Veilig Digitaal Magazine

Deepfake AI porno
Air Gap malware
Sypply Chain Attack
Binnen vijf jaar gaat helft van alle rechtszaken over cybercrime

en meer….

Jaargang 2 **April 2018**

INDEX

Veilig Digitaal Magazine is een uitgave van veiligdigitaal.com

Ga naar de Facebookpagina

Ga naar de website

Rubrieken:

2

Hoe air gap malware zonder internet toch toe kan slaan

Wat doe je als je een netwerk met zó veel gevoelige informatie hebt dat je iedereen koste wat kost bij je data vandaan wilt houden? Dan is het 'air-gappen' van je systeem één van de beste opties. Het infiltreren van zo'n netwerk is vaak zo ingewikkeld dat het amper de moeite waard is – maar dankzij air gap malware niet onmogelijk.

In 2011 raakten de turbines van de Iraanse kerncentrale Natanz ernstig verstoord. Deze turbines werkten plotseling veel te snel, waardoor ze zichzelf volkomen kapot draaiden. Stukje bij beetje werd duidelijk dat het controversiële atoomprogramma van het land was gesaboteerd door een agressief virus, maar hoe? Natanz was compleet afgesloten van het internet … De Amerikanen en Israëliërs deden er veel moeite voor om het 'air-gapped' netwerk te infiltreren.
Een air-gapped netwerk is een netwerk dat compleet is afgesloten van het internet en daarmee van de buitenwereld. Geen netwerkkabels naar buiten, geen wifi op apparaten, maar een geïsoleerd systeem. Het is de heilige graal van beveiliging, de ultieme stap om een computersysteem veilig te houden van de buitenwereld. Beveiligingsexperts en hackers proberen constant nieuwe manieren te vinden om air-gapped systemen af te luisteren en binnen te dringen. Maar hoe doe je dat? Hoe infecteer je het oninfecteerbare? Dat laatste blijkt nog wel het lastigste te zijn.

Kernwapens
Iedere paar maanden duikt er weer een bericht op, meestal van sensatiesites als Buzzfeed, dat laat zien hoe de Amerikaanse kernwapenfaciliteiten zogenaamd verouderd zijn. Er duiken dan fotoseries op waarop antieke, kamervullende computers te zien zijn, waarop enkel dos-achtige programma's draaien in zwart-witte lijnen code. De software wordt geladen van floppy's van acht inch.

Het 'Defense Department's Strategic Automated Command and Control System' (DDSACCS) is verouderd, geeft de Amerikaanse overheid zelf ook toe. Onderdelen die aan vervanging toe zijn, zijn nergens meer te krijgen. Floppy's zijn door hun magnetische opslag maar beperkt houdbaar en er zijn amper programmeurs te vinden die het oude IBM-platform uit de jaren 70 snappen.
Dat laatste is echter niet alleen een probleem, maar ook een uitkomst. Qua veiligheid gaat er namelijk niets boven een systeem dat niet te kraken is – en als niemand weet hóé je het moet kraken, lijkt dat een slimme stap.

Infrastructuur
De DDSACCS maakt gebruik van een eigen air-gapped netwerk, en het is niet de enige instantie die dat doet. Volgens beveiligingsexpert Jornt van der Wiel van Kaspersky worden air-gapped netwerken voornamelijk gebruikt bij systemen die sowieso niet van internet afhankelijk zijn om te functioneren. In de meeste gevallen gaat het dan om industriële systemen, zoals bij de faciliteit in Natanz ook het geval was. Kritieke infrastructuur wordt daarbij zoveel mogelijk offline gehouden om geen hackers van buitenaf binnen te laten. Het is daarnaast niet ondenkbaar dat ook instanties zoals de politie en de AIVD in ieder geval een deel van hun netwerk air-gapped hebben afgesloten, maar daarover doen beide diensten uit veiligheidsoverwegingen geen uitspraken.

Overigens worden in sommige air-gapped systemen alsnog verbindingen gebruikt waardoor dataverkeer op één of andere manier toch naar buiten kan, bijvoorbeeld met een data-diode waarbij gegevens via een proxy naar buiten kunnen worden gestuurd. Dat vermindert de veiligheid van zo'n netwerk echter wel, en het komt dan ook niet vaak voor.

Het infiltreren in een air-gapped systeem is dus voornamelijk bedoeld voor belangrijke en extreem gevoelige informatie, en zulke netwerken zijn dan ook gewilde doelwitten. Om die af te luisteren heeft een aanvaller dan ook fysieke toegang tot het systeem nodig. Dat is de voornaamste reden dat air-gapped netwerken zo veilig zijn, want het krijgen van fysieke toegang is vaak het lastigste proces – al is het vrijwel altijd noodzakelijk.

Op staatsniveau
Air-gapped malware-aanvallen en air-gapped datadiefstal zijn vaak zo ingewikkeld uit te voeren dat je al snel aan staatsniveau moet denken: de NSA, de FSB of Noord-Korea. Meestal betekent dat ook dat de aanvalsvector niet de simpelste is, want hoe krijg je toegang tot een vijandelijke instelling? In het geval van Stuxnet is nog steeds niet duidelijk hoe dat is gebeurd, maar er zijn wel vermoedens. Het virus werd via een usb-stick bij Natanz naar binnen gesmokkeld doordat de CIA vijf verschillende onderaannemers van de faciliteit wist te hacken – bedrijven die dus géén air-gapped netwerk hadden. Dat staat te lezen in het boek 'Countdown To Zero Day' van Wired-journalist Kim Zetter, die de cyberaanval onder de loep nam.

Door zich niet te richten op Natanz zelf, maar op bedrijven die componenten maakten voor Natanz, wisten de aanvallers uiteindelijk alsnog binnen te dringen in het verder afgesloten netwerk.

Hoe air gap malware werkt
Onderzoekers spelen al jaren een kat-en-muis-spel met air-gapped systemen, maar is er geen enkele groep zo belangrijk in het veld als het cybersecurity-lab van Mordechai Guri van de Ben Gurion Universiteit in Israël. Guri en zijn team komen keer op keer in het nieuws met nieuwe manieren om data van air-gapped systemen te onderscheppen.

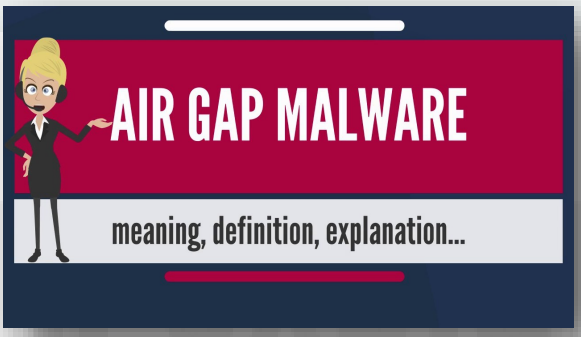
Bijna alle onderzoeken van Guri's team volgen hetzelfde patroon: een air-gapped systeem wordt binnengedrongen en er wordt malware op een computer of ander component geladen. Die malware manipuleert geluiden, lichten of de hitte van een computer, zodat die op een bepaalde manier corresponderen met de data die worden verwerkt. Het gaat bijna altijd om binaire data: knippert het ene lampje, dan is dat een 0, en als het andere lampje knippert een 1.

Ook bij andere methodes wordt zulke binaire informatie gebruikt: een ventilator die op 1.000 rpm draait telt als een 0, en 1.600 rpm telt als een 1. Een cpu met een temperatuur van 37 graden is een 0, 38 graden een 1 … Nadat de malware op het systeem is gezet, worden de nieuwe signalen afgeluisterd. Dat kan door een camera gebeuren die naar de lampjes van een pc of router kijkt, of met een smartphone in de buurt die de geluidssignalen van een computer opvangt.

Die aanpak werkt in bijna alle gevallen, en de onderzoekers proberen vooral nieuwe methodes te vinden waarop malware de data en de output van computers en randapparatuur kan manipuleren. Een relatief recente manier om dat te doen is via lichtsignalen, wat Guri en zijn team op twee manieren deden. In het eerste geval wisten de onderzoekers een virus genaamd xLed op een DD-WRT-router te laden dat door toegang tot de gpio-pinnen de routerledjes kon manipuleren op basis van de verwerkte data.

Door de lichtjes vervolgens af te lezen met een videocamera die op de router gericht stond konden de onderzoekers 8000 bits aan data per seconde achterhalen. Dat is net genoeg om binaire informatie zoals wachtwoorden en encryptiesleutels, en de inhoud van kleine bestanden te achterhalen.

Hoewel de onderzoekers proberen hun bevindingen tot een zo realistisch mogelijk scenario te maken (zoals het gebruik van een goedkope, doorsnee DD-WRT-router en een simpele camera zoals een GoPro) is het maar de vraag of een dergelijke penetratie in het echt makkelijk uit te voeren is. Daarvoor is namelijk fysieke toegang tot het systeem nodig en moet er alsnog een verbonden beveiligingscamera worden opgesteld, zodat het amper mogelijk lijkt een dergelijke aanval op te zetten.



Google Chrome gaat HTTPS-loze websites markeren als onveilig

Webbrowser Google Chrome gaat vanaf juli websites zonder veilige HTTPS-verbinding actief markeren als onveilig. Dat maakt het techbedrijf bekend op zijn blog. Websites die wel een veilige HTTPS-verbinding hebben, worden in de adresbalk van Chrome al gemarkeerd met een groen slotje en het woord 'Veilig'.

Bij websites die gebruik maken van HTTP in plaats van HTTPS ontbreekt dit slotje. In plaats daarvan geeft Chrome een waarschuwingsicoon weer. Pas wanneer gebruikers op dit icoon klikken, vertelt de webbrowser dat de website niet veilig is.

Vanaf juli gaat Chrome zijn gebruikers actiever waarschuwen. Naast het waarschuwingsicoon voegt Google in de adresbalk de woorden 'Niet veilig' of het woord 'Onveilig' toe.
Met de expliciete waarschuwing wil Google zijn gebruikers beter informeren over onveilige websites. Ook hoopt het bedrijf dat websitebeheerders hierdoor sneller overstappen van HTTP naar HTTPS.

Versleuteling
Met een HTTPS-verbinding versleutelen websites het verkeer van en naar hun website. Daarmee wordt het lastiger om verkeer af te luisteren.
Websitebezoekers die gevoelige gegevens, zoals wachtwoorden of persoonlijke gegevens, via een onveilige HTTP-verbinding versturen, lopen het risico dat deze gegevens onderschept worden door kwaadwillenden.

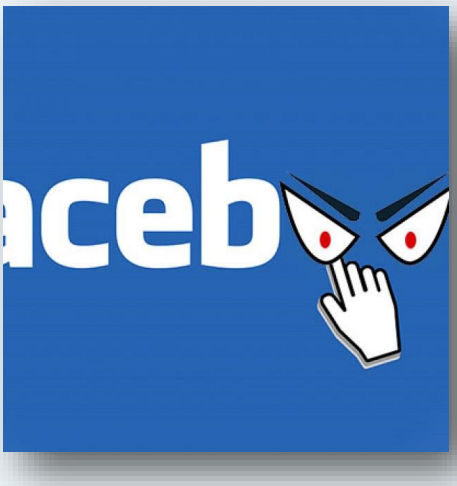
Consumentenbond: 'gebruik beveiligings-app van Facebook niet'

De Consumentenbond raadt smartphone- en tabletgebruikers af de beveiligings-app die Facebook promoot, te gebruiken. Facebook belooft met zijn Onavo Protect - VPN Security extra bescherming van persoonlijke gegevens, maar in feite schendt de app juist de privacy van gebruikers.

De app creëert een virtual private network (VPN) op je smartphone of tablet, om je te beschermen tegen meekijkende hackers. De meeste VPN-providers doen niets anders dan het verkeer omleiden, de data zelf laten ze ongemoeid.
Maar Onavo Protect werkt anders. De app analyseert continu ál het internetverkeer van het mobiele apparaat en deelt die kennis met Facebook en zijn advertentiepartners. De Onavo-app is al langer beschikbaar, maar Facebook promoot deze nu ook actief binnen de 'gewone' app.

Misleiding
De Consumentenbond vindt vooral de manier waarop Facebook de app aan de man brengt, niet deugen. Onder het misleidende mom van extra privacy en veiligheid verzamelt het bedrijf met de app alle denkbare gegevens van de gebruiker, zoals naam, telefoonnummer, apparaatgegevens, locatie, apps op het apparaat, bezochte websites. Facebook eigent zich het recht toe deze gegevens te analyseren én door te spelen aan andere partijen, maar dat is alleen te lezen in de volledige privacyverklaring die is weggestopt achter een link. In de verkorte versie van de verklaring die gebruikers bij de installatie zien, staat hier niets over.

Gebruik van een VPN is zeker aan te raden. Omdat de communicatie tussen jouw computer, smartphone of tablet versleuteld is, kunnen derden niet zien welke sites je bezoekt of wat voor e-mails je krijgt of stuurt. Zo blijf je anoniem, maar je kunt zo ook veilig openbare wifinetwerken gebruiken. Bijkomend voordeel is dat je landerestricties kunt omzeilen, bijvoorbeeld voor het kijken van bepaalde televisieprogramma's.

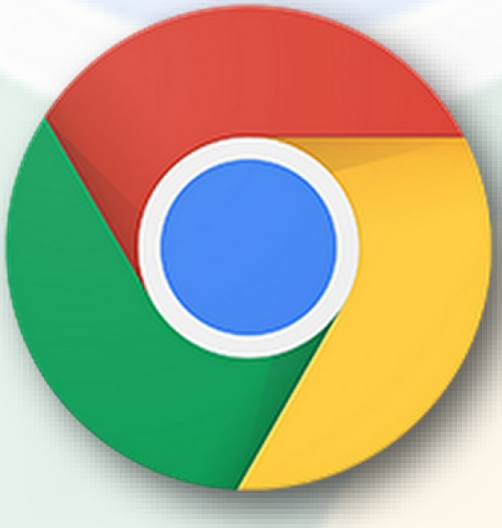


Adblocker in Chrome van start

Met ingang van nu blokkeert Google reclames die niet aan standaarden van de zoekgigant voldoen voortaan in de Chrome-browser.

De veranderingen werden vorig jaar in juni bekendgemaakt, maar treden donderdag 15 februari in werking. Het filter zorgt niet dat alle reclames worden geblokkeerd, maar alleen advertenties die niet voldoen aan de advertentierichtlijnen van de Coalition for Better Ads. Daarbij zijn onder meer Google, Facebook en The Washington Post bij aangesloten.
Google zegt dat één op de vijf feedbackformulieren van gebruikers meldingen bevatten over vervelende advertenties. Op de computer worden met name pop-up reclames en videoreclames die automatisch afspelen genoemd. Op mobiel gaat het bijvoorbeeld om beeldvullende advertenties en reclames die op een vaste plek blijven staan.

Beleid
Uitgevers krijgen van Google 30 dagen om aan de richtlijnen te voldoen. Verandert er niets en blijven "irritante" advertenties verschijnen, dan filtert Chrome ze zelf. Als websites hun reclamebeleid aanpassen, komen ze in aanmerking voor een herziening van het filter.
Google is voornamelijk een advertentiebedrijf en bereikt minder mensen als veel gebruikers adblockers inschakelen. Het bedrijf hoopt het gebruik van adblockers daarom te ontmoedigen met zijn eigen reclamefilter.



Europarlement wil af van geoblocking

Het Europees Parlement wil geoblocking en doorleiden naar een website van de winkel in een ander EU-land afschaffen. Dat is vooral goed nieuws voor fervente online shoppers.

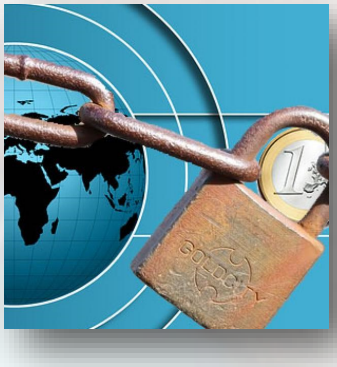
Geoblocking is het fenomeen dat je wordt doorgeleid naar een andere landsversie van bijvoorbeeld een webwinkel dan je gekozen had, maar het kan ook zijn dat een webshop in een ander land je betaalmiddel niet accepteert of dat je je op basis van je adres niet kunt registreren. Dat belemmert consumenten om goederen te kopen waar ze willen om zo de beste prijs te vinden.

Het Europees Parlement wil dat deze discriminatie wordt beëindigd, zodat mensen zowel online als offline kunnen profiteren van de geïntegreerde interne markt. Op 6 februari 2018 stemden de Europarlementsleden dan ook voor een verordening om een einde te maken aan geoblocking van klanten die een website in een ander EU-land bezoeken. De Europese Raad moet een en ander echter nog wel goedkeuren.

Materiaal dat beschermd is door auteursrecht zoals e-books en audiovisuele producten, is voorlopig van de wet uitgesloten, du voor die buitenlandse series zul je toch nog van een omweg via bijvoorbeeld VPN gebruik moeten maken.

Online winkelen maakt deel uit van het dagelijks leven van veel Europeanen: 57% van de EU-burgers heeft in 2017 online iets gekocht. Daarnaast is online winkelen één van de favoriete activiteiten van internetgebruikers: 68% van de internetgebruikers winkelde online in 2017. In 2017 kocht een derde van de online shoppers bij een winkel in een ander EU-land.

Uit een studie van de Europese Commissie die duizenden websites in de EU heeft geanalyseerd, bleek dat in slechts 37% van de gevallen gebruikers uit een ander EU-land de aankoop konden voltooien en de goederen konden kopen die ze wilden. In de andere gevallen ondervonden gebruikers geoblocking in een of andere vorm.



Deep fake AI-porno problematisch en moeilijk te stoppen

Reddit, Twitter en zelfs Pornhub proberen het fenomeen al aan banden te leggen, maar de opmars van nep-pe AI-porno, ofwel 'deep fake', lijkt niet te stoppen. En dat levert problemen op.

De term staat voor het gebruiken van foto's van gezichten in andere beelden - in dit geval de gezichten van beroemdheden die 'gephotoshopt' worden in bestaande pornovideo's.

Beroemdheden als gewilde doelwitten

Beroemdheden zijn al jaren een gewild doelwit van perverselingen. 'The Fappening' staat nog vers in het geheugen, toen de iCloud-accounts van tientallen vrouwelijke entertainers werden gehackt en duizenden naaktfoto's over het web werden verspreid. De dader werd later opgepakt en veroordeeld voor 18 maanden, maar daarmee is de interesse in gewone actrices en zangeressen in seksuele posities en situaties niet minder geworden.

Dat kan sinds kort met deep fake-AI-porno, waarmee 'gewone' gezichten in bestaande porno-video's worden geplakt.

Deep fakes

De term 'deep fake' om de porno te beschrijven lijkt van een Reddit-gebruiker genaamd DeepFakeApp te komen. Hij ontwikkelde in december een experimenteel desktopprogramma (vernoemd naar zichzelf) om dergelijke fake video's en gifjes te maken - voornamelijk pornografisch materiaal met beroemdheden. Hij zette de applicatie online en begon een community op Reddit, die al snel tienduizenden volgers kreeg.

Machine learning

Het programma maakt gebruik van open source machine learning-algoritmes zoals Googles TensorFlow. Een gebruiker hoeft het maar te downloaden en er een batch foto's aan toe te voegen om zelf al een video te maken.

Verboden op sociale media

Het gemak waarmee geruikers met deep fake-algoritmes video's kunnen maken zorgt voor problemen bij sociale media zoals Reddit of Twitter. Die waren er dan ook snel bij om hun regels aan te passen en nagemaakte content te blokkeren. Reddit en Twitter zijn, in tegenstelling tot bijvoorbeeld Facebook of Instagram, normaal gesproken erg tolerant wat porno betreft. Dat deep fake-video's dan ook zo snel verboden worden is veelzeggend. Inmiddels is de subreddit /r/deepfakes gebanned van de website. Een afgeleide subreddit genaamd /r/fakeapp bestaat nog steeds, opgericht door een gebruiker genaamd DeepFakes - waarvan wordt aangenomen dat het óf dezelfde persoon is als DeepFake-App, of in ieder geval iemand met wie hij nauw samenwerkte.

In tegenstelling tot die oude subreddit is het in /r/fakeapp ten strengste verboden om niet-wederzijdse porno te plaatsen. Daar staat een ban op. Toch lijkt een groot gedeelte van de discussies op de subreddit te draaien om pornografie, en worden er vooral veel links gedeeld naar fora waar die beelden wél verspreid mogen worden.

Pornosites tegen deep fakes

Het zijn niet alleen sociale media die worstelen met het fenomeen. Ook 's werelds bekendste pornosite Pornhub verbiedt het plaatsen van deep fakes, maar de manier waarop dat moet gebeuren is nog onduidelijk. Een snelle zoekterm op de site laat op moment van schrijven 47 actieve deep fake-pornovideo's zien met verschillende bekende actrices. Pornhub zegt zelf dat het deep fake-video's behandelt zoals iedere andere vorm van content: als iemand een verwijderverzoek indient vanwege copyright-schending of wraakporno.

Maar juist die aanpak krijgt veel kritiek. Pornhub is juist groot geworden door het feit dat de website zo overspoeld wordt door video's dat copyright-houders niet tegen het enorme volume kunnen opvechten en het daarom maar opgeven.

Vechten tegen de bierkaai

Bovendien is het effect van één website (hoe invloedrijk dan ook) vechten tegen de bierkaai. Er zijn immers tienduizenden andere sites die maar wat graag verkeer trekken met dergelijke video's, zoals het relatief onbekende EroMe waar nu al tientallen deep fakes op worden aangeboden. Ook zijn er al een groot aantal forums online gekomen waar het delen van video's wordt gestimuleerd - het duurde ons niet veel langer dan 5 minuten om zulke websites te vinden.

Machine learning

AI-porno wordt gemaakt met machine learning-algoritmes. Waar die tot een paar jaar geleden nog voornamelijk voor onderzoekers beschikbaar waren wordt het steeds makkelijker voor doorsnee gebruikers om op die manier dergelijke nepvideo's te maken.

Netwerken zoals TensorFlow van Google zijn inmiddels open source beschikbaar, en gratis te gebruiken voor studenten en onderzoekers, maar ook voor iedereen die wil experimenteren met machine learning.

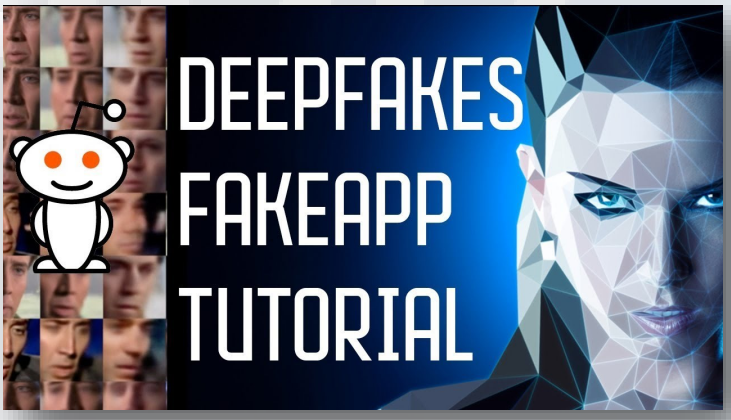
Dat leidt tot apps zoals Deep Fake, die nu gratis te downloaden zijn en die uitgerekend een gebruiksvriendelijke interface hebben.

Makkelijk te maken

Programmeurs hebben dan enkel nog een aantal foto's of video's nodig om de beelden zo echt mogelijk te laten lijken. Daarom zijn beroemdheden zo aantrekkelijk voor het maken van de video's. Via Google en YouTube zijn met een paar zoektermen miljoenen beelden van een actrice beschikbaar.
Opvallend is ook dat voor machine learning geen industriële high-end hardware nodig is. Met gewone consumenten-gpu's en -cpu's is het al mogelijk om beelden te renderen - al is het natuurlijk afhankelijk van de kracht van een chip hoe snel dat gebeurt.

Gewone mensen

Omdat het steeds makkelijker wordt zulke beelden te maken is het maar de vraag wanneer het niet meer alleen over beroemdheden gaat, maar ook over 'gewone mensen'; de kennissen, vrienden of zelfs familie van een maker. Hoe geavanceerder de algoritmes worden, des te makkelijker het wordt om beelden te genereren. Experts voorspellen dan ook dat het in de toekomst doodnormaal wordt om zelfgemaakte porno te maken met wie je dan ook wil zien.



Legaliteit

Het is dan ook maar de vraag of zulke namaakporno wel legaal is, maar gek genoeg is dat niet zo makkelijk als het lijkt.
Daarbij kun je de link leggen met wraakporno, ook een relatief nieuw concept dat in groeiende mate problematisch wordt. Wraakporno is pornografisch materiaal dat door iemand anders wordt geüpload, vaak door bijvoorbeeld een rancuneuze ex.

"Verwerking van persoonsgegevens"

Aan de oppervlakte voelt het alsof deep fake-porno illegaal is - het is in ieder geval zwaar onethisch. Maar is het ook echt tegen de wet? Volgens Arnoud Engelfriet van ICT Recht wel, maar niet rondom dezelfde principes als wraakporno. Neppe porno is volgens Engelfriet 'een geautomatiseerde verwerking van een persoonsgegeven', en daarvoor zou de maker uitdrukkelijke toestemming nodig hebben.
Voor zover bekend heeft er nog geen rechter uitspraak gedaan over het fenomeen, maar als dat gebeurt kan dat leiden tot een precedent waarin het maken van neppe porno inherent wordt verboden.

Van de andere kant: wie houdt zich nou netjes aan zo'n uitspraak?

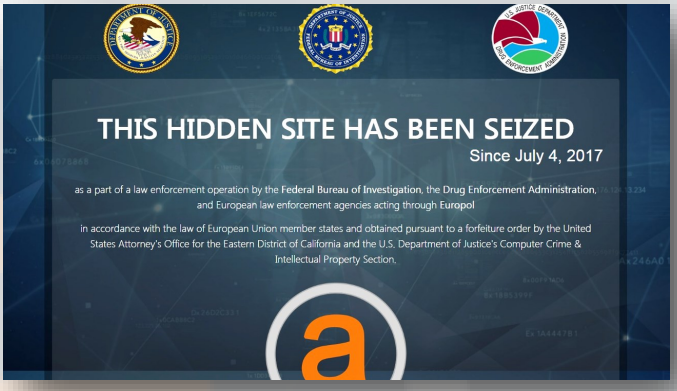
Recherche over de vloer bij ‘anonieme’ kopers

Enkele tientallen klanten van de vorig jaar opgerolde illegale marktplaats Hansa hebben de afgelopen dagen de politie aan de deur gehad.

Bij deze actie, die december 2017 al wasaangekondigd, gaat het om mensen die dachten dat ze anoniem drugs kochten op Hansa.
Maar wat ze (vooral mannen tussen 20 en 30 jaar) niet wisten, was dat de Nederlandse politie het beheer over Hansa had overgenomen.

In totaal is op 41 adressen in heel Nederland zo’n ‘knock-and-talk’ bezoekje gebracht. 37 klanten waren thuis. ‘Hallo, wij zijn van de politie, mogen we even binnenkomen’. Volgens projectleider Nanina van Zanden van de politie zat de schrik er bij de meesten goed in. ‘Dat wij ze gevonden hebben, hadden ze niet verwacht’.

Van Zanden vertelt dat de drugskopers ook uitgelegd is dat het gevaarlijk is, drugs kopen van anonieme dealers, en bovendien toch niet zo anoniem als gedacht. De meeste kopers worden vanwege de geringe (gebruikers)hoeveelheden drugs die ze kochten, niet vervolgd. Een man (25, uit Wilp) die 150 xtc-pillen bestelde, werd wel aangehouden.



Supply-chain-aanvallen: wat is het en hoe werkt het?

Supply-chain-aanvallen
Een supply-chain-aanval is een aanval waarbij een bedrijf of individu wordt getroffen door een aanval die vanuit een leverancier (een 'supplier') wordt uitgevoerd. In veel gevallen is dat een aantrekkelijke manier van malwareverspreiding of spionage.
Supply-chain-aanvallen hebben een paar voordelen ten opzichte van andere aanvallen: het kan bijvoorbeeld soms makkelijker zijn om een bedrijf te infecteren.

Een keten is zo sterk als zijn zwakste schakel: een willekeurig slecht beveiligd bedrijf in de toeleveringsketen kan dan makkelijk al zijn klanten én diens klanten infecteren. Dat is best logisch: waarschijnlijk heeft een maker van bijvoorbeeld boekhoudsoftware zijn beveiliging minder goed op orde dan een bedrijf dat beveiligingssoftware maakt.

McAfee zag bijvoorbeeld ooit een voorbeeld van een supply-chain-aanval die via een update voor de gpu van computers werd uitgevoerd. "Dat is slim, want je verwacht van een gpu-update niet dat er veel mis mee kan zijn", vertelt Christiaan Beek, lead scientist & principle engineer bij McAfee. "Je vertrouwt het dus eerder. Een gpu-fabrikant controleert updates waarschijnlijk minder goed dan een bedrijf dat zich enkel richt op software."

Het opzetten van een supply-chain-aanval is op zichzelf niet moeilijk, denkt Beek, maar het efficiënt uitvoeren van een aanval wel. "Een command-and-control-server beginnen en malware schrijven die daar bepaalde gegevens naartoe stuurt is simpel. Het lastige is juist om het zo lang stil te houden."
In veel gevallen wordt de malware niet (of erg laat) opgemerkt door antivirussoftware, omdat die niet precies weet waarnaar moet worden gezocht.

Effectief
Het is een beetje raar om anno 2017/2018 nog te spreken over 'de opkomst van het internet', maar de digitalisering en de toenemende hoeveelheid gegevens van klanten en gebruikers bij bedrijven is wel reden voor minder geavanceerde criminelen om supply-chain-aanvallen serieus te nemen.
Volgens Michael van der Vaart, CTO van ESET Nederland, zijn Petya en CCleaner slechts het begin van wat een steeds populairdere methode van infectie gaat worden. "Criminelen kijken goed naar elkaar en leren zo wat goed werkt." De voorbeelden van Petya en CCleaner lieten precies dat op pijnlijke wijze zien.

Bedrijven vs. consumenten
Er zijn ruwweg twee soorten supply-chain-aanvallen. Aan de ene kant is er de soort die zich richt op bedrijven die op zichzelf moeilijk te infiltreren zijn, maar waarbij een leverancier mogelijk een zwakke plek in zijn systeem heeft.
Die vorm van bedrijfsspionage is al jaren oud. Maar er is tegenwoordig ook een nieuwe vorm van supply-chain-aanvallen, waarbij juist een grote massa eindgebruikers wordt aangepakt.

De CCleaner-aanval in augustus 2017 is daarvan het bekendste voorbeeld, maar ESET en ook andere beveiligingsbedrijven zoals Kaspersky ontdekten zowel vorig jaar als dit jaar steeds meer gevallen van dergelijke malware die op deze manier verspreid werd, zie ook het kader 'Voorbeelden aanvallen'.

Volgens Van der Vaart zijn eindgebruikers, gewone consumenten dus, steeds vaker het doelwit van zulke aanvallen. "Je ziet dat in malware die ESET heeft gevonden in bijvoorbeeld video-encoder Handbrake, of in oktober in een populaire videospeler voor macOS.
Criminelen vinden de massa steeds interessanter en zullen vaker supply-chain-aanvallen gebruiken om gewone consumenten te infecteren."

Moeilijk te detecteren
Supply-chain-aanvallen zijn voor veel criminelen ook aantrekkelijk omdat ze moeilijk te detecteren zijn in een systeem. Beek: "Het duurt vaak heel lang voordat je een infectie opspoort, en dat is criminelen veel waard. Hoe langer je in een systeem zit, hoe meer informatie je kunt verzamelen."

Van der Vaart is het daarmee eens. Hij benadrukt dat het lastig is voor antivirussoftware om lekken op te sporen. "Dat lukt vaak wel als we heel gericht gaan zoeken; dan kunnen we bijvoorbeeld redelijk makkelijk de command-and-control-server van een malafide applicatie vinden. De moeite is echter om in de eerste plaats te vinden wáár je onderzoek moet gaan doen."

Infiltratie waardevol
Maar als een crimineel dan eindelijk in een systeem is binnengedrongen, wat is dan het einddoel? Van CCleaner is tot op de dag van vandaag niet precies bekend wat het doel was, maar alles wijst erop dat de trojan bedoeld was om gebruikers te bespioneren.
Alleen ... welke gebruikers? Was de hack bedoeld om zo veel mogelijk argeloze downloaders te infecteren, of zocht de trojan naar iets specifieks?

Zowel Van der Vaart als Beek kunnen er alleen maar over speculeren, maar beiden vermoeden dat het waarschijnlijk vooral bedrijven waren die de dupe werden. De overige downloaders waren dan eerder 'collateral damage'. Vooral Beek denkt niet dat de trojan was bedoeld om bijvoorbeeld op een later moment ransomware te verspreiden, zoals al snel na de hack werd gespeculeerd. "Daarvoor is een dergelijke infiltratie te waardevol. Het kost redelijk veel moeite om in een bedrijfsnetwerk terecht te komen, en al helemaal om daar zo lang onopgemerkt te blijven. Dat voordeel wil je niet verspillen aan ransomware."
Beek denkt dat spionage, en dan met name gerichte bedrijfsspionage, interessanter is voor hackers. Ransomware is al lucratief genoeg en heeft met gewone phishingcampagnes al voldoende effect wat betreft het aantal infecties.

Onbekende daders
Je kunt je dan ook afvragen wie er doorgaans achter supply-chain-aanvallen zitten, maar ook daarover is eigenlijk weinig concreets te zeggen. Beek denkt dat je dan groot moet denken: aan 'nation states' en inlichtingendiensten. Van der Vaart denkt eerder dat dat het 'gewone' hackers zijn. Al zijn beiden het er wel over eens dat het geen 'script kiddies' zijn en dat er wel meer kennis nodig is dan gemiddeld om zo'n aanval uit te voeren.

Beveiligingsadvies

Het probleem met supply-chain-aanvallen (en dan met name de preventie ervan) voor gewone consumenten, is dat het regelrecht indruist tegen al het beveiligingsadvies dat de industrie al decennia probeert door te voeren.

Dat advies is namelijk: schakel auto-updates in, want daarmee voorkom je dat er misbruik wordt gemaakt van lekken in je software. Echter: supply-chain-aanvallen via malafide updates staan haaks op het feit dat updates een harde noodzaak in software zijn. Als je je tegen dit soort aanvallen wilt beschermen, dan zou je in theorie juist niet moeten updaten .

Van der Vaart denkt echter niet dat dat altijd-update-advies het raam uit kan. “Het gevaar dat je oploopt door auto-updates uit te schakelen, staat niet in verhouding tot het mogelijke risico op een supply-chain-aanval, dus je hoeft dat echt niet tegen elkaar af te wegen.” Hij vertelt verder: “ESET ziet steeds meer gevallen van supply-chain-aanvallen die gericht zijn op consumenten, maar in totale aantallen valt dat gelukkig nog mee.”

Om ransomware weer als voorbeeld aan te halen: het risico op een besmetting en de schade daarvan zijn vele malen groter dan die van een aanval als die van CCleaner. Beek onderschrijft dat, mede omdat het risico van besmetting zo klein is: “Omdat dergelijke malware vaak zo gericht wordt verstuurd, is er maar een kleine kans dat je zo wordt geïnfecteerd.”

Hash

Is er dan niets dat je zelf kunt doen om te voorkomen dat je slachtoffer wordt? Jawel, maar het detecteren en stoppen van zo'n aanval is voor de gemiddelde computergebruiker (te) lastig en tijdrovend. Volgens Beek en Van der Vaart kunnen consumenten bijvoorbeeld de MD5- of SHA1-hash controleren van een programma dat zij downloaden.

Het is niet gek als je bij die begrippen even achter de oren krabt, want zulke vorm van downloadauthenticatie wordt nog maar weinig gebruikt door de gemiddelde gebruiker. Toch een korte uitleg: je controleert of de hash op een website hetzelfde is als die van je download, daaraan kun je dan zien of het programma aangepast is sinds het online is gezet.

Een eerste probleem is dat zo’n hash bij maar weinig softwaredownloads makkelijk te vinden of te gebruiken is (als die er überhaupt is). Je vindt hem vooral wel bij software die specifiek gericht is op privacy, zoals de Tor-browser of het beveiligde besturingssysteem Tails. Een tweede moeilijkheid is dat dat bedrijven vaak geen idee hebben hoe diep hackers in een systeem zijn geïnfiltreerd.

Dus áls een consument al de stap neemt om de hash van een download te verifiëren met wat er op een website staat, hoe weet hij dan dat die hash niet óók is aangepast door de indringers?

En de derde en belangrijkste belemmering is dat er een cultuuromslag zou moeten plaatsvinden voordat consumenten bij iedere download alle moeite nemen om de hash te controleren.

Supply-chain-aanvallen zijn nog maar een marginale bedreiging en dit zal daarom niet snel een reden zijn om daar zulke maatregelen tegen te treffen.Voor jou als gewone gebruiker is er daarom weinig tegen supply-chain-aanvallen te doen, behalve de vrij standaard security-maatregelen die je (hopelijk!) al neemt. Gebruik een goede virusscanner, laat software gewoon automatisch updaten en gebruik vooral je gezond verstand.

Versleutel je harde schijf op Windows 10 Pro

In een ideale wereld zou je op elke computer encryptie gebruiken, maar dat blijft spijtig genoeg nogal vaak achterwege. Op Windows 10 Pro en Enterprise heb je echter een ingebouwde tool die de bestanden op je computer versleuteld.
Het enige wat je hoeft te doen om van de bescherming te profiteren, is deze in te schakelen. Om de extra veiligheid te garanderen zal je computer iets minder snel reageren. Je zal dus moeten afwegen wat je het belangrijkste vindt.

BitLocker is een tool die encryptie op een volledige drive uitvoert. Je kan zelf kiezen welke drives je op je pc met BitLocker encrypteert. Wil je BitLocker toepassen op je systeemdrive, dan zijn er wel wat voorwaarden die je in acht moet nemen. Normaal gezien kan je BitLocker enkel gebruiken op een systeemschijf als je computer een Trusted Platform Module (TPM) bevat, een hardwarecomponent op je moederbord. Er is echter een omweg waarbij je toch de encryptie op de schijf kan activeren zonder TPM. Deze methode is minder veilig, maar nog altijd beter dan geen encryptie.

Geen TPM
Als je een TPM hebt, kan deze stap overslaan. Open het 'Uitvoeren'-venster met de sneltoets 'Win+R' en tik 'gpedit.msc' in. Dit opent de Groepsbeleid-editor op je computer. Vervolgens moet je door verschillende mappen navigeren: 'Computerconfiguratie', 'Beheersjablonen', 'Windows-onderdelen', 'BitLocker-stationsversleuteling' en tot slot 'Besturingssysteem-stations'. Dubbelklik in de rechterkant van het venster op de optie 'Aanvullende verificatie bij opstarten vereisen' en selecteer 'Ingeschakeld' in het venster dat je te zien krijgt. Zorg er ook voor dat je onderaan de optie om Bitlocker toe te laten zonder TPM aanvinkt en klik op 'OK' om de aanpassingen door te voeren.

Activeren
Om BitLocker te activeren open je Windows Verkenner en klik je met je rechtermuisknop op de drive die je wil versleutelen. Klik op de optie 'BitLocker inschakelen' en er zal een set-upwizard verschijnen. Het eerste dat je moet doen is een ontsluitingsmethode kiezen. Heb je geen TPM en gaat het over je systeemdrive, dan zijn er twee keuzes: een USB-sleutel, of een wachtwoord.

Met een TPM heb je de optie om je drive automatisch te laten ontsleutelen tijdens het opstarten. Je kan ook een pincode of biometrische authenticatie gebruiken. Bij een gewone drive krijg je altijd standaard twee keuzes: een wachtwoord of een smart card. Maak je keuze en configureer BitLocker.

Herstelsleutel
Nadat je de ontsleutelingsmethode voor BitLocker hebt gekozen, zal Microsoft je vragen waar je je herstelsleutels wil bewaren. Deze dienen als noodoplossing mocht je ooit je wachtwoord vergeten of USB-sleutel kwijtspelen. Je kan van alle bewaaropties gebruik maken, ze sluiten elkaar niet uit. Vervolgens schuift Microsoft nog wat dilemma's naar voor: welk deel van de drive wil je encrypteren, en welk type van encryptie je wil gebruiken.

De vensters leggen helder uit welke keuze de optimale is voor welk systeem. Heb je je keuzes gemaakt, dan ben je bij het einde beland. Om BitLocker in gang te zetten, klik je op 'Start encryptie'. Versleutel je je systeemschijf, dan krijg je nog de optie om een systeemcontrole uit te voeren. Bevestig de controle, en start vervolgens je pc opnieuw op. Windows zal na het booten beginnen met het encryptieproces.

Afhankelijk van de grootte van de schijf kan de tijdsduur variëren. Bij een gewone drive begint de encryptie meteen zonder herstart.

FIFA 2018 en Bitcoin meest gebruikt voor spam en phishing

Volgens het rapport 'Spam and phishing in 2017' van Kaspersky Lab hebben criminelen een wereldwijde agenda. Ze hebben zich de afgelopen twaalf maanden gericht op populaire verschijnselen als FIFA 2018 en Bitcoin om gebruikers om de tuin te leiden en hen geld of persoonlijke informatie afhandig te maken.

Spammers hebben inmiddels ruimschoots bewezen dat ze bedachtzaam te werk gaan. Over de hele wereld houden ze belangrijke kwesties en grote evenementen scherp in de gaten, met het doel de aandacht van hun slachtoffers te trekken en hier misbruik van te maken. Het doorlopende onderzoek van Kaspersky Lab naar spam- en phishing-activiteiten bevestigt dat de methoden die spammers hanteren effectief zijn, omdat de aandacht van het publiek verslapt en het vertrouwen alleen maar groter wordt. Deze factoren tezamen hebben tot gevolg dat mensen eerder geneigd zijn valse instructies op te volgen.

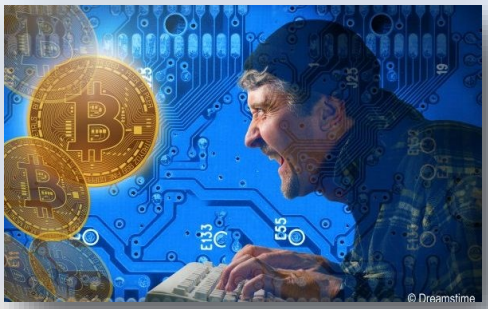
Gratis kaartjes

Terwijl de wereld zich in 2017 aan het voorbereiden was op FIFA 2018, waren spammers volop in de weer met het verspreiden van gerelateerde e-mails. Zo hebben ze slachtoffers frauduleuze berichten gestuurd met officiële logo's van het evenement en informatie over de organisatoren en sponsoren. Ook werden gebruikers geïnformeerd over gewonnen loterijen en werd hen zelfs gratis kaartjes beloofd.

Een ander actueel onderwerp van spam en phishing in 2017 was crypto currency, aangezien de waarde van de Bitcoin drastisch steeg in 2017.

Onderzoekers van Kaspersky Lab hebben al in het derde kwartaal van 2017 een toename in blockchain-gerelateerde trucs vastgesteld. Tegen het einde van het jaar was een uitgebreid arsenaal aan spamgereedschappen in kaart gebracht.

Over het geheel genomen is de gemiddelde hoeveelheid spam in 2017 gedaald tot 56,63 procent, wat 1,68 procentpunten minder is dan in 2016. Tegelijkertijd is het aantal phishing-aanvallen toegenomen: het Anti-Phishing-systeem van Kaspersky Lab werd 246.231.645 keer geactiveerd op computers van gebruikers van Kaspersky Lab-producten, een toename van bijna 59 procent ten opzichte van 2016.



Halt geeft meer aandacht aan online jeugdcriminaliteit

Halt houdt zich bezig met beginnende jeugdcriminaliteit. Steeds vaker vindt deze jeugdcriminaliteit online plaats, zoals ongewenste sexting, online pesten en cybercrime. Halt heeft hiervoor in 2017 verschillende nieuwe interventies ontwikkeld.

In 2017 is Halt met een aantal pilots gestart om online grensoverschrijdend gedrag bij jongeren te straffen en herhaling te voorkomen.
Met de nieuwe Halt-interventie sexting: Respect online heeft Halt, samen met het kenniscentrum seksualiteit Rutgers, een passende aanpak ontwikkeld bij ongewenste sexting, online seksuele pesterijen of beledigingen.
Het is een individueel gerichte interventie waarbij de focus ligt op bewustwording van veilig en respectvol online (seksueel) gedrag.

Cybercrime
Ook heeft Halt in 2017 als pilot een aantal 'cyberzaken' behandeld. Bij deze pilot hebben het Openbaar Ministerie, de Raad voor de Kinderbescherming en Halt nagedacht over een passende straf. Als onderdeel van de Halt-interventie moesten de jongeren een werkopdracht uitvoeren bij een IT-bedrijf.
De IT-bedrijven werkten mee om het risicovol en strafbaar online gedrag van jongeren om te zetten naar het inzetten van talent op een legale manier.

Om online jeugdcriminaliteit te voorkomen, geeft Halt lessen in online veiligheid in het basis- en voortgezet onderwijs over de risico's van online grensoverschrijdend gedrag.

Ouders aan zet
Een andere pilot waar Halt in 2017 mee is gestart is om ouders een grotere invloed te geven op de Halt-interventie. Ouders spelen altijd al een belangrijke rol in de Halt-interventie door aanwezig te zijn bij de gesprekken met jongeren.
Maar de pilot 'Ouders aan zet' gaat nog wat verder. Hierin krijgen ouders meer inspraak in het bepalen van de straf van hun kinderen.
De gedachte van Ouders aan zet is dat ouders levenslang verbonden zijn met hun kind en dat zij als geen ander weten wat hun kind nodig heeft.

Tweede kans
Jongeren experimenteren, dat hoort bij hun leeftijd. Daarbij denken ze niet altijd goed na over de gevolgen. Als jongeren van 12 tot 18 jaar grenzen overschrijden, biedt Halt een tweede kans.
Jongeren die bij Halt komen krijgen een interventie met een focus op het pedagogisch effect: wat helpt de jongere om niet opnieuw de fout in te gaan?
"Dit doen wij door de jongeren te leren de gevolgen van het eigen gedrag in te zien, dit gedrag te herstellen en gedragsalternatieven aan te leren. Door het positief doorlopen van de Halt-interventie voorkomen deze jongeren dat zij een strafblad krijgen en behouden zij een kansrijke toekomst".

In 2017 heeft Halt zo'n 17.000 jongeren deze kans gegeven.

Bron: HALT

Hulp voor alle bedrijven tegen risico's cybercrime

Drie initiatieven: zelfde doel, andere aanpak.

Het Ministerie van Veiligheid en Justitie opende in 2012 het Nationaal Cyber Security Centrum en dit jaar richtten Cisco, Dearbytes, KPN en McAfee de stichting Cyber Central op. Daarnaast kondigde het ministerie van Economische zaken aan dat in 2018 het Digital Trust Centre zijn deuren opent.
Alle initiatieven zetten in op samenwerking tussen ondernemers en kennisdeling, maar hun doelgroepen en aanpak verschillen.

Het eerste is het Nationaal Cyber Security Centrum (NCSC). Dit richt zich voornamelijk op de Rijksoverheid en organisaties in de vitale infrastructuur, zoals water- energie- en telecombedrijven. Het centrum is het Nederlandse aanspreekpunt op het gebied van ICT-dreigingen en cybersecurity-incidenten.
Het NCSC deelt actuele dreigingen en geeft beveiligingsadviezen: hoe richt je als ondernemer bijvoorbeeld succesvol een Security Operations Center (SOC) in en hoe bescherm je een domeinnaam tegen phishing?

Het tweede wordt het Digital Trust Centre (DTC). Het grootste deel van de Nederlandse bedrijven kan bij cybercalamiteiten niet terecht bij het NCSC en is op zichzelf aangewezen.

Daarom start de overheid dit jaar het Digital Trust Centre. Het doel van het DTC is om in nauwe samenwerking met het NCSC het gehele bedrijfsleven weerbaarder te maken tegen cyberdreigingen.
Het DTC gaat bedrijven adviseren over dreigingen en maatregelen. Bovendien helpt dit kenniscentrum samenwerkingen tussen bedrijven tot stand te brengen op regionaal niveau en binnen branches.

Nummer drie is Cyber Central. De stichting Cyber Central is een initiatief van vier marktpartijen.

Volgens Cyber Central kan niemand de strijd tegen cybercriminaliteit alleen winnen. Daarom is het belangrijk dat cybersecurity voor iedereen begrijpelijk is. Zodat ondernemers bijvoorbeeld weten welk beleid ze moeten uitzetten en medewerkers aanvoelen hoe ze veilig kunnen werken.

Cyber Central vergroot die kennis onder meer met workshops waarin cyberaanvallen worden gesimuleerd. Daarnaast organiseert Cyber Central een maandelijkse bijeenkomst, vrij toegankelijk, met wisselende thema's. Voor dit initiatief staat het beleven van digitale veiligheid centraal.

Downloaden zonder te betalen meest gepleegd cyberdelict

Jongeren beoordelen fysieke overtredingen ernstiger dan online varianten van hetzelfde vergrijp. Zo keurt 81 procent het af om een dvd uit een winkel te stelen. Als het gaat om illegaal downloaden, beschouwt slechts 6 procent dit als verkeerd. Dat blijkt uit het onderzoek Safer Internet Day 2018: Cybercrime.

Het onderzoek wijst verder uit dat 37 procent van de ondervraagde jongeren weleens illegaal gedownload heeft, terwijl zij weten dat het verboden en strafbaar is. Twintig procent van de respondenten zegt illegaal downloaden te overwegen. Vijf procent heeft weleens een online-product gekocht tegen een prijs die te mooi is om waar te zijn (heling).

Niet strafbaar maar wel veel gedaan, is valsspelen in een online game: 20 procent van de ondervraagden geeft aan dit weleens te hebben gedaan en 22 procent zou valsspelen overwegen. 7 procent geeft aan iemand online gepest of beledigd te hebben.

BREIN-directeur Tim Kuik: “Ik denk dat het verschil in beoordeling tussen fysiek en online ook te maken heeft met anonimiteit van zowel de dader als het slachtoffer. De illegale downloader weet wel dat hij of zij iets verkeerd doet maar waant zich anoniem op internet. Het slachtoffer is niet zo herkenbaar als een meneer of mevrouw achter een toonbank. Mijn ervaring in gesprekken met jongeren is dat zij zeggen dat ze doorgaan met illegaal downloaden en streamen zolang er geen boete op staat. ‘Omdat het gratis is’, geven zij op als de belangrijkste reden. Op de tweede plaats komt de legale beschikbaarheid.” Kuik geeft muziek als voorbeeld. “Dit segment wordt minder illegaal gebruikt dan voorheen vanwege de ontwikkeling van legaal aanbod.

Wat daarbij steekt is dat er meer muziek wordt geluisterd dan ooit maar het voor artiesten moeilijker dan ooit is om hun brood ermee te verdienen. De top 1 procent uitgezonderd. Het grote geld verdwijnt in de zakken van YouTube en die deelt die rijkdom onvoldoende met de makers. Voor series hoor je dat jongeren niet willen kiezen tussen de verschillende legale online platforms. Als ze een abonnement op een dienst hebben en er staat populaire serie op een andere dan zijn ze geneigd die dan maar illegaal te downloaden of streamen.
Toch is het juist de concurrentie tussen legale platforms die de kwaliteit en hoeveelheid van het aanbod aanzwengelt. Daar heeft de consument baat bij.”

Bron: BREIN

Binnen vijf jaar gaat helft van alle rechtszaken over cybercrime

Binnen vijf jaar is de helft van de zaken die voor de rechter verschijnt een zaak van online criminaliteit. Daarbij moet gedacht worden aan diefstal via internetbankieren, maar ook aan tentamenfraude en het kraken van computersystemen van bedrijven. Dat zegt Bart Jacobs, professor digitale veiligheid aan de Radboud Universiteit in Nijmegen.

Justitie in Nederland krijgt het snel drukker met de bestrijding van cybercriminaliteit. In Oost-Nederland pakte het Openbaar Ministerie vorig jaar 45 internetmisdaadzaken op. Daarbij gaat het om DDos-aanvallen en hacken.
,,Cybercrime vraagt echter een hele andere aanpak. Het kan zijn dat iemand op een zolderkamertje in ons gebied achter zijn computer zit, maar dat de server in Afghanistan of Pakistan staat en iemand in Zuid-Amerika wordt afgeperst. Daar moeten we grote stappen in gaan zetten om überhaupt greep op deze materie te krijgen.''

Bewijzen.
Tijd om tevreden achterover te gaan leunen is er niet, beseft de politie. ,,We zijn een organisatie die in staat is gebleken om de traditionele criminaliteit aan te pakken, maar nu zullen we ons moeten bewijzen op cybergebied'', zei hoofdcommissaris Oscar Dros van de politie Eenheid Oost eerder.

Om de bestrijding van cybercriminelen eenvoudiger te maken zijn er sinds deze maand nieuwe richtlijnen ingesteld voor officieren van justitie. Die moeten het makkelijker maken om een straf te bepalen voor vergrijpen als diefstal via internetbankieren. Ook wordt de strafmaat voor zaken als inbreken in een computeraccount met het wachtwoord van een ex-geliefde, of diefstal van gegevens van bedrijven, bijvoorbeeld door een ex-werknemer, duidelijker.

Tot nu toe keek de officier van justitie bij het opleggen van de straf naar de geleden schade, of er slachtoffers waren en naar eventuele jurisprudentie.

2,5 miljoen delicten
In 2016 vonden naar schatting 2,5 miljoen cybercrimedelicten plaats waar Nederlanders naar eigen zeggen slachtoffer van waren. Het gaat om identiteitsfraude, koop- en verkoopfraude, hacken en cyberpesten. Ruim een kwart (27 procent) van deze delicten werd gemeld bij de politie of andere instanties, zo blijkt uit de jaarlijkse Veiligheidsmonitor.

Malafide webshops
Bij de politie kwamen door aangiften honderden online webshops aan het licht. Soms worden websites van bestaande winkels tot in detail gekopieerd om consumenten op te lichten. Dat blijkt uit jaarcijfers van de politie. In 2017 werd in 438 gevallen actie ondernomen tegen malafide webwinkels, een jaar eerder gebeurde dat nog 35 keer.

Sophos bestrijdt malware met deep learning

Sophos heeft een nieuwe versie van Intercept X uitgebracht, die voor malwaredetectie gebruik maakt van deep learning. Dat moet voor veel betere detectie zorgen en zeer lage percentages false positives. Maar wat doet het voor security beter dan 'gewone' AI?

Intercept X speurt volgens Sophos nu met behulp van deep learning naar malware en ongewenste applicaties. Nu nog vertrouwen veel van dergelijke producten op handtekeningen (signatures) maar dat is bijna ondoenlijk aan het worden.
Kris Hagerman, CEO van Sophos wijst er op dat het bedrijf dagelijks 300.000 malware-samples aantreft binnen het netwerk van zijn eigen gebruikers. “Daarbij gaat het om 100 miljoen endpoints van gebruikers. Dat is wel heel veel informatie om te verwerken. Met deep learning kun je veel sneller al die data verwerken met een beter resultaat dan ‘gewone’ AI.”

Murray stelt dat het een illusie is dat cybercrime – net als ‘fysieke’ misdaad – uitgeroeid zal worden. “Wij als leveranciers van beveiligingsproducten moeten in de strijd tegen cybercrime ervoor zorgen dat onze producten minstens zo goed, creatief en effectief zijn als die van de criminelen. En een van de spannendste ontwikkelingen daarvoor is AI. Zeker als je deep learning kunt gebruiken in je cybersecurity, kun je flinke stappen maken in effectiviteit van je product.”
AI maakt het al mogelijk om zeer snel enorme hoeveelheden data te verwerken en vrijwel real time te reageren op mogelijke bedreigingen, ook als die in die vorm nog nooit zijn gedetecteerd.

Overtreffende trap
Deep learning, de overtreffende trap van machine learning, werkt ongeveer zoals het menselijk brein: vanuit een breed overzicht van veel data, zoomt het steeds preciezer in.
Hagerman: “Daarmee kun je veel sneller en met een veel beter resultaat data verwerken.Je profiteert dan van buitengewoon grote hoeveelheden data. En dat kan steeds sneller, naarmate deep learning langer wordt gebruikt.

Je kunt dreigingen herkennen die niet eerder zijn opgemerkt. Maar de grotere snelheid is ook van zeer groot belang. Zodra cybercriminelen een gat in de verdediging hebben gevonden, slaan ze razendsnel toe. Het is een race en hoe sneller jij als beveiliger op kunt treden, hoe meer schade je kunt voorkomen.
En als daar dan veel minder mensen aan te pas komen, kun je meer snelheid maken want overleg kost tijd. Het gaat dus om snelheid, accuraatheid en de mogelijkheid om te kunnen voorspellen en dus te anticiperen op aanvallen."

Sophos richt zich op het middensegment: bedrijven met maximaal 5000 werknemers, hoewel 20 procent van zijn klanten groter is.
Hoeveel indruk maakt het op hen dat Intercept X wordt uitgebreid met deep learning-technologie?
“Bij de introductie vorig jaar van de eerste versie van Intercept X twijfelden we van tevoren of klanten en partners wel zouden zien hoe innovatief en geweldig het was.
En ja, ze snappen niet hoe het werkt, maar wel dát het werkt. En dat is wat voor hen telt. Als een product werkt en doet wat het moet doen en dat het dan ook nog zo makkelijk mogelijk in gebruik en beheer is, dan is het voor hen prima. En nu krijgen ze er een turbo charge bij met deep learning.”

Zo ontmasker je nepmails

Internetcriminelen worden steeds gewiekster en de tijd dat nepmailtjes vol met taalfouten stonden ligt definitief achter ons. Maar hoe weet je dan of een bericht waarin je gevraagd wordt om bepaalde gegevens te verifiëren authentiek is? We helpen je op weg bij het herkennen van fake e-mails.

Check de aanhef
In vrijwel alle phishingmails wordt de geadresseerde aangesproken met “Beste meneer” of “Beste mevrouw” en eigenlijk nooit met uw achternaam.
De reden hiervoor is dat de internetcriminelen wel uw e-mailadres hebben maar meestal geen andere gegevens. Een onpersoonlijke aanhef van een partij die wel om allerlei persoonlijke gegevens vraagt, is bij voorbaat al verdacht.

Controleer de links
In een nepmail word je altijd om naar een bepaalde website op internet te gaan om gegevens in te vullen. Door met je muis over die link te gaan (dus niet klikken), wordt in veel gevallen het achterliggende webadres getoond.
Bij nepmails is dit vrijwel altijd een adres dat niet overeenkomst met de echte url van de website van de partij waarvoor ze zich willen uitgeven. Soms is het verschil maar een paar letters en niet zelden staan er onderaan ook juiste url’s!

Gebruik je gezonde verstand
Financiële instellingen, verzekeringen en overheidsinstellingen zullen je nooit in een e-mail vragen om je persoonsgegevens via een website te controleren of bij te werken.
Laat je ook niet bang maken door berichten met dreigende taal, bijvoorbeeld in een mail waarin gesproken wordt over in beslagname als u een bepaalde factuur niet betaald. Haal even diep adem en gebruik uw gezonde verstand.

Twijfel je? Zoek dan via internet de contactgegevens op van de partij waarvan u deze mail zogenaamd heeft gekregen, controleer eventuele rekeningnummers en neem desnoods telefonisch contact op.

Kijk naar de bijlagen
Niet zelden zijn nepmails voorzien van een bestand in de bijlage en wordt er gevraagd om deze te openen. Heeft dit bestand de extensie zip, .exe, .js, .lnk, .wsf, .scr, .jar dan weet u eigenlijk al dat het foute boel is.
En ook een .doc of .docx van een onbekende partij moet u nooit openen omdat er macro’s in kunnen zitten die malware kunnen bevatten.

Verifieer het bericht
Internetcriminelen gokken erop dat wanneer ze een grote hoeveelheid nepmails uitsturen er een klein percentage is dat erin tuint. Je bent dan ook zeker niet de eerste die zo’n bericht ontvangt.

Op Fraudehelpdesk is een lijst te vinden met actuele phishingberichten. Komt de onderwerp regel van het mailtje dat jij ontvangen hebt overeen met één van de berichten op deze site, dan weet je dat dit bericht kunt negeren.

Internet.nl controleert nu ook striktheid anti-mailspoofing-standaarden

Platform Internetstandaarden heeft recentelijk een verbeterde versie van de testtool Internet.nl gelanceerd, waarmee gebruikers in 2017 meer dan 750 duizend testen uitvoerden. Vanaf nu controleert de testtool niet alleen of standaarden tegen mailspoofing op een domeinnaam aanwezig zijn, maar ook of ze voldoende strikt zijn ingesteld zodat misbruik van een domein echt wordt tegengegaan.

Sinds het redesign van Internet.nl in de zomer van 2017, is het aantal bezoekers dat testen uitvoert enorm toegenomen. Bezoekers voerden dit jaar tot juli rond de 100.000 testen uit. In de tweede helft van het jaar, dat wil zeggen na het redesign, zijn er ongeveer 650 duizend uitgevoerde testen bijgekomen.

Gerben Klein Baltink, voorzitter van Platform Internetstandaarden:
“De groei is prachtig maar klaar is modern internet helaas nog niet. We zien gelukkig wel ook een sterk groeiend aantal domeinen met een 100%-score die in onze Hall of Fame staan. Tegelijkertijd zijn er nog teveel domeinen die niet of niet helemaal voldoen aan moderne internetstandaarden. Blijf daarom testen, leren en vragen om moderne internet!”.

Controle op policy voor DMARC en SPF
Deze nieuwe versie van Internet.nl controleert nu ook of de syntax van je DMARC- en SPF-record geldig is. Bovendien controleert de testtool of deze records een voldoende strikte policy bevatten om misbruik van je domein door phishers en spammers tegen te gaan.
Controle op geldigheidsduur voor HSTS
Daarnaast controleert de nieuwe versie van Internet.nl nu ook de geldigheidsduur van de HSTS-policy.
Een HSTS-geldigheidsduur van tenminste zes maanden achten we voldoende veilig. Een lange geldigheidsduur heeft als voordeel dat ook infrequente bezoekers beschermd zijn. Het nadeel is dat wanneer je wil stoppen met HTTPS, je langer moet wachten totdat de geldigheid van de HSTS-policy in alle browsers die je website bezochten, is verlopen.

Impact op testscore
De DMARC-/SPF-policy en de HSTS-geldigheidsduur tellen voorlopig nog niet mee in de procentuele totaalscore. Afwijkingen worden als oranje waarschuwingen weergegeven in de testresultaten. Vanaf april 2018 wegen de resultaten van deze testonderdelen wel mee in de score.

Voorbeelden 'Nigeriaanse' fraude

Al jaren circuleren ze, mailtjes die je wijsmaken dat je een loterij hebt gewonnen of die een groot geldbedrag 'zomaar' aanbieden. Deze vorm van oplichting wordt Nigeriaanse fraude genoemd, omdat het in dit Afrikaanse land is ontstaan.

Tegenwoordig worden deze oplichtingstrucs wereldwijd gebruikt en worden deze berichten niet
alleen maar via e-mail verstuurd, maar bijvoorbeeld ook via sociale media en sms. De term voorschotfraude wordtook vaak gebruikt voor deze vorm van fraude. In dit artikel vind je een aantal voorbeelden en tips.

Je hebt een prijsvraag of loterij gewonnen (waaraan je niet hebt meegedaan).
Je bent de gelukkige winnaar van een prijsvraag of loterij! Een groot geldbedrag, een auto; het is van jou, als je maar even contact opneemt.

Lijkt het te mooi om waar te zijn?
Dat is dan ook zo! Vaak staat een link in het bericht, die leidt naar een website waar je de prijs kunt claimen of een mailadres waar je jouw gegevens heen moet sturen. Daarna zal je altijd worden gevraagd om een geldbedrag te over te maken als administratiekosten'.

Dit geld ben je kwijt en de prijs zul je nooit zien, want die bestaat niet.
Als je je niet kunt herinneren ooit mee te hebben gedaan aan een loterij of prijsvraag, ga er dan niet op in en verwijder het mailtje.

Iemand heeft je hulp nodig om een geldbedrag beschikbaar te krijgen

Je krijgt een (vaak Engelstalige) mail, waarin iemand je een zakenvoorstel wil doen. Hij geeft vaak een vage uitleg over hoe hij aan je mailadres is gekomen. Deze persoon wil een groot geldbedrag (vaak enkele miljoenen) naar je overmaken. Je mag dan uiteindelijk een percentage van het geld houden. Maar eerst moet je een bedrag overmaken, zodat het geld vrijgegeven kan worden.

Reageer niet op dit soort e-mails en maak nooit geld over. Dit geld ben je kwijt en het beloofde bedrag zal nooit op je rekening verschijnen.
Je krijgt een (te) hoog bod voor een product dat je aanbiedt op een advertentiesite. Je krijgt een hoog bod voor een product dat je aanbiedt op een online advertentiesite. Je gaat enthousiast op het bod in en ontvangt binnen een paar dagen een betalingsbewijs van Paypal, van de bank, of in de vorm van een cheque. Na het product verstuurd te hebben blijken deze betaalbewijzen nep te zijn en zit u zonder product én zonder geld.

Wantrouw (te) hoge biedingen en probeer meer informatie te achterhalen over de potentiële koper. Wees op je hoede als de koper je vraagt het product naar Nigeria te verschepen of je vraagt om transactie of verzendkosten te betalen. Deel je ervaringen en twijfels met anderen als je het niet 100% vertrouwt.

Een zakenman vraagt je cheques te verzilveren
Via een datingsite kom je in contact met een Nigeriaanse zakenman, die je overstelpt met romantische correspondentie en goedkope cadeaus. Zo komt een vertrouwensband tot stand waar hij misbruik van maakt. Hij vertelt je dat zijn werkgever alleen maar uitbetaalt met Money Orders en dat hij die onmogelijk kan incasseren in Nigeria. Hij verzoekt je de cheques te verzilveren en hem het geld via Western Union te sturen. Je mag zelfs een percentage van het geld zelf houden.
Je komt bedrogen uit, want na een paar weken blijkt dat de cheques niet gedekt waren. Het slachtoffer is dan verantwoordelijk voor het terugbetalen van het geld, omdat hij degene is die de cheque heeft verzilverd.

Je kunt een dergelijke oplichter onder andere herkennen aan een professionele foto. Persoonlijke vragen worden genegeerd en hij stuurt veel liefdesgedichten die zo van internet geplukt zijn. Zijn correspondentie bevat veel spelfouten en in het weekend is hij vaak niet online. Ook draagt hij vaak een trouwring terwijl hij beweert single te zijn.

Wees alert bij ontmoetingen via datingsites en probeer zoveel mogelijk over iemand te weten te komen. Verzilver nooit buitenlandse of onbekende cheques en vergelijk de money orders met fake cheques die er in omloop zijn.

Hoe WPA3 je wifi veiliger maakt

Na dertien jaar trouwe dienst is het WPA2-protocol aan een update toe. De Wi-Fi Alliance, de organisatie die belast is met het opstellen van officiële standaarden voor wifi, kondigde begin dit jaar de komst van WPA3 aan.

Het Wi-Fi Protected Access II (WPA2)-protocol beschermt je draadloze verbinding door ieder datapakketje te versleutelen dat tussen je toestel en je router wordt uitgewisseld. Het protocol is sinds 2004 in voege en wordt tegenwoordig nagenoeg universeel gebruikt om draadloos internetverkeer af te schermen van hackpogingen.

Dat het protocol al zo lang meegaat zonder aanpassingen komt door het feit dat het tot voor kort als een solide verdedigingsmiddel werd beschouwd. Die reputatie kreeg in 2017 letterlijk en figuurlijk een barst. Een Belgische onderzoeker vond een zwakke plek in het WPA2-protocol en wist de encryptie te verschalken. De exploit kreeg de naam Krack. De kwetsbaarheid was op te lossen met een patch en is dus niet de aanleiding voor de update van het protocol, maar het nieuws van het lek signaleerde wel duidelijk dat WPA2 aan vervanging toe was. Opvolger WPA3 brengt drie grote aanpassingen met zich mee die de beveiliging van wifi optrekken.

Een belangrijke update is dat WPA3 gebruik zal maken van 192-bit encryptie in plaats van de 128-bits van WPA2. De langere encryptiesleutels tillen de beveiliging van wifi op naar de hoogste beveiligingsstandaard van het moment. Dat moet ervoor zorgen dat de verbindingsstandaard geschikt is voor overheden en bedrijven in kritieke sectoren, en gewone gebruikers profiteren mee van de geavanceerde encryptie.

De Wi-Fi Alliance pakt met WPA3 een oud veiligheidsprobleem aan en poogt de risico's van openbare wifi-netwerken te neutraliseren. Dit door de introductie van "geïndividualiseerde data-encryptie" in het protocol, specifiek gericht op publieke netwerken.

Datastromen op openbare netwerken verlopen doorgaans zonder encryptie, wat het voor hackers eenvoudig maakt om die communicatie te onderscheppen. Door elke datastroom tussen een toestel en een router af te schermen met een unieke encryptiesleutel, zal het voor hackers veel moeilijker worden om in te breken op je dataverkeer op een openbaar netwerk.

WPA3 bevat ook een standaard die gebruikers tegen zichzelf beschermt. Het Simultaneous Authentication of Equals (SAE)-protocol, ook wel het Dragonfly protocol genoemd, moet wifi-netwerken met een zwak wachtwoord toch de nodige bescherming geven. Het Dragonfly protocol voorkomt brute-kracht-aanvallen waarbij hackers eindeloos wachtwoorden uitproberen op je netwerk tot ze het juiste gevonden hebben. Dragonfly maakt dat onmogelijk via een ingebouwde blokkering die voorkomt dat iemand na verschillende foute inlogpogingen nog verder wachtwoorden kan uitproberen.

De lancering van WPA3 staat gepland voor 2018, meer details over een specifieke datum zijn niet bekend.

Bron: WiFi Alliance

Gezichtsherkenning politie identificeerde 93 verdachten in 2017

Met de gezichtsherkenning-software Catch heeft de Nederlandse politie in 2017 in 93 gevallen een verdachte weten te koppelen aan een foto in de database.

In totaal werden zo'n duizend foto's verwerkt, in ruim negenhonderd gevallen was identificatie onmogelijk – de persoon stond niet in de database (van ruim één miljoen foto's van veroordeelden en verdachten) dan wel was de kwaliteit van de foto onvoldoende.

Catch, sinds 2016 in gebruik, werkt 'niet zoals in CSI', zegt biometriespecialist John Riemen van de Nationale Politie.
Foto's worden eerst beoordeeld op kwaliteit en bij een match door twee experts, onafhankelijk van elkaar, beoordeeld. Een match is volgens Riemen hooguit een indicatie voor iemands identiteit, geen hard bewijs. 'Onze gezichtsherkennings-software laat alleen maar zien dat er veel overeenkomsten zijn'.

Het programma wordt 'breed ingezet', in diverse zaken, van winkeldiefstal tot terreur. De foto's komen van uiteenlopende bronnen als beveiligingscamera's, pinautomaten, sociale media, observatie-eenheden en – in sommige gevallen – ook de vreemdelingendatabank. In 2017 is ook een smartphone-app ontwikkeld waarmee agenten beelden rechtstreeks naar Catch kunnen sturen. Deze wordt door 'een beperkte doelgroep' getest, aldus Riemen.

Burgerrechtenorganisaties als Bits of Freedom hebben kritiek en zien 'het gevaar van het hellende vlak'.
Directeur Hans de Zwart van Bits of Freedom merkt op dat zulke technologie langzaam maar zeker breder wordt ingezet omdat het zo handig is. 'Straks gaat de politie misschien wel op allerlei locaties gezichten scannen' en worden mensen die ooit zijn gearresteerd, 'de rest van hun leven worden gecontroleerd'.

Volgens Riemen gebeurde dat in 2017 alleen met foto's van rellende Feyenoord-supporters die strafbare feiten hadden gepleegd. Onderzocht wordt of de technologie ook real-time werkt.

Bron: Nationale Politie

INDEX

Schakel Windows-herstelpunten in

Windows-herstelpunten kunnen een cruciale rol spelen bij het herstellen van bestanden nadat je computer is gecrasht. Zo'n herstelpunt geeft je immers de kans om terug te gaan naar een oudere status van je computer voordat er zich problemen voordeden. In Windows 10 zijn de herstelpunten van Windows standaard uitgeschakeld. Wie graag sleutelt aan zijn computers of nieuwe applicaties uitprobeert, schakelt de functie best in.

Inschakelen

Open het startmenu en zoek naar 'Een herstelpunt maken'. Selecteer je systeemdrive in het venster dat zich opent – doorgaans is dat schijf C – en klik vervolgens op 'Configureren'. Vink 'Systeembeveiliging inschakelen' aan en verander eventueel de hoeveelheid schijfruimte die systeembeveiliging gebruikt. Standaard staat deze instelling op 1 procent. Klik tenslotte op 'Toepassen' en op 'OK' om het instellingenmenu te verlaten. Windows maakt nu automatisch een herstelpunt aan wanneer belangrijke systeemveranderingen zich voordoen, zoals net voor de installatie van een grote Windows-update.

Manueel herstelpunt

Nu systeembeveiliging is ingeschakeld, creëert Windows een herstelpunt telkens je grote veranderingen aanbrengt aan het systeem. Je kan echter tussendoor manueel herstelpunten aanmaken, indien je dat wenst. Open hiervoor wederom het 'Een herstelpunt maken'-venster en ga naar 'Systeembeveiliging'. Selecteer de systeemdrive en klik vervolgens op 'Maken'. Alvorens je het proces kan starten, moet je een beschrijving voor het herstelpunt opgeven. Stel dat je op het punt staat om een nieuwe applicatie te installeren dat mogelijk een negatieve invloed heeft op je systeem, dan kan je hier de naam van die applicatie invullen. Op deze manier vind je eenvoudig het juiste herstelpunt terug, moest er iets misgaan. Klik tenslotte op 'Maken' om het herstelpunt te creëren.

Systeem herstellen

Als je systeembeveiliging hebt ingeschakeld en er gaat iets mis, dan kan je je systeem herstellen vanaf een herstelpunt. Open hiervoor wederom het herstelpuntvenster en klik op 'Systeemherstel'. Klik vervolgens op 'Volgende' en selecteer in de lijst die verschijnt het juiste herstelpunt. Je kan op de knop 'Zoeken naar programma's die worden beïnvloed' klikken om na te gaan welke applicaties je na het herstelpunt hebt geïnstalleerd of geüpdatet. Klik nogmaals op 'Volgende' en tenslotte op 'Voltooien' om je computer te herstellen. Je toestel zal nu terugkeren naar een vorige status.

Automatisch herstel

In sommige gevallen wil je computer simpelweg niet meer opstarten omwille van een probleem. In dat geval werkt de voorgaande stap uiteraard niet. Wanneer je je pc driemaal achter elkaar onsuccesvol hebt proberen op te starten, opent Windows 10 automatisch het herstelvenster. Klik op 'Problemen oplossen' en ga vervolgens naar 'Geavanceerde opties'. Klik op 'Systeemherstel', kies het juiste herstelpunt en klik tenslotte op 'Voltooien'. Windows zet een vroegere versie van je systeem terug. Indien deze versie wel stabiel is, kan je je computer weer zonder problemen gebruiken.

11 procent Nederlanders slachtoffer cybercrime

Elf procent van de Nederlanders is vorig jaar slachtoffer van cybercrime geweest, net zoveel als in 2016, zo staat in de Veiligheidsmonitor van het Centraal Bureau voor de Statistiek (CBS). De data die voor de Veiligheidsmonitor werd gebruikt is gebaseerd op online en papieren vragenlijsten die door bijna 150.000 mensen werden ingevuld.
Van de cybercrimedelicten kwam hacken vorig jaar het meest voor (5 procent). Dit wordt gevolgd door koop- of verkoopfraude (4 procent), pesten via het internet (3 procent) en identiteitsfraude (minder dan een half procent). Het aandeel Nederlanders dat slachtoffer van skimming werd daalde van 1,1 procent in 2012 naar 0,1 procent in 2017. Vorig jaar deed 8 procent van de slachtoffers van cybercrime aangifte bij de politie. Dit is vergelijkbaar met voorgaande jaren.

Hacken
Het CBS omschrijft hacken als het met kwade bedoelingen inbreken of inloggen op iemands computer, e-mailaccount, website of profielsite (bijvoorbeeld Facebook, Twitter). Vorig jaar werd 4,9 procent van de Nederlanders slachtoffer van deze vorm van cybercrime, waarmee het de meestvoorkomende vorm is. Dit is hetzelfde als in 2016, maar minder dan in 2012 (6 procent). Het aantal delicten bedroeg 7,5 per 100 inwoners. Ook dit komt overeen met 2016 (7,4 per 100) en is minder dan in 2012 (8,8 per 100). In de meeste gevallen heeft de hack plaatsgevonden door in te breken op een website of profielsite (2,6 delicten per 100 inwoners).

Leeftijd
Als er wordt gekeken naar de leeftijd van slachtoffers van cybercrime, dan zijn jongere leeftijdsgroepen vaker slachtoffer dan oudere. Het aandeel van slachtoffers tussen de 15 - 24 jaar is met 17 procent ruim drie keer zo groot als het aandeel 65-plussers (5 procent). Ook bij cyberpesten zijn jongere leeftijdsgroepen vaker slachtoffer dan oudere. Bij koop- en verkoopfraude en bij hacken zijn naast 15- tot 24-jarigen ook 25- tot 44-jarigen relatief vaak slachtoffer. Identiteitsfraude laat een ander beeld zien. Hier zijn jongeren minder vaak slachtoffer dan de oudere leeftijdsgroepen.

Aangifte
Dertien procent van alle gevallen van identiteitsfraude, koop- en verkoopfraude, hacken en cyberpesten samen is vorig jaar gemeld bij de politie. Dit is vergelijkbaar met de jaren daarvoor. Aangifte bij de politie werd in 2017 in ruim één op de twaalf gevallen (8 procent) gedaan. Ook dit is vergelijkbaar met voorgaande jaren. Het aandeel dat via internet werd aangegeven is in 2017 ongeveer even groot als het aandeel dat via een proces-verbaal werd aangegeven. Dit was in 2016 ook het geval. In 2012 was het aandeel aangiften van cybercrime via internet kleiner dan het aandeel aangiften via een proces-verbaal.

Malware: de symptomen

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. Tegenwoordig kan dat ook gewoon via je browser, om bijvoorbeeld cryptocoins te minen.

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.

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.

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.

“We maken het de cybercrimineel wel érg makkelijk”

Als de dood voor cybercrime maar er niks aan doen om het te voorkomen.

Nog steeds doen Nederlanders veel te weinig om zich te beschermen tegen internetcriminaliteit: vier op de tien gebruikt hetzelfde wachtwoord voor meerdere accounts, een op de zes maakt nooit een back-up en de helft wéét niet eens hoe ze zich moeten beschermen.

Het ministerie van VenJ is daarom een nieuwe publiekscampagne gestart. ‘Het is voor iedereen logisch de buitendeur op slot te draaien, maar dat geldt niet voor onze digitale deuren’, aldus minister Ferdinand Grapperhaus.

In 2017 werden 2,6 miljoen cybercrimedelicten gepleegd, in totaal 11% van de Nederlanders werd slachtoffer. Een tegengeluid komt van specialist digitale beveiliging Michel van Eeten, ook hoogleraar aan de TU Delft.

Volgens Van Eeten wordt er te veel van mensen verwacht. ‘Je hebt tegenwoordig zoveel wachtwoorden nodig, we kunnen niet verlangen dat iedereen allemaal unieke varianten gebruikt’. Bewustwording vergt volgens hem tijd. ‘Gemiddeld zijn we het echt beter gaan doen, er zijn veel minder computerbesmettingen dan tien jaar geleden’.

Cops in Cyberspace

Omdat sexting 'je levenslang kan achtervolgen' hebben wijkagenten Kelvin en Tanja uit Katwijk, in samenwerking met Halt en welzijnsorganisatie Welzijnskwartier, de game Shitzooi bedacht. De game, bedoeld voor 12-15 jarigen, bevat het verhaal van een scholiere die een pikant filmpje deelde met een vriendje. Dat lekte uit en belandde op pornosites. Het meisje doet aangifte, de scholieren moeten de zaak proberen op te lossen: om wat voor foto's gaat het, wie deelde ze, met wie, wie is er verdachte, wie moet worden verhoord. De bedoeling van de game is vooral jongeren te waarschuwen, zegt wijkagent Tanja. 'En wat sluit er nou beter aan bij de belevingswereld dan een game'. En sexting blijft een probleem: een op de vier jongeren maakt naaktselfies, een op de acht verstuurt die via sociale media, de laatste tijd vooral via Snapchat. Maar daar blijven veel beelden toch bewaard, weet iedereen. 'Sexting is onuitwisbaar'. Maar dan heb je wel kinderporno op je telefoon, wat je zelfs een strafblad kan opleveren, zegt Nadine van Welzijnskwartier. 'En stel dat je later kinderen krijgt en dat die op een dag ergens op internet blootfoto's van jou zien staan?'

———————————————

Er was nog een flinke speurtocht voor nodig maar de politie heeft eindelijk de identiteit van 'The Climbing Dutchman' weten te achterhalen. De jongen (17, uit Delft) liftte mee aan de buitenkant van treinen en zette beelden daarvan op YouTube. ProRail deed aangifte tegen de jongen, de politie heeft hem nu geïdentificeerd aan de hand van zijn YouTube-filmpjes én beelden van NS-camera's. De jongen werd uitgenodigd op het bureau maar beriep zich aldaar op zijn zwijgrecht. Het betreft bovendien een overtreding en geen misdrijf. Het OM beslist of de jongen vervolgd wordt.

———————————————

'Sorry hoor, we waren boeven vangen'. De politie Heerhugowaard heeft zich op facebook verontschuldigd voor de schoten die midden in de nacht gelost werden bij een zoektocht. En de helikopter hing ook boven de wijk … De agenten probeerden een auto te laten stoppen; toen de bestuurder vol gas wegreed, loste een agent enkele waarschuwingsschoten. Dat leidde tot verontruste berichten op facebook. De een durfde het bed niet meer uit, de ander niet naar zijn auto te lopen. Enzovoort. Waarop de politie op datzelfde facebook excuses aanbood. 'Bedenk dat als u een politieheli hoort, dat de politie dan uw directe omgeving veiliger maakt'. In de later aangehouden auto, vol met gestolen spullen, zaten drie jongens (17 tot 23). Zij zijn aangehouden.

———————————————

Nederlanders doen steeds minder aangifte via de website van de politie. Er zijn teveel problemen, onder meer bij het inloggen en het invoeren van gegevens, zegt NPB-voorzitter Jan Struijs. 'Het lukt ze niet, ze raken gefrustreerd en uiteindelijk stoppen ze ermee'. Veel problemen lijken terug te voeren op de verplichte sms-authenticatie waarmee het systeem een extra inlogcode verstuurt. Anderen haakten af omdat ze geen DigiD hadden. Struijs noemt dat ernstig 'want de politie heeft alle aangiftes nodig om goed prioriteiten te stellen'.

Rechtspraak

Internetoplichter Maikel B. (23, uit Roermond) is door de rechtbank veroordeeld tot 150 uur taakstraf en twee maanden voorwaardelijke jeugddetentie. De verdachte wist in 2011 en 2012 via Marktplaats in totaal 104 mensen op te lichten door spullen als smartphones, tablets maar ook schoenen en treinkaartjes te verkopen maar nooit te leveren. Bij het LMIO kwamen ruim vierhonderd klachten over de verdachte. Ruim honderd mensen deden uiteindelijk aangifte. De man werd al in januari 2015 opgepakt. Naar eigen zeggen besteedde de verdachte het geld aan kleding en Efteling-bezoekjes.

———————————————-

Een Belg (23, uit Jette) die in facebook-filmpjes opschepte over de snelheden waarmee hij in zijn auto reed, is vijf jaar zijn rijbewijs kwijt. In een filmpje – gemaakt met een GoPro op zijn hoofd – is te zien hoe hij met 249 km/u over de ring van Brussel scheurt. Toen dat filmpje op facebook werd opgemerkt, en er meerdere van zulke filmpjes gevonden werden, startte de politie een onderzoek. De verdachte werd aangeklaagd voor veertien strafbare feiten, waarvoor het OM aanvankelijk twee maanden ontzegging en het opnieuw afrijden eiste. De rechtbank oordeelde dat de man een hardere straf verdiende, vooral vanwege het 'wederkerend patroon met voorbedachte rade'. De verdachte moet 150 uur taakstraf doen in een revalidatiecentrum voor verkeersslachtoffers, opnieuw rij-examens afleggen, 1000 euro boete betalen; zijn auto is verbeurd verklaard.

———————————————-

Een Britse wetenschapper die mensen dwong zichzelf te filmen terwijl ze vernederende opdrachten moesten uitvoeren, is tot 32 jaar celstraf veroordeeld voor internetafpersing. De man, Matthew Falder (29) zei tegen iedereen op internet dat hij vrouw was en 'artiest' en naaktfoto's nodig had om kunstwerken te maken. Met die beelden chanteerde hij echter zijn slachtoffers. Die moesten onder meer hondenvoer eten en wc-brillen aflikken én dat filmen natuurlijk. Falder bekende maar liefst 137 zaken. De verdachte was vooral actief op het darkweb waar de beelden volop werden gedeeld. Zijn naam dook op in een internationaal onderzoek.

———————————————-

De rechtbank in Den Haag heeft een man (78, uit Voorburg) voor bezit en verspreiding van kinderporno veroordeeld tot een half jaar voorwaardelijk. De politie had het materiaal eind 2016 op een computer van de verdachte gevonden. De verdachte, die met zijn vrouw regelmatig naar Gambia reist, 'een land dat bekend staat om kindersekstoerisme', had die beelden via chatkanalen met anderen gedeeld. Hij moet de komende vijf jaar toestemming vragen als hij weer naar het buitenland wil. Tegen de man was één jaar celstraf (de helft voorwaardelijk) geëist.

———————————————-

Agenten filmen mag, maar 'grievende teksten' worden bestraft – net als 'zuigend commentaar'. De rechtbank in Rotterdam veroordeelde een man (28, uit Rotterdam) die politieagenten filmde en hen het bloed onder de nagels vandaan haalde. De verdachten filmde twee agenten die zijn broer kwamen ophalen die nog een straf had uitstaan. 'Ik mag filmen, ik mag filmen', riep de man enkele keren. Maar wat niet mocht, was om dat filmpje te voorzien van beledigende teksten. De verdachte sprak in het filmpje over 'twee sukkeltjes' en 'grafkoppen' die 'te veel gesnoven of te veel pillen' op hadden. De agenten deden aangifte toen ze de video zagen. Met succes dus. De rechtbank achtte twee van de drie aanklachten bewezen: laster en belediging wel, bedreiging niet. De verdachte kreeg twee weken voorwaardelijk met een proeftijd van twee jaar.

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 veilig heid
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
- Mousejack

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