmamanagement wordt strakker geregeld. Dat was kwantitatief en kwalitatief ontoereikend en er ontbrak “integrale verantwoordelijkheid" waardoor er “geen sturing plaatsvindt op het totale proces van begin tot eind waardoor verstoringen en vertragingen eerder regel dan uitzondering zijn. Er kan niet proactief worden gehandeld."

Het gevolg daarvan is dat bepaalde lopende projecten stilgelegd of getemporiseerd moeten worden. Op een later moment wordt heroverwogen wanneer deze projecten wel kunnen worden uitgevoerd. “Het stilleggen of temporiseren van projecten brengt mogelijke projectverliezen met zich mee. Met het stilleggen (en het op een later moment voortzetten) van projecten zijn mogelijk afbouw- en (her)opstartkosten gemoeid", schrijven de CIO's. Er wordt nog een inventarisatie van die kosten gemaakt.

Met het uitstel en afstel van projecten moet de ICT-dienstlening van de politie beter de kans krijgen “gestabiliseerd" worden. Daarvoor is vtsPN verantwoordelijk, de voorziening tot samenwerking Politie Nederland. Zo

Bron: webWereld / Volkskrant

Index

De wet computercriminaliteit III die de politie extra bevoegdheden geeft is noodzakelijk.

OM: wet computercriminaliteit nodig voor opsporen

De wet computercriminaliteit III die de politie extra bevoegdheden geeft, zoals het binnendringen op de computers van verdachten, is noodzakelijk om de opsporing en vervolging van cybercriminelen te versterken, zeker nu er steeds vaker encryptie wordt gebruikt, zo beweert het Openbaar Ministerie.

Volgens het OM hebben ook criminelen toegang tot steeds meer en verder ontwikkelde digitale middelen en technieken. "Ze gebruiken onder meer encryptie om bestanden te beveiligen, beveiligde communicatiediensten, zoals Whatsapp, Skype en Viber en Telegram, anonieme hotspots en cloudcomputingdiensten", zo stelt de organisatie. "Daarmee proberen ze hun criminele activiteiten te verhullen en uit handen te blijven van Openbaar Ministerie en politie."

Top 10-

Het OM stelt vervolgens dat Nederland in de top 10 van landen ter wereld staat met de meeste cyberaanvallen, hoewel een bron hiervoor niet wordt vermeld. Dit zou aan de Nederlandse internetinfrastructuur te danken zijn. De snelle, goedkope en stabiele verbindingen zouden Nederland aantrekkelijk voor cybercriminelen maken, die servers bij Nederlandse hostingpartijen voor illegale praktijken gebruiken.

Encryptie

De huidige bevoegdheden van OM en politie zouden gezien de technologische ontwikkelingen echter tekort schieten. Daarbij wordt vooral naar het gebruik van encryptie gewezen. De huidige strafvorderlijke bevoegdheden zijn vooral gericht op communicatie die te onderscheppen is. Zoals het plaatsen van een tap of het onderzoeken van al in beslag genomen gegevensdragers.

"Voor de niet te kraken gegevens en de huidige -en in de toekomst steeds meer te verwachten - ongrijpbare (gecrypte) communicatie, bieden de bestaande bevoegdheden van opsporingsambtenaren onvoldoende soelaas", zo claimt het Openbaar Ministerie. "Het OM acht het om die reden noodzakelijk dat de wet computercriminaliteit III wordt aangenomen en ingevoerd, om de opsporing en vervolging van (computer)criminelen te verbeteren en te versterken." De wet computercriminaliteit moet zowel nog door de Eerste als Tweede Kamer worden behandeld.

Bron: Security.nl

Index

Cameratoezicht steeds vaker ingezet door organisaties.

Toezichthouder publiceert regels voor cameratoezicht

De Autoriteit Persoonsgegevens heeft vandaag de regels gepubliceerd voor organisaties die cameratoezicht willen inzetten. Volgens de toezichthouder komt het steeds vaker voor dat cameratoezicht door organisaties wordt ingezet.

Tevens worden de technische mogelijkheden van camera's geavanceerder, bijvoorbeeld op het gebied van gezichtsherkenning. "Wij krijgen jaarlijks honderden vragen en tips over cameratoezicht", zegt Wilbert Tomesen, vicevoorzitter van de Autoriteit Persoonsgegevens. "Deze vragen én alle nieuwe toepassingen en mogelijkheden zijn voor ons reden om beleidsregels uit te brengen die organisaties helpen bij de vraag of de inzet van een camera is toegestaan."

Tomesen merkt op dat cameratoezicht een belangrijk middel kan zijn om bijvoorbeeld eigendommen te beschermen of de openbare orde te handhaven. "Maar cameratoezicht betekent ook een inbreuk op de persoonlijke levenssfeer van betrokkenen. Deze inbreuk kan groot zijn, zeker als mensen niet weten dat ze worden gefilmd en zich onbespied wanen".

Noodzakelijk

De gepubliceerde beleidsregels zijn uitwerkingen van de belangrijkste bepalingen uit de Wet bescherming persoonsgegevens (Wbp) en Wet politiegegevens (Wpg) die gelden voor de verwerking van persoonsgegevens door middel van een camera. Zo moet de inzet van een camera noodzakelijk zijn om de gestelde doelen te bereiken, moeten mensen worden geïnformeerd dat er cameratoezicht is vóórdat zij worden gefilmd en moeten de beelden adequaat worden beveiligd.

Er bestaat geen aparte privacywetgeving voor 'slimme camera's'. De beleidsregels geven wel enkele specifieke aandachtspunten voor drones, slimme camera's en dashcams. Een drone met een camera kan bijvoorbeeld opnames maken op plaatsen waar mensen verwachten onbespied te zijn en kan mensen volgen. Een drone kan daardoor een grotere inbreuk maken op de privacy dan een statische camera. Ook voor dashcams geldt dat in beginsel de Wbp van toepassing is als herkenbaar personen of kentekens worden gefilmd.

AUTORITEIT
PERSOONSGEGEVENS

Bron: Autoriteit Persoonsgegevens

Index

De Europese Commissie wil eind juni strengere regels voor virtuele valuta zoals bitcoin en prepaidkaarten voorstellen, om zo anonieme betalingen in te perken en de financiering van terrorisme tegen te gaan.

Europese Commissie wil bitcoingebruik terroristen aanpakken

Dat blijkt uit een nieuw actieplan dat is voorgesteld.

Volgens de Europese Commissie bestaat er een risico dat virtuele valuta door terroristische organisaties worden gebruikt om financiële transacties te verbergen. De Commissie wil daarom wisselplatformen voor dergelijke virtuele valuta, waar bijvoorbeeld bitcoins voor echt geld kunnen worden gewisseld, onder bestaande regelgeving tegen witwassen laten vallen, zodat de mensen die in virtuele valuta handelen kunnen worden geïdentificeerd.

Ook wordt er gekeken of licentie- en toezichtsregels van de bankrichtlijn Payment Services Directive (PSD) op virtuele valuta en aanbieders van virtuele portemonnees, zoals bitcoin wallets, kan worden toegepast. Dit moet voor meer controle zorgen en uiteindelijk witwassen en financiering van terrorisme voorkomen, aldus de Europese Commissie.

Verder wil de Europese Commissie ook het gebruik van anonieme prepaidkaarten tegengaan. Als het aan de Commissie ligt moeten de aanbieders van dit soort kaarten, die met een bepaald bedrag kunnen worden opgeladen, straks eerst hun klanten identificeren. Tevens wordt ook overwogen om biljetten van 500 euro mogelijk te verbieden. Deze biljetten zouden namelijk erg in trek zijn bij criminele organisaties die zich bezighouden met het fysiek transporteren van cash vanwege de hoge waarde en het kleine volume. De Commissie zal op dit gebied met de Europese Centrale Bank, Europol en andere partijen samenwerken om te bepalen of een verbod noodzakelijk is.

Bron: EU

Index

Het internet der dingen (Engels: Internet of things) refereert aan de situatie dat door mensen bediende computers (desktops, tablets, smartphones) in de minderheid zullen zijn op het internet.

Het Internet der dingen

De meerderheid van de internetgebruikers zal in deze visie bestaan uit semi-intelligente apparaten, zogenaamde embedded systems. Alledaagse voorwerpen worden hierdoor een entiteit op het internet, die kan communiceren met personen en met andere objecten, en die op grond hiervan autonome beslissingen kan nemen.

Een hedendaagse definitie van het internet der dingen is: Een voorgestelde ontwikkeling van het internet, waarbij alledaagse voorwerpen zijn verbonden met het netwerk en gegevens kunnen uitwisselen.

Als het belangrijkste aspect van het Internet der dingen wordt genoemd: de mogelijkheden die ontstaan wanneer fysieke objecten en de virtuele wereld samenkomen.

In de huidige visie spelen 'slimme' objecten een sleutelrol in het internet der dingen. Dit omdat ingebedde informatie- en communicatie-technologie het potentieel heeft om de bruikbaarheid van objecten revolutionair te doen toenemen. Met gebruik van sensors kunnen deze hun omgeving in zich opnemen, en via ingebedde netwerktechnologie kunnen ze met elkaar communiceren, internetdiensten gebruiken en met mensen interageren. In de huidige betekenis refereert de term internet der dingen dus aan 'dingen' die zelf computers zijn, en via internet zaken monitoren en regelen.

De verwachtingen rond het internet der dingen zijn dat er vanuit diverse gezichtspunten voordelen zullen zijn:

commercieel: efficiëntere processen, minder kosten voor logistiek/opslag, verkoop meer toegespitst op klanten;

sociaal en politiek: duidelijkere informatie voor klanten en burgers, betere zorg, betere veiligheid (bijvoorbeeld in het verkeer);

persoonlijk: nieuwe diensten die het leven aangenamer en veiliger maken.

Het internet der dingen wordt mogelijk gemaakt door een aantal basistechnologieën. Dat betekent dat de meeste toepassingen op een groot aantal van de onderstaande technologieën gebaseerd zullen zijn .

Communicatie en samenwerking

Apparaten (objecten) kunnen communiceren met het internet, of zelfs met elkaar. Ze kunnen gebruikmaken van internet-data en -services, en dan hun eigenschappen veranderen (bijvoorbeeld van stilstaand naar rijdend). Hierbij zijn ontwikkelingen in draadloze communicatie zoals UMTS en wifi cruciaal.

Adresseerbaarheid

Als adres van het object heeft een IP-adres het voordeel dat dit goed gestandaardiseerd is, en dus goed samenwerkt met het netwerk.[9] Door het internet der dingen neemt het aantal benodigde IP-adressen naar verwachting explosief toe. Een vereiste is immers dat elk object een eigen 'adres' heeft. Door de nu al plaatsvindende overgang van IPv4 naar IPv6 wordt voorzien in de behoefte aan (zeer) grote aantallen IP-adressen

Identificatie

De apparaten (objecten) moeten uniek identificeerbaar zijn. Voor passieve objecten (d.i. objecten zonder energiebron) kan identificatie via RFID of barcodes plaatsvinden. Hierbij kan een RFID-lezer of mobiele telefoon als medium fungeren. Hierdoor kan een object (bv. een tandwiel met barcode) gelinkt worden aan informatie die elders daarover opgeslagen is (niet zozeer over wat voor tandwiel het is, maar over welk tandwiel het is; bijvoorbeeld dat het tandwiel in jaar x aan fabriek y verkocht is en onderdeel is van machinenummer 123456).

Sensors

Met een sensor verzamelen apparaten data over hun omgeving. Ze leggen deze vast of sturen ze door of reageren er direct op. Sensors zetten een analoog signaal (bijvoorbeeld temperatuur of lichtintensiteit) om in een digitaal signaal (enen en nullen), zie analoog-digitaalomzetter.

Actuatoren

Via een actuator beïnvloeden de apparaten de fysieke wereld. Een actuator zet een signaal om in een actie, bijvoorbeeld een beweging.

Ingebedde informatieverwerking

Slimme apparaten hebben een microcontroller en opslagcapaciteit voor informatie, zie embedded system.

Lokalisatie

In het internet der dingen moeten de objecten gevonden kunnen worden, dat wil zeggen: gelokaliseerd en herkend via opzoekdiensten. Denk hierbij aan hoe mobiele telefoons gevonden en gelokaliseerd worden. Apparaten zijn zich 'bewust' van hun fysieke locatie. Dit gebeurt door deze zelf vast te stellen, dan wel doordat deze bepaling voor hen gedaan wordt. gps en mobiele-communicatietechnologie maken dit mogelijk. In Groot-Brittannië is men inmiddels begonnen het frequentiespectrum anders in te richten vanwege het internet der dingen.

Gebruikersinterface

Slimme objecten moeten met mensen kunnen communiceren, dit gebeurt direct dan wel indirect (via smartphone). Hierbij zijn vooral technologieën als spraakherkenning, beeldherkenning en geluidsherkenning van belang.

Anno 2016 met het internet verbonden apparaten

Er zijn anno 2016 al heel veel embedded systemen permanent, of tijdelijk met het internet verbonden. Zo zijn er onder meer moderne fototoestellen, kopieerapparaten, wasmachines, robots, auto's. Van de overgrote meerderheid hiervan kan echter niet gezegd worden dat ze hun omgeving in zich opnemen, of met wie dan ook een communicatie starten. De apparaten zijn misschien wel in de meerderheid op het internet, maar er is nog geen sprake van een internet der Dingen .

Er zijn in Nederland nog geen consumenten slachtoffer van contactloos zakkenrollen geworden, zo laat Betaalvereniging Nederland weten naar aanleiding van onderzoek van de Consumentenbond waaruit blijkt dat een contactloze zakkenroller ongemerkt duizenden euro's kan stelen.

Nog geen slachtoffers contactloos zakkenrollen in Nederland

Volgens de organisatie zijn er nog wel onduidelijkheden over contactloos betalen bij consumenten. "Klanten krijgen soms van hun bank te horen dat bij betalingen vanaf 50 euro, de betaalpas altijd in de automaat gestoken moet worden en dat klopt niet", aldus Betaalvereniging Nederland, waar ook de banken lid van zijn. De organisatie stelt dat erin Nederland nog geen mensen slachtoffer van contactloos zakkenrollen zijn geworden.

"Deze vorm van contactloos zakkenrollen is in Nederland echter nog nooit voorgekomen, mede omdat pashouders hun betaalpas meestal veilig opbergen en hun pincode goed afschermen. Als iemand hiervan toch slachtoffer wordt, zal de bank alle schade vergoeden." Vanwege de onduidelijkheid gaan de banken hun uitleg over contactloos betalen verbeteren.

Pincode

Bij contactloze betalingen boven 25 euro moet altijd de pincode worden ingetikt. In het geval van bedragen tot en met 25 euro hoeft meestal geen pincode te worden ingetikt. Alleen wanneer achter elkaar meerdere bedragen tot en met 25 euro contactloos worden betaald, moet de pincode alsnog worden ingetikt. Het beschermen van de pincode is dan ook belangrijk. Recentelijk waarschuwde de politie echter voor criminelen die met een infraroodfoto de pincode van een geldautomaat afkeken.

Volgens Betaalvereniging Nederland is de kans dat op deze manier pincodes worden gestolen klein. De organisatie wijst naar onderzoek van de Radboud Universiteit Nijmegen, waaruit blijkt het onwaarschijnlijk is dat met een infraroodcamera de pincode van het toetsenbord van een werkende geld- of betaalautomaat kan worden afgelezen. De elektronica onder het toetsenbord geeft al zoveel warmte af dat alle toetsen daardoor fel oplichten op een infraroodbeeld en de toetsaanslagen niet meer te herleiden zijn.

Betaalvereniging Nederland heeft het oorspronkelijke artikel "Onduidelijkheid over contactloos betalen" van de eigen website verwijderd en

Bron: Betallvereniging Nederland

Index

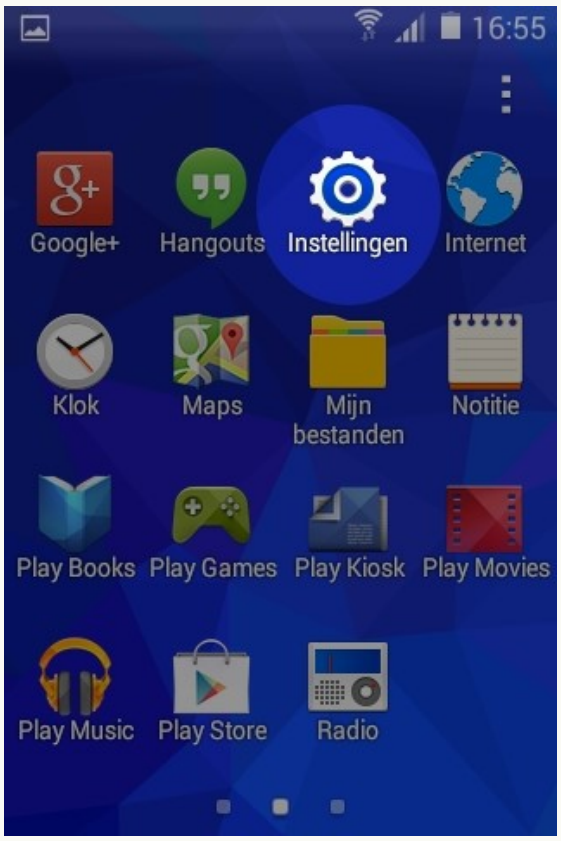
Onderweg of thuis bankieren met een app op je tablet of smartphone is snel en makkelijk. Met behulp van de app, een klein programmaatje dat je moet installeren op je mobiele apparaat, boek je in een handomdraai geld over naar je spaarrekening of betaal je een acceptgiro.

Internetbankieren met apps

Smartphones hebben meestal geen virusscanner en een kaartlezer of TAN-code is niet nodig. Banken nemen de nodige maatregelen om bankieren met een app te beveiligen. Zo kun je bij de meeste banken alleen naar bekende rekeningnummers (rekeningnummers waarnaar je in de afgelopen periode geld hebt overgemaakt of die in je adresboek staan) overmaken. En vaak zit er een maximum gesteld aan wat je maximaal kan overboeken. Uiteraard kan je zelf ook dingen doen en laten om veiliger te bankieren met een app , zoals het beveiligen van je smartphone en tablet.

Je Android smartphone beveiligen met een wachtwoord >

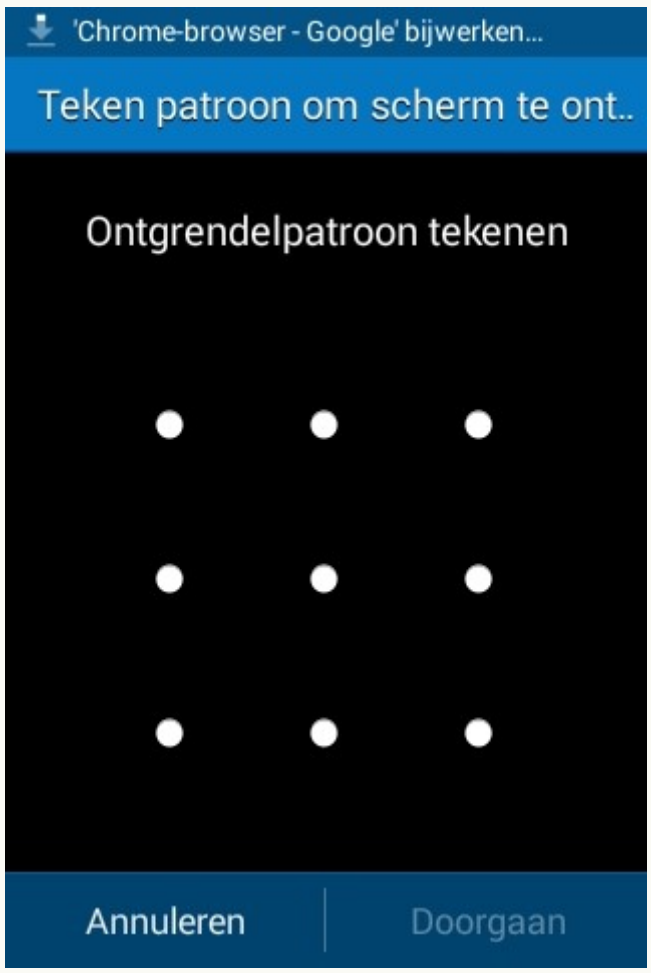
A > Ga op je Android naar 'Instellingen'.



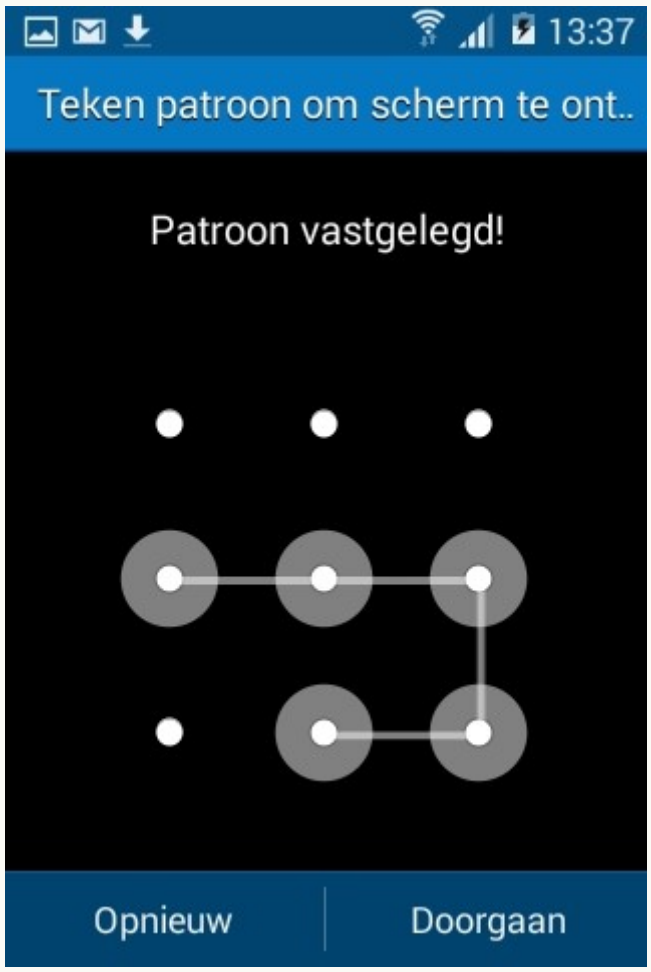
B > Klik op 'Mijn apparaten'.

C > Klik op 'Vergrendelscherm'.

D > Kies 'Schermvergrendeling'.



E > Geef een patroon in.



F > Bevestig het patroon.

G > Verlaat het menu.

Banken nemen de nodige maatregelen om bankieren met een app te beveiligen. Zo kun je bij de meeste banken alleen naar bekende rekeningnummers (rekeningnummers waarnaar je in de afgelopen periode geld hebt overgemaakt of die in je adresboek staan) overmaken. En vaak zit er een maximum gesteld aan wat je maximaal kan overboeken. Uiteraard kan je zelf ook dingen doen en laten om veiliger te bankieren met een app, zoals het beveiligen van je smartphone en tablet.

Download de mobiel bankieren app van je bank:

Rabobank: Rabo Bankieren app

ING: ING Bankieren

ABN AMRO: ABN AMRO Mobiel Bankieren

SNS Bank: SNS Mobiel Bankieren app

Triodos: Triodos Bankieren

ASN Bank: ASN Mobiel bankieren

Delta Lloyd bank: Delta Lloyd Mobile Banking

Bron:

Index

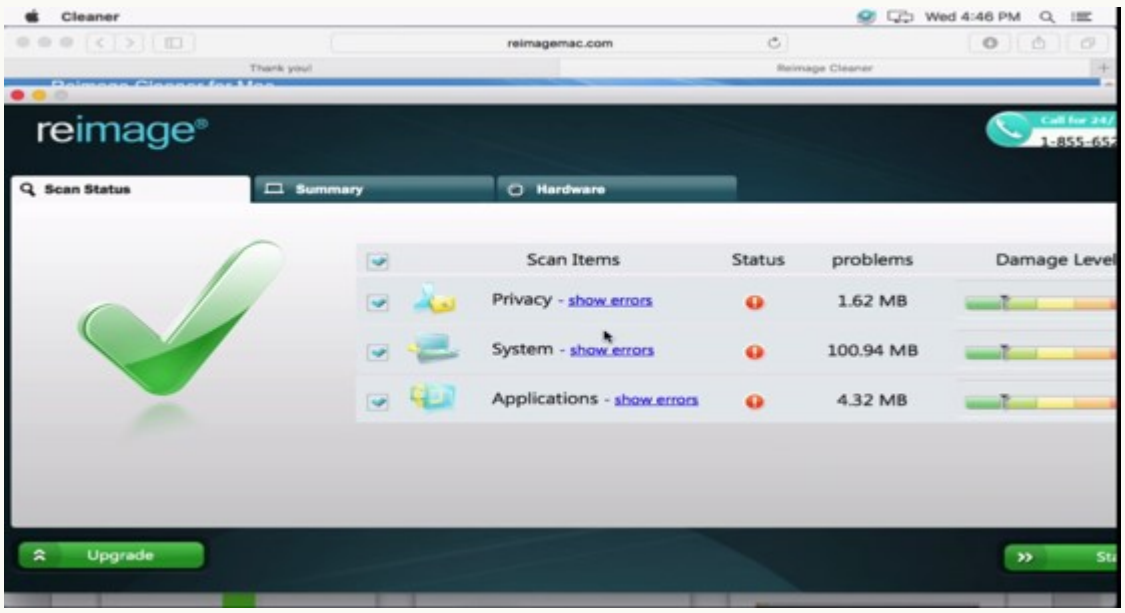
Social engineering is nog altijd een succesvolle manier voor cybercriminelen om internetgebruikers ongewenste software te laten installeren.

Nepversie Flash Player leidt Mac-gebruikers naar scareware

ISC-directeur Johannes Ullrich kreeg tijdens het internetten een pop-up te zien die stelde dat zijn Flash Player was verouderd en hij de aangeboden update moest installeren om door te kunnen gaan.

De pop-up wees naar een pagina die een "installer" van Adobe Flash Player aanbood. Deze nepversie was gesigneerd met een geldig Apple ontwikkelaarscertificaat. Standaard staat Mac OS X zo ingesteld dat alleen apps uit de Mac App Store en apps met een geldig ontwikkelaarscertificaat mogen worden geïnstalleerd. Na de "installatie" laadt de nepversie het echte installatieprogramma van Adobe Flash Player. Tevens wordt erin de achtergrond een website geladen met een pop-up die meldt dat er fouten op het systeem zijn gevonden. De gebruiker kan die echter laten herstellen.

De pop-up wijst naar een website die het progamma "Reimage Cleaner" aanbiedt. Dit programma moet de gebruiker zelf downloaden en installeren. In werkelijkheid is dit programma scareware dat de gebruiker laat geloven dat er problemen op het systeem aanwezig zijn. Vervolgens moet voor het oplossen hiervan worden betaald. De gebruiker speelt in dit geval een hoofdrol, omdat hij continu wordt verleid om op pop-ups en bestanden te klikken. Beveiligingsbedrijf Symantec liet vorig jaar nog weten dat adware en misleidende of ongewenste applicaties de meestvoorkomende dreigingen op Mac OS X zijn.



Bron: ICS

Index

Jongeren veranderen de sociale media in Nederland. Facebook en Twitter zijn inmiddels voor oudjes, want tieners en twintigers vertrekken massaal naar Snapchat en Instagram. En WhatsApp? Dat gebruiken we nog allemaal.

Jongeren kiezen voor Snapchat, maar niet voor Twitter

Dat blijkt uit het rapport van onderzoeksbureau Newcom, dat 10.395 Nederlanders van 15 jaar of ouder heeft ondervraagd. Het allergrootste sociale medium is WhatsApp, dat in Nederland 9,8 miljoen gebruikers heeft. Daarvan starten 7 miljoen mensen dagelijks de app op.

Facebook kleiner dan WhatsApp
Facebook is in Nederland met 9,6 miljoen gebruikers iets kleiner dan WhatsApp, waarvan 6,8 miljoen de site dagelijks bezoeken. Het dagelijks bezoek van Facebook steeg wel met 3 procent van 6,6 miljoen naar 6,8 miljoen mensen.

De grootste groei bij Facebook zit in de groep 80 jaar en ouder (52 procent). Het aantal jongeren dat een Facebook-account registreert, neemt bij de twintigers juist af en bij de tieners een klein beetje toe.

Twitter is ook voor oudjes
Het aantal Nederlanders dat Twitter dagelijks gebruikt, is volgens het onderzoek van Newcom flink gedaald: met 10 procent van 1 miljoen naar 0,9 miljoen. In totaal hebben 2,6 miljoen Nederlanders een Twitter-account. Vorig jaar daalde het aantal dagelijkse Twitter-gebruikers ook al met zo'n 33 procent.

De daling komt grotendeels omdat de toename van jongere gebruikers (15 tot 39 jaar) flink daalt. Het sociale netwerk verkeert al langer in zwaar weer omdat de groei van gebruikers stagneert. Vandaag werd ook bekend dat vijf topmannenTwitter verlaten.

Waar zijn de jongeren heen?
Jongeren kiezen niet voor Facebook of Twitter, maar gaan eerder naar Instagram (2,1 miljoen gebruikers), Pinterest (2 miljoen gebruikers) of Snapchat (1 miljoen gebruikers). Deze drie platformen stijgen dit jaar flink.

Het aantal mensen dat Instagram dagelijks gebruikt stijgt met 37 procent van 722.000 naar 992.000. Dat komt grotendeels door de flinke toename van jongere gebruikers tussen de 15 en 39 jaar.

Bij Pinterest is de stijging iets lager: van 261.000 naar 334.000, wat neerkomt op een toename van 28 procent. Daar zie je dat gebruikers van alle leeftijdsgroepen interesse hebben in het sociale netwerk.

De allergrootste stijger is Snapchat met 69 procent: van 320.000 naar 541.000 dagelijkse gebruikers. Daar zijn tieners de belangrijkste reden voor de stijging.

Zorgen om privacy
De zorgen om privacy blijven ook in 2016 bestaan. Zo'n 71 procent van de afhakers van één of meerdere platformen maakt zich zorgen over wat er precies met zijn of haar gegevens gebeurt.

De gebruikers van 65 tot 79 jaar maken zich het meest zorgen om hun privacy, terwijl tieners zich juist het minst zorgen maken.

Bron: Security.nl

Index

Internetters kunnen makkelijk naar slapende kids kijken

Internetters kunnen makkelijk naar slapende kids kijken

De garagedeur, de koelkast en de thermostaat: anno 2016 is bijna elk apparaat in het huishouden verbonden met het internet. Superhandig, maar experts waarschuwen dat dit fenomeen - het zogenaamde internet der dingen (IDD) - steeds onveiliger wordt. Zo is het sinds kort mogelijk om met behulp van online webcams in andermans huizen te kijken, en dat allemaal met een simpele zoekmachine. Een zorgwekkende ontwikkeling, zegt security-expert Dan Tentler tegen techsite Ars Technica.

Tentler, die jarenlang onderzoek deed naar webcam-veiligheid, meldt dat de zoekmachine Shodan een tool heeft gepubliceerd waarmee het mogelijk is om de webcam-feeds van onbeveiligde camera's te bekijken. Volgens de onderzoeker is er van alles te zien: garages, keukens, ski-pistes, wietplantages en misschien wel het meest zorgwekkende resultaat: slaapkamers.

Na een korte (en vooral makkelijke) zoektocht met de zoekmachine, wordt al snel een klaslokaal in China, een man op de bank, een keuken in Spanje en een slapende baby in Canada gevonden.

Hoe het mogelijk is, is een technisch verhaal, maar in de essentie gaat het erom dat de camera's niet beveiligd zijn met een wachtwoord. Hierdoor kan Shodan gemakkelijk toegang krijgen tot de apparaten. Tentler vermoedt dat er miljoenen onbeveiligde webcams aan staan in de wereld en dat is volgens hem grotendeels de schuld van nalatigheid bij de consument.

Onbelangrijk

Volgens Tentler vindt de consument veiligheid en privacy helemaal niet belangrijk. Als gevolg betaalt de klant ook niet extra voor die waardes. Het resultaat: webcamproducenten die geen aandacht schenken aan de veiligheid om zoveel mogelijk geld te verdienen. ,,De consument zegt dat ze niks afweten van cybersecurity, het bedrijf wil niet helpen omdat het geld kost'', zegt Trentler.

Volgens hem is noodzaak dat bedrijven en overheden meer geld gaan steken in het veiliger maken van het IDD. Men moet zich niet blindstaren op het feit dat een anonieme internetter rechtstreeks in het ledikantje op de slaapkamer kan kijken. Als de veiligheid van producten die verbonden staan met het internet niet verbeterd, kunnen er nog veel schokkender dingen gebeuren, aldus de onderzoeker.

Wat is het Internet der Dingen en wat doet Shodan?

De printer op kantoor en het waterreinigingssysteem in het dorp. Beide zijn verbonden met het internet maar worden doorgaans niet bediend door mensen, zoals dat wel gebeurt bij een pc, tablet of smartphone. De algemene gedachte is dat deze ‘dingen’ uiteindelijk veel meer op het internet aanwezig zijn dan ‘echte’ mensen. Die situatie noemt met het Internet der Dingen.

Shodan – een zoekmachine uit 2009 gemaakt door de Amerikaan John Matherly – geeft de mogelijkheid om te zoeken naar die apparaten. Ook is het mogelijk om slecht beveiligde apparaten te 'hacken' en vervolgens daadwerkelijk te gebruiken. Het was bij de ontwikkeling van de zoekmachine de bedoeling dat bedrijven konden waarnemen waar consumenten hun producten gebruikten, maar het werd na verloop van tijd duidelijker dat de zoekmachine steeds meer gebruikt werd door security-experts. Zij gebruikten Shodan om aan te tonen dat er systematische fouten zaten in de veiligheid van de systemen van die bedrijven. Zo konden onbekende internetters via Shodan simpel de systemen van een Franse stuwdam besturen. Wat bleek: de installatie had nog een standaardwachtwoord actief.

Bron: Ars Technica

Index

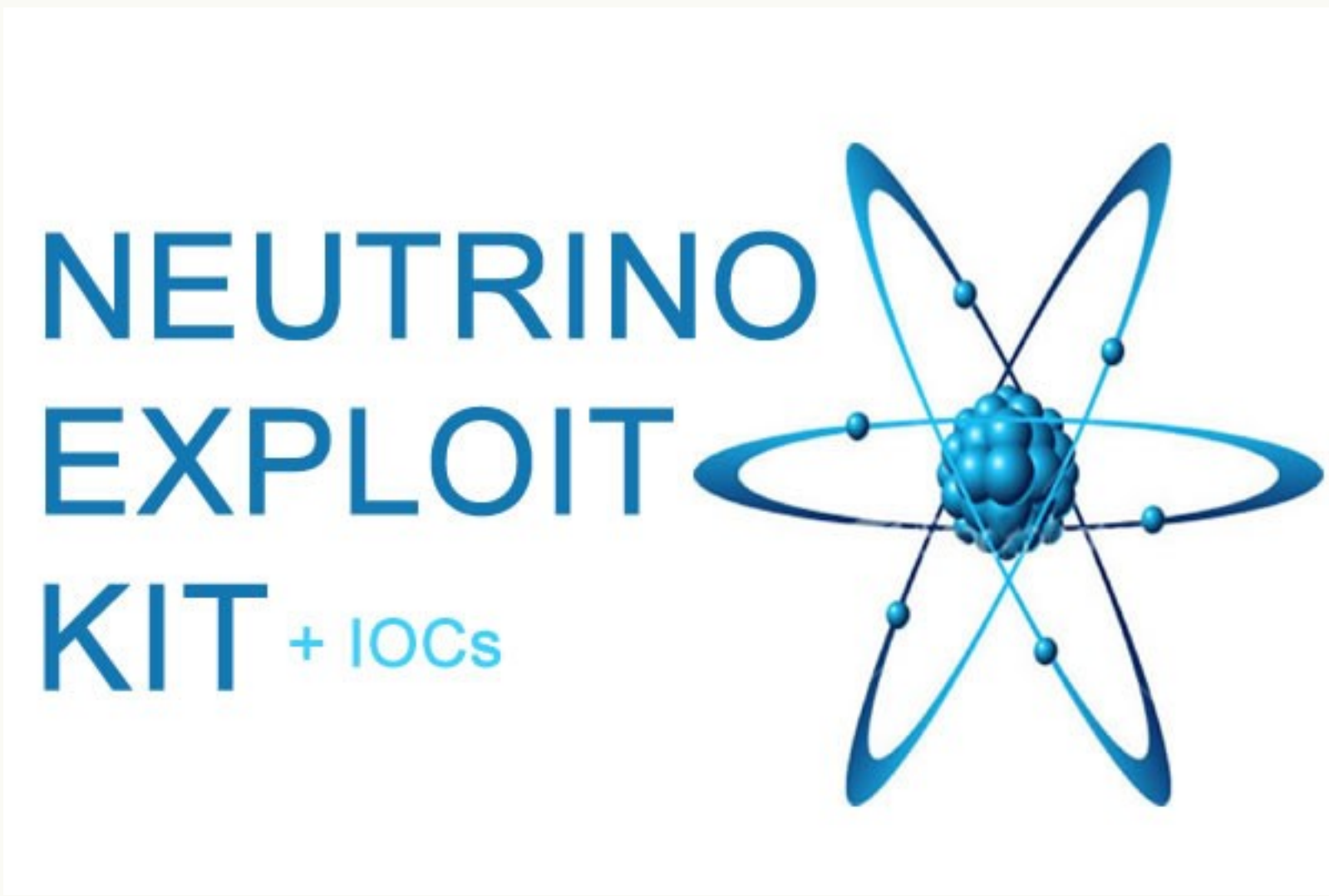
Een exploitkit die internetgebruikers via kwetsbaarheden in Adobe Flash Player probeert te infecteren blijkt computers met Linux te vermijden.

Toolkit voor cybercriminelen vermijdt Linux-computers

Dat meldt beveiligingsbedrijf Trustwave. Op gehackte websites plaatsen cybercriminelen code die bezoekers ongemerkt naar een pagina met de Neutrino-exploitkit doorsturen. In het geval bezoekers een kwetsbare Adobe Flash Player geïnstalleerd hebben, wordt er stilletjes malware op het systeem geplaatst. Tegenwoordig gebruikt de Neutrino-exploitkit een module voor de iptables-firewall om te kijken welk besturingssysteem bezoekers gebruiken. In het geval van Linux worden deze computers vervolgens geblokkeerd, zodat de pagina met de exploitkit niet wordt geladen.

Volgens Daniel Checkik van Trustwave is het zinnig voor exploitkits om Linux-computers te filteren, aangezien deze machines vaak beveiligingsproducten, servers of andere machines zijn en geen potentiële slachtoffers. Door deze aanpak verkleint de exploitkit daarnaast dat het wordt gevonden door geautomatiseerde scans of beveiligingsonderzoekers. Het komt vaker voor dat exploitkits maatregelen treffen om beveiligingsonderzoekers en andere ongewenste bezoekers op afstand te houden, maar in de meeste gevallen worden deze maatregelen op http-niveau genomen, waarbij de webserver een foutmelding geeft of de bezoeker naar een andere pagina doorstuurt.

Het implementeren van het filter op tcp-niveau, zoals de Neutrino-exploitkit nu doet, is volgens Chechik een slimme keuze, omdat er vaak wordt aangenomen dat een server die niet reageert onbereikbaar is. Aangezien exploitkits vaak van locatie veranderen, kan dit gedrag aan een onbereikbare server worden toegeschreven, terwijl in werkelijkheid de server alleen bezoekers krijgt die het kan infecteren.



Bron: TrustWave

Index

Een botnet dat vooral wordt gebruikt om geld van online bankrekeningen te stelen blijkt nu een virusscanner van Avira te verspreiden .

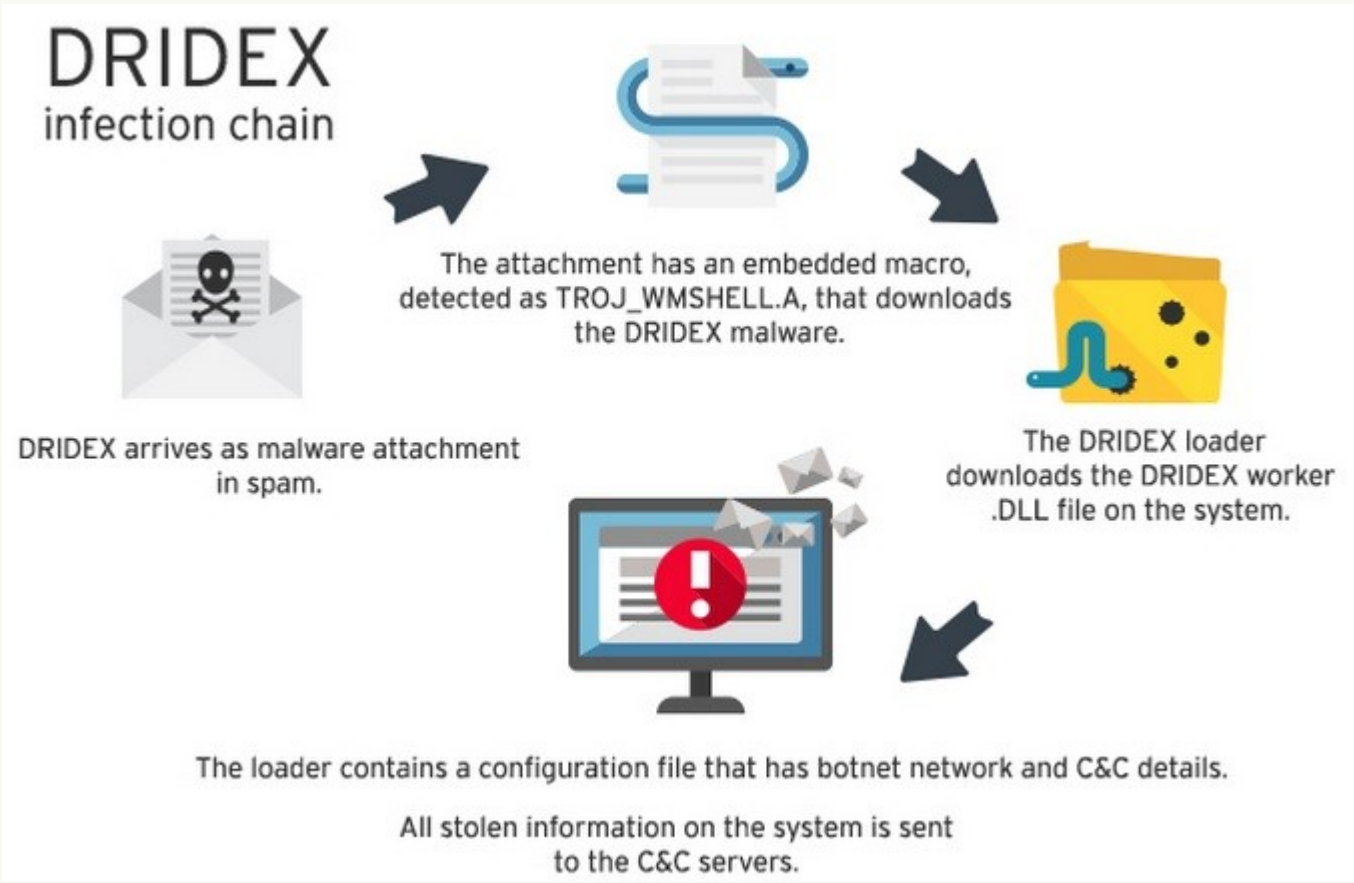
Dridex-botnet verspreidt virusscanner Avira

Het gaat om het Dridex-botnet, dat vorig jaar nog doelwit van een operatie van Europol en de FBI werd.

Volgens de Duitse virusbestrijder Avira is een distributiekanaal van Dridex gehackt. In plaats van malware krijgen mensen nu schone versies van Avira Antivirus aangeboden. Ondanks de operatie van de opsporingsdiensten is Dridex nog steeds actief. De malware verspreidt zich vooral via kwaadaardige macro's in Office-documenten. Zodra gebruikers de macro inschakelen zal die de malware op de computer downloaden. Tot verrassing van Avira wordt de Avira-webinstaller echter gedownload.

In plaats van een computerinfectie krijgen de gebruikers op deze manier een virusscanner. "We weten nog steeds niet wie hier achter zit en waarom, maar we hebben een aantal theorieën", zegt malware-expert Moritz Kroll. De eerste theorie is dat cybercriminelen op deze manier het detectieproces van anti-virusbedrijven proberen te verstoren, maar Kroll denkt niet dat dit het geval is.

De tweede theorie is volgens hem waarschijnlijker, namelijk dat een 'white hat hacker' verantwoordelijk is. Mogelijk heeft deze hacker dezelfde kwetsbaarheden gebruikt die ook de Dridex-auteurs hebben gebruikt om servers te hacken en daar hun malware te plaatsen. De hacker zou de malware vervolgens hebben vervangen met de webinstaller van Avira. Volgens Kroll is deze werkwijze in de meeste landen illegaal en zal de hacker zich daarom waarschijnlijk niet bekendmaken.



Bron: Avira

Index

Het in de browser streamen van torrents is het nieuwe hoofdpijndossier van de auteursrechtendindustrie, dat de nieuwe technologie maar amper kan bijbenen en niet goed weet hoe het om moet gaan met de makkelijk te installeren alternatieven.

Torrents streamen in browser

Wat wordt de volgende stap in het kat-en-muis-spel tussen de downloaders en de beschermers?

Het nieuwste wapenfeit van de illegale up- en downloaders is Torrents Time, een plugin waarmee je onder andere Popcorn Time in je browser kunt gebruiken. Die techniek werd vorige week gepresenteerd, maar begint nu al naar andere sites te verspreiden - en dat levert een groot probleem op voor de filmindustrie, die niet weet wat het tegen zulke diensten moet doen.

Torrents streamen in de browser

De meest notoire (en meest gebruikte) torrentsites van dit moment, The Pirate Bay en Kickass Torrents, maken nu al gebruik van die techniek. Als je de Torrents Time-plugin gebruikt, kun je de torrents direct daar afspelen.

Popcorn Time is niet alleen een doorn in het oog van de industrie vanwege het hoge aantal gebruikers, maar vooral ook om hoe moeilijk het te stoppen is. De broncode is openbaar, en inmiddels zijn er installatiegidsen geschreven waarmee iedereen met maar een klein beetje kennis zelf de site kan hosten op een eigen domein. Wanneer Brein of de MPAA of wie dan ook de ene site offline halen, komen er weer 3 alternatieve diensten op.

De ontwikkeling van Popcorn Time gaat te snel voor de industrie. Die kan het aantal snel opgezette sites niet bijbenen, en weet niet goed hoe het om moet gaan met al die nieuwe sites. Op dit moment probeert bijvoorbeeld Brein dat nog wel, door het snel aanschrijven van nieuwe websites in de hoop die af te schrikken.

Soms gaat dat snel, zoals bij de eerste 'Popcorn Time voor in de browser' die bijna meteen offline werd gehaald. Ook alternatieven zoals Nacho Time werden snel aangepakt door Brein, maar er zijn minstens zo veel alternatieven die nog gewoon werken.

Net de Pirate Bay

Het kat-en-muisspel met Popcorn Time lijkt erg veel op dat met The Pirate Bay van een paar jaar geleden. Ook toen worstelde de filmindustrie met het aanpakken van de torrent-site, want hoewel die keer op keer offline werd gehaald wisten downloaders altijd wel een alternatief te vinden. Later kwamen daar open source alternatieven voor in de plaats waardoor iedereen zijn eigen Pirate Bay-proxy kon opzetten - met het pragmatisch genaamde FuckTimKuik.orgvoorop.

De industrie lijkt weinig geleerd te hebben van dat 'hydra-effect', waarbij het neerhalen van één site weer drie nieuwe andere sites oplevert. Dat gebeurt nu namelijk ook met Popcorn Time: Toen de originele dienst offline werd gehaald, kwamen er meteen nieuwe forks op zoals PopcornTime.io en Popcorn-Time.se. Ook die zijn inmiddels offline, waardoor de Popcorn Time-app niet meer werkt.

De volgende stap?

De volgende stap in dat ingewikkelde spelletje is de browserplugin, want daardoor ben je nu niet meer afhankelijk van één dienst die het streamen mogelijk maakt. Je kunt dat namelijk op meerdere sites doen, zoals nu The Pirate Bay en later ook diensten als Porn Time en Kickass Torrents.

Wat wordt de volgende stap van Tim Kuik en zijn consorten? Gaat de industrie weer individuele diensten offline halen? Gaat het naar de bron? En hoe voorkomt het dat die bron weer verder verspreid wordt?

Bron: PCMweb

Index

Wie wel eens online een filmpje bekijkt, heeft er waarschijnlijk al mee te maken gehad: in een venster wordt je gevraagd een bepaalde update uit te voeren om de video te kunnen bekijken.

Google blokkeert voortaan valse downloadknoppen

In sommige gevallen dient je software inderdaad up-to-date te zijn alvorens je van een filmpje kan genieten. De kans is echter groter dat het om een vorm van oplichting gaat waarbij nietsvermoedende surfers worden aangezet tot het delen van persoonlijke informatie of downloaden van gevaarlijke software.

Safe browsing

Om een einde te maken aan dergelijke praktijken, heeft Google 'Safe Browsing' in het leven geroepen. Deze dienst in Google Chrome beschermt je al meer dan acht jaar tegen phishingpraktijken en zal je voortaan eveneens een waarschuwing geven telkens er een vorm van social engineering wordt gedetecteerd.

Inhoud op webpagina's worden als social engineering aanzien, indien ze zich proberen te gedragen als een vertrouwde site of dienst, zoals je browser of de website waarop je zit. Content die je probeert te overhalen om persoonlijke informatie te delen die je normaal gezien alleen aan vertrouwde diensten zou geven, worden eveneens als social engineering bestempeld.

Gemarkeerde sites

Google zal surfers eveneens waarschuwen wanneer ze een site bezoeken waarop content met betrekking tot social engineering staat. Om te achterhalen of jouw website als gevaarlijk wordt bestempeld, kan je het rapport 'Beveiligingsproblemen' van Google bekijken. Met name advertenties en andere content van derden kunnen je in de problemen werken.

Bron: Google

Index

Vorig jaar zijn Nederlanders voor miljoenen euro's via het internet opgelicht, zo laat de Fraudehelpdesk vandaag weten.

Nederlanders vorig jaar voor miljoenen via internet opgelicht

Het aantal slachtoffers dat melding bij de organisatie maakte verdubbelde van 1887 in 2014 naar 3625 in 2015. Deze 3600 gedupeerden werden voor 12,2 miljoen euro opgelicht.

Eind 2014 bedroeg de gemelde schade 8,3 miljoen euro. De grootste groep werd via webwinkels en aankopen op Marktplaats opgelicht, waarbij er wel werd betaald maar niets geleverd. De grootste bedragen verloren slachtoffers echter via voorschotfraude. Internetoplichters benaderen in dit geval hun potentiële slachtoffers met een mooi verhaal, waarvan de kern is dat zij eerst iets moeten betalen voordat ze iets kunnen krijgen. Bekendste voorbeelden hiervan zijn dating-, erfenis- en loterijfraude.

Datingfraude

Zo betaalden 133 slachtoffers van datingfraude die zich hadden gemeld ruim 2,7 miljoen euro aan de oplichters, wat een gemiddelde van 20.000 euro per slachtoffer is. Sommigen raakten niet meer dan honderd euro kwijt, maar er was ook een uitschieter met 380.000 euro schade. Relatief de meeste slachtoffers werden op Facebook benaderd. De vaakst genoemde datingwebsites waarop oplichters actief zijn waren Lexa en Badoo.

In het bedrijfsleven is het aantal ondernemers en bedrijfsadministraties dat per ongeluk een spookfactuur betaalde, ruim verdubbeld van 190 in 2014 naar 481 vorig jaar. Hier ging het om relatief kleine bedragen met een gemiddelde van 96 euro. Bijna vijfhonderd gedupeerden van cybercrime meldden een totale schade van 822.000 euro. Van de Nederlanders die met internetoplichting te maken krijgen meldt 10 tot 13 procent dit bij de Fraudehelpdesk, zo blijkt uit onderzoek. "De werkelijke cijfers over aantallen slachtoffers en schadebedragen liggen dus aanzienlijk hoger", aldus de organisatie.

Bron: Fraudehelpdesk

Index

Fabian Wosar van Emsisoft heeft aangekondigd dat hij de encryptie die gebruikt wordt in de LeChiffre ransomware heeft gekraakt

Onderzoeker Emsisoft kraakt Le Chiffre Ransomware

Dit betekent dat slachtoffers van deze ransomware gratis hun bestanden kunnen ontsleutelen door gebruik te maken van de Emsisoft decrypter tool.

Ransomware is het type malware dat de PC van een slachtoffer blokkeert of de aanwezige bestanden versleutelt. Pas als er losgeld wordt betaald worden de bestanden weer ontsleuteld. Een bekend voorbeeld van ransomware in Nederland is de KLPD Ransomware.

De LeChiffre ransomware werkt net iets anders dan de standaard ransomware. Aanvallers moeten deze ransomware namelijk handmatig op een geïnfecteerd systeem installeren. Normaal gesproken gebeurt dit automatisch na een malware infectie. De LeChiffre ransomware meldt zelf overigens de bestanden na 6 maanden gratis te ontsleutelen.

Wosar was in staat de encryptie van LeChiffre kraken omdat er gebruik wordt gemaakt van een vaste encryptiesleutel aangevuld met een aantal kenmerken van het geïnfecteerde systeem

http://emsi.at/DecryptLeChiffre

Bron: Computer Totaal

Index

Google-onderzoeker Tavis Ormandy heeft een waarschuwing afgegeven voor de browser van anti-virusbedrijf Comodo, omdat het een serieus beveiligingsrisico is.

Google-onderzoeker waarschuwt voor browser Comodo

Google-onderzoeker Tavis Ormandy heeft een waarschuwing afgegeven voor de browser van anti-virusbedrijf Comodo, omdat het een serieus beveiligingsrisico is. Bij de installatie van Comodo Internet Security wordt standaard een nieuwe browser geïnstalleerd, genaamd Chromodo.

Het is een op Chromium-gebaseerde browser. Chromium vormt ook de basis voor Google Chrome. Na de installatie maakt Chromodo zich de standaardbrowser en vervangt alle snelkoppelingen met links van Chromodo. Tevens worden alle cookies en instellingen uit Chrome geïmporteerd. De browser verricht meerdere 'dubieuze zaken', aldus Ormandy, waaronder het kapen van de dns-instellingen.

Hoewel Chromodo claimt het hoogste niveau van beveiliging, snelheid en privacy te bieden, blijkt het de webbeveiliging juist uit te schakelen. De browser schakelt namelijk de same-origin policy uit. Dit is een zeer belangrijke beveiligingsmaatregel die bijvoorbeeld toestaat dat een script op een pagina toegang tot data op een tweede pagina heeft, maar alleen als beide pagina's van dezelfde locatie afkomen.

Gebruikers van Chromodo lopen dan ook een groot risico. Comodo kwam uiteindelijk met een oplossing voor het probleem, maar die is volgens Ormandy niet correct en nog steeds eenvoudig te omzeilen. Het oplossen van de overige problemen kan mogelijk nog weken gaan duren. "Het verkopen van anti-virus maakt je nog niet geschikt om Chromium aan te passen", zo haalt Ormandy op Twitter uit naar Comodo.

Bron: Google

Index

De tijd dat You Tube alleen bestemd was voor het bekijken van videoclips en zelfgemaakte filmpjes ligt inmiddels achter ons.

YouTube is onderdeel geworden van het nieuwe leren.

(Voor u gevonden op YouTube……..en Tek Tok.

TEK TOK

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

YouTube
Teach
~~Broadcast~~ Yourself™

Mobiele Eenheid achter de schermen

Verleiding van de misdaad

Kun jij beslissen wat de hoogste prioriteit heeft

Draadloos netwerk

Doe jij het veilig online

Malware

WiFi ontvangst verbeteren

Inbraakbeveiliging

Hoe gaat de inbreker te werk

Internetfraude via de telefoonDocumentaire: 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

Veilig politiewerk

Gezag op straat .. Als het moeilijk wordt

Bron: YouTube

Index

Schatkist

Naslag:

- Handleiding Twitter
- Gebruik tweetraps authenticatie
- Windows 10 installatie
- Online verdwijnen
- Centraal cloudbeheer
- Online kopen
- Cybersecurity 2015
- Stickware
- Netwerk in de knoop

Software:

- 360 Total Security
- AS SSD benchmark
- Cdex
- Cleanmaster
- CPU-Z
- Emsisift Emergency Kit
- KillDiskSuite
- Mp3Gain
- MultiCommander
- SyneiSystemUtilities

Index

Het eigen risico voor fraude bij internetbankieren en skimming wordt verlaagd naar 50 euro, zo heeft minister Dijsselbloem van Financiën in een brief aan de Tweede Kamer laten weten. Slachtoffers moeten nu nog maximaal 150 euro zelf betalen. Het lagere bedrag is onderdeel van de nieuwe Europese bankrichtlijn Payment Service Directive 2, die later dit jaar van kracht wordt.

De richtlijn biedt Europese lidstaten de mogelijkheid om het eigen risico verder te verlagen, maar Dijsselbloem wil hier geen gebruik van maken. De minister wil naar eigen zeggen op deze manier voorkomen dat klanten anders onzorgvuldig met elektronisch betalen en internetbankieren omgaan.

————————————————————

Het vinden van de juiste balans op internet tussen veiligheid en privacy is door het toegenomen gebruik van encryptie en anonimiteitstools een stuk lastiger geworden, zo claimt Europol. Volgens de onderzoeksorganisatie beschikt het over robuust beleid voor het beschermen van gegevens. "Hierdoor kunnen we georganiseerde misdaad en terrorisme voorkomen en bestrijden terwijl de fundamentele rechten van individuen wordt beschermd."

In het kader van Databeschermingsdag laat Europol weten dat de balans tussen privacy en veiligheid een belangrijke rol speelt bij politie-operaties. "Echter, het vinden van de juiste balans in cyberspace is door het toegenomen gebruik van encryptie en online anonimiteitstools een stuk lastiger geworden." Europol erkent dat het gebruik van dergelijke technologieën in veel gevallen legitiem is, bijvoorbeeld in het geval van burgers die hun privacy belangrijk vinden of bedrijven die hun gegevens willen beschermen.

"De realiteit is echter dat cybercriminelen misbruik van encryptie- en anonimiteitsoplossingen maken om hun identiteit, communicatie en data te beschermen en virtuele munteenheden gebruiken om hun financiële transacties te verbergen. Allemaal op een manier die het onmogelijk maakt om deze personen te vervolgen. Zijn we als maatschappij bereid om dit als 'nevenschade' voor onze vrijheid te accepteren?", stelt Europol de vraag. In mei organiseert de organisatie in Den Haag eenconferentie over encryptie en anonimiteit op internet, waarbij het wil kijken hoe de juiste balans tussen vrijheid en veiligheid kan worden gevonden.

————————————————————

Facebook Inc zegt voortaan beter te gaan letten op mensen die via facebook of Instagram een vuurwapen willen verkopen. Wapenhandel door particulieren is vanaf nu verboden en groepen waarin dat gebeurt, zullen afgesloten worden. In veel openbare groepen worden wapens openlijk aangeboden en besproken. Nog wel toegestaan zijn bedrijven die legaal wapens verkopen. De verkoop van illegale wapens werd in 2014 al verboden maar de afgelopen twee jaar bleek dat verbod simpel te omzeilen zodat de regels nu strenger worden, verklaart facebookwoordvoerder Monicka Bickert. Critici van het verbod hebben al opgeroepen om wapens voortaan ‘sportgoederen’ te noemen en vooral niet de woorden ‘for sale’ te gebruiken – termen waarop facebook filtert.Volgens The New York Times was Facebook een van de grootste online verkoopplaatsen voor wapens in de VS.

————————————————————-

Van vier op de tien Nederlanders staan ‘ongewenste foto’s op internet, blijkt uit onderzoek van Multiscope. De helft daarvan doet daar vervolgens niks mee, de andere helft vraagt of de foto er weer af kan. Het plaatsen van foto’s op internet vinden we heel normaal, zo blijkt. Driekwart van de ondervraagden doet dat wel eens, vooral facebook scoort heel hoog. Een kwart vraagt echter nooit toestemming aan anderen om die foto online te zetten. Van alle ondervraagden zegt 60% er rekening mee te houden dat een foto gebruikt kan worden voor identiteitsfraude, in totaal 2% zegt daarvan slachtoffer te zijn geweest. Ook zegt 10% iemand te kennen wiens foto is misbruikt.

————————————————————

In India is IS actief op zoek naar hackers die overheidsdatabestanden kunnen kraken. Op sociale media wordt druk geadverteerd, zo’n dertigduizend mensen zijn benaderd. Het salaris bedraagt 10 mille per opdracht; geen andere organisatie betaalt zo veel, zeggen beveiligingsexperts. Een van de opdrachten is het opzetten van een database met potentiële jihadstrijders, te werven op twitter en facebook, blijkt uit de advertenties die worden verspreid via verschillende (underground) communities als Silent Circle, Telegram en Whatsapp.

————————————————————

‘Ik bid elke avond om tien graden vorst zodat het ongedierte dood vriest’. Tegen deze en andere ‘haatcommentaren’ op facebook en andere sociale media strijden Chantal (31, uit Purmerend) en Susan (52, uit Uden). Een uurtje of vijf per dag zijn ze online, vooral op facebook. Daar reageren ze op alle haatberichten die verschijnen. ‘Hopen dat mensen doodvriezen, de liefde straalt er vanaf’, schreef Chantal bijvoorbeeld onder het bewuste commentaar. In NRC Handelsblad doen de vrouwen hun verhaal. Over hoe ze zich moeten beheersen, zich niet moeten laten verleiden tot schelden. ‘Racist’ zeggen mag, weten ze. ‘Nazi’ niet. De twee zijn niet de enigen, aldus het artikel waaruit blijkt dat ‘Het Verzet op Internet’ groter is dan menigeen wellicht denkt. Maar ook de vrouwen krijgen bedreigingen en scheldkannonade’s. Ze werden al uitgemaakt voor ‘linkse Gutmenschen’, voor struisvogels en voor NSB-ers natuurlijk. Anderen kregen mailtjes dat ze thuis bezoek konden verwachten of werden voor kinderlokker uitgemaakt. De vrouwen, het zijn vooral vrouwen blijkt uit het verhaal, gaan echter door. In totaal zijn ze met zo’n drieduizend schatten ze zelf, actief in verschillende ‘positieve communities’. Om ‘een tegengeluid’ te laten horen. Hoe? Waar de een vooral negatieve comments verzamelt, checken anderen filmpjes of postings op echtheid. Weer anderen leggen uitingen vast en bellen het meldpunt internetdiscriminatie of de politie. Of iemands werkgever. Een kleine groep gaat nog verder en zet de racistische uitingen online, compleet met voor- en achternaam en profielfoto, bijvoorbeeld op de pagina Racisten in de Spotlight. Of hun tegengeluid zin heeft, weten de meesten niet. ‘Maar je laat potentiële relschoppers wel weten dat ze gezien worden’.

————————————————————

Index

Om ‘een signaal af te geven’, is de politie in Brummen een strafrechtelijk onderzoek gestart naar de onbekende die via facebook agenten in het dorp beledigd heeft. Volgens de agenten is het geen probleem dat ‘niet iedereen even gecharmeerd is van ons werk’ maar wordt ‘van eenieder’ ook verwacht dat ‘we respectvol met elkaar omgaan. Ook op social media’. Onbekend is wat de belediging was, deze is verwijderd. Maar het was kennelijk zo erg dat er actie volgt. ‘Jammer dat het moet, maar laat het een signaal zijn voor de rest’, aldus een bericht op de facebookpagina. De afzender ‘komt er niet mee weg’, klinkt het strijdbaar.

———————————————————

Politieman Tim die onlangs op Marktplaats spullen aanbood die afkomstig waren uit het ramptoestel van MH17, deed niets strafbaars. Het OM heeft besloten de agent niet te vervolgen. De spullen die hij aanbood, een tissuezakje en een stukje vliegtuigromp, waren weliswaar echt maar buiten het onderzoeksgebied gevonden en bovendien ‘niet van belang voor het onderzoek naar de schuldigen van de ramp’. De man bood ook kleding aan die echter nooit was ingenomen. Omdat ‘geen van de te koop aangeboden spullen onrechtmatig verkregen is’, heeft de manniets strafbaars gedaan. De man wordt wel gestraft door zijn werkgever. Hij is teruggezet in rang en kreeg voorwaardelijk strafontslag opgelegd. Volgens de korpsleiding is het ‘onethisch, ongepast, kwetsend en choquerend’ om MH17-spullen aan te bieden. Niet alleen voor slachtoffers en nabestaanden maar voor ‘onze hele samenleving’.

———————————————————

Een prachtige zaak uit Wales waarbij facebook voor veel bewijs zorgde. De zaak draait om de familie Yandell. Vader Byron heeft een garage, zijn zoons werken er – normaal familiebedrijf, zo op het eerste gezicht. Maar er blijkt gedoe met gestolen auto’s, zwendel met verzekeringen, dure claims na zelf veroorzaakte botsingen, vrienden die nep-ongelukken maken, uitvoeren van reparaties aan auto’s die helemaal niet stuk waren etcetera. De politie zit er jaren achteraan maar krijgt de Yandells niet veroordeeld. Totdat het dossier – de ‘grootste autoverzekeringfraude in heel Wales ooit’ – wordt aangevuld met informatie die van facebook komt. Dan blijkt dat de Yandells het wel erg breed hadden, gezien de inkomsten die ze bij de belasting opgaven. Foto’s van dure vakanties en zo. Bij een vakantie schreven ze dat het wel 1900 pond had gekost – precies het bedrag dat een van de verdachten een week eerder had teruggekregen van de verzekering, voor een ongeluk dat nooit gebeurd was. Geconfronteerd met de foto’s konden de verdachten niet meer ontkennen. Mensen die ze zeiden niet te kennen, stonden afgebeeld op vakantiefoto’s; een onbekende die haar auto door Yandell liet repareren, stond naast het echtpaar op de huwelijksfoto; een vrouw die verklaarde dat ze een week thuis zat na een aanrijding, bleek aanwezig op het huwelijk van haar zoon; en zelfs iemand die een selfie maakte in een heuvelig gebied terwijl ze zogenaamd ziek thuis zat na een aanrijding. Mooie foto’s, vond detective constable Sara Morris. Maar ook dom van de verdachten. ‘Iedereen kon deze foto’s zien. Vrienden en familie van de Yandells hebben het plaatje voor ons mooi ingevuld’. Dat de Yandells beveiligingscamera’s in/rond de garage hadden opgehangen, was ook al niet zo slim. Daarop stond precies hoe ze de nepbotsingen arrangeerden, hoe ze eerst waardevolle onderdelen verwijderen en daarna tegen een muur reden. De politie heeft berekend dat met de totale zwendel meer dan twee miljoen pond was gemoeid. Zeven leden van de familie zijn nu veroordeeld, met straffen tot zes jaar.

———————————————————

Wie politie en sociale media zegt, stuit al gauw op Rick de Haan, die onlangs in de Eenheid Noord-Holland het Blauwe Hart ontving voor zijn nimmer aflatende enthousiasme om politiemensen ‘digitaal blauw’ te krijgen. Voor het Haarlems Dagblad was dat aanleiding Rick te interviewen. In het artikel vertelt Rick hoe hij al snel doorhad hoe twitter een prima middel is om met het publiek in contact te komen. En dan niet alleen als zéndmiddel, als alternatief kanaal om persberichten te versturen, maar als interactief communicatiemiddel. Met de nadruk op interactief. Daarnaast bleek twitter al snel een enorme informatiebron, bij evenementen, demonstraties, maar ook bij grote incidenten en crises. ‘We willen meer blauw op straat maar die straat is deel gedigitaliseerd. Wij moeten dus waakzaam en dienstbaar zijn op de plekken waar ons publiek is’. Rick zegt ook de valkuilen goed te kennen. ‘De gouden regel is: wat je op straat niet doet, moet je ook online niet doen’. Want ja, iedereen kijkt en leest mee. Overigens ziet hij ook dat er online ‘een zelfreinigend vermogen is dat discussies vaak in ons voordeel oplost’. De Haan zegt het liefst te zien dat de politie 24/7 digitaal bereikbaar is. ‘Als je moet bellen om een melding te doen, gaat er tijd verloren’. Verder ziet hij wel iets in digitale vragenuurtjes en in realtime video’s op Facebook.

———————————————————

De speciale Facebookavond die de politie Almere-Buiten vorige week organiseerde, heeft niks opgeleverd. Er kwamen geen meldingen van verdachte situaties. De facebookactie werd gehouden in het kader van het Donkere Dagen Offensief; burgers konden verdachte situaties of personen via facebook doorgeven. Ook de politie zelf had weinig te melden.

———————————————————-

De politie Oost-Nederland krijgt binnenkort een speciaal internetteam dat online prostitutie moet gaan controleren. Politiemensen gaan reageren op internetadvertenties waarin seks wordt aangeboden.

———————————————————

Een rechtbank in Denemarken heeft Lisa Broch (15) veroordeeld tot negen jaar celstraf voor het vermoorden van haar moeder. Broch keek samen met haar Iraakse vriendje Baktiar Abdullah (29) urenlang naar IS-video’s en stak daarna haar moeder twintig keer. Abdullah kreeg 13 jaar. Het meisje werd zo de zwaarst gestrafte tiener in Denemarken ooit. Volgens familieleden was ze in de ban geraakt van IS en deed ze weinig anders meer dan executiefilmpjes bekijken.

Index

Handig

opgeletopinternet.nl

Actuele phishingmails:

klik hier

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
Delta Lloyd Bank	Staal Bankiers
DHB Bank	Triodos Bank
Friesland Bank	Van Lanschot Bank
ING Bank	ASN Bank

Meldingen

Het KLPD heeft een Meldpunt Cybercrime waar burgers melding kunnen maken van kinderporno en radicale en terroristische uitingen die zij op het internet tegenkomen: www.meldpuntcybercrime.nl.

Voor het melden van identiteitsfraude kunt u terecht bij het Centraal Meld- en Informatiepunt Identiteitsfraude:

http://www.overheid.nl/identiteitsfraude.

Het CMI zorgt dat de juiste instanties uw melding afhandelen.

Het Meldpunt Internetoplichting van de politie en het Openbaar Ministerie samen met Marktplaats.nl maakt het voor burgers mogelijk om online melding en aangifte te doen van internetoplichting:

https://www.mijnpolitiebureau.nl/if.shtml.

Een klacht over spam kan worden ingediend bij de OPTA, die deze meldingen gebruikt voor handhaving van het spamverbod:

www.spamklacht.nl.

Meldingen over discriminatie kunnen ook worden gedaan bij het 'Meldpunt Discriminatie Internet' van de stichting Magenta:

http://www.meldpunt.nl.

Computerwoordenboek

POLITIE Meldpunt internetoplichting

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

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 een deel van de informatie die u daar heeft verstrekt door het Meldpunt Internetoplichting aan Marktplaats doorgestuurd.

Index

Cybercrime wetsartikelen

Wetsartikelen voor computercriminaliteit in enge zin

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

Voor cybercrime in enge zin zijn de volgende wetsartikelen beschikbaar:

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

. Artikel 161 sexies WvSr: opzettelijk veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk of werk voor de telecommunicatie.

. 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. afluisterapparatuur.

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.

————————————————————

Haatzaaien.

'Het zaaien van haat of het (opzettelijk) beledigen of discrimineren van een groep mensen wegens hun ras, hun godsdienst of levensovertuiging, hun hetero- of homoseksuele gerichtheid 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.

'Cyberstalking' is de verzamelnaam voor het stelselmatig lastigvallen van een persoon doorprovocerende 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.

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 Lanzarote 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 contactenmet 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').

————————————————————

Handel in mensen of foute goederen.

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.

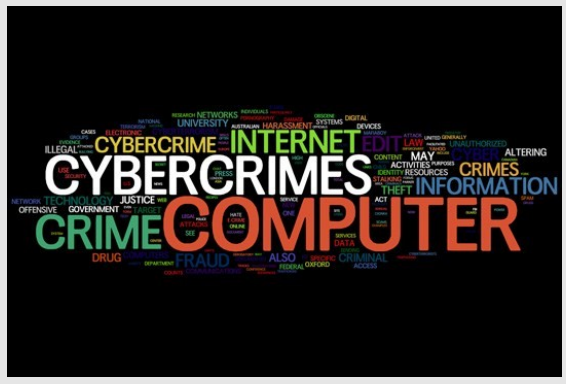
Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



Index

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 vervalsers, 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 groei-industrieën

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.

———————————————————————————

Index