Mei 2016

JAARGANG 5

Secure Computing

(NB: met Ctrl+ scrolwieltje kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen. Via de hyperlinks verkrijgt u nog meer info.)

W.Bosgra

Taakaccenthouder Digitale Criminaliteit Basisteam Enschede

Snel index

Klik op een link voor snelle toegang . Om terug te keren klik op index onder aan de pagina.

Secure Computing

Secure Computing Magazine Online

Vaste rubrieken

De Wbp is van toepassing op iedere verwerking van persoonsgegevens. In de Wbp staat een rechtmatige en zorgvuldige omgang met persoonsgegevens voorop. De reikwijdte van de Wbp wordt onder meer bepaald door een tweetal definities uit deze wet, persoonsgegevens' en 'verwerken'.

Bescherming van persoonsgegevens bij onderzoeken

Onder een persoonsgegeven wordt verstaan: "elk gegeven betreffende een geïdentificeerd of identificeerbare natuurlijke persoon". Dus ook bij een combinatie van gegevens die leiden tot een identificeerbaar persoon is er sprake van een persoonsgegeven. Wanneer zonder onevenredige inspanning de identiteit van de persoon kan worden vastgesteld, is er sprake van persoonsgegevens.

Onder verwerken wordt verstaan: "elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken (...) of vernietigen van persoonsgegevens".

Voor cybercrime is een IP-adres in principe een persoonsgegeven. Daarom zijn bij de verzameling, opslag en verwerking van IP-adressen de rechten en plichten volgens de Wbp van toepassing. Op Europees niveau lijkt eenzelfde lijn gevolgd te worden. Is de identiteit van een persoon herleidbaar op basis van diens IP-adres, dan zal in beginsel worden aangenomen dat het gaat om een beschermd persoonsgegeven.

Een recente uitspraak van het College Bescherming Persoonsgegevens (CBP) over de toelaatbaarheid van een zogenoemde IP-checker onderstreepte dit. Het CBP stelde in deze zaak dat het IP-adres weliswaar niet altijd door eenieder herleidbaar is tot een individueel persoon, maar dat het toch een persoonsgegeven is, omdat een derde - bijvoorbeeld de internetprovider - eenvoudig de identiteit van de gebruiker kan achterhalen. Hetzelfde geldt voor een bedrijf, dat op basis van interne gegevens makkelijk kan achterhalen welke werknemer bij het betreffende IP-adres hoort.

Een IP-adres hoeft niet altijd als een beschermd persoonsgegeven te worden aangemerkt. Zo zijn groepen van IPadressen die gekoppeld zijn aan het land van herkomst, geen persoonsgegevens. Een dergelijke koppeling geeft beheerders van webpagina's de mogelijkheid om hun websites zó in te stellen, dat de gepresenteerde informatie automatisch in de taal van de gebruiker wordt weergegeven. Aangezien deze koppeling van IP-adressen aan de voertaal van de gebruiker niet tot gevolg heeft dat de identiteit van deze persoon direct herleidbaar is, worden deze gegevens niet beschouwd als beschermde persoonsgegevens.

De verantwoordelijke voor de verwerking van de persoonsgegevens is verplicht de betrokkene te informeren over het feit dat er gegevens over hem worden vastgelegd. De betrokkene moet worden geïnformeerd over (art. 33 en 34 Wbp):

- welke persoonsgegevens over hem worden verwerkt;
- met welk doel deze gegevens worden verwerkt;
- wie de ontvangers zijn van zijn persoonsgegevens;
- welke rechten hij kan uitoefenen tegen het feit dat er persoonsgegevens van hem worden verwerkt.

De informatie van de betrokkene mag plaatsvinden (art. 34 lid 1 Wbp):

a. op het moment van vastlegging van hem betreffende gegevens, of

b. wanneer de gegevens bestemd zijn om te worden verstrekt aan een derde, uiterlijk op het moment van de eerste verstrekking.

Tijdens een rechercheonderzoek is het onwenselijk om de betrokkene in een vroegtijdig stadium te alarmeren. Onder art. 34 lid 1 sub b is het mogelijk om het informeren uit te stellen tot het onderzoeksrapport voor het eerst wordt overhandigd aan de opdrachtgever. Eventueel kan opschorting van de informatieplicht plaatsvinden op grond van de opsporing van strafrechtelijke feiten (art. 43 sub b en d Wbp). Naast het recht om geïnformeerd te worden heeft degene van wie persoonsgegevens worden verwerkt recht op inlichtingen, inzage, correctie en verzet. De informatieplicht van de verantwoordelijke voor de gegevensbescherming is dus ook een recht van de betrokkene.

Voor de verwerking van persoonsgegevens bij een recherche-onderzoek naar een cyberincident kan het beste een zo hoog mogelijke beveiliging worden nageleefd. Maatregelen moeten ten minste voldoen aan het niveau van Wbp risicoklasse II. Systemen waarop de verwerking plaatsvindt moeten zijn versleuteld (encryptie) en voorzien van sterke toegangscontrole (authenticatie met token en wachtwoord/ pincode/certificaat). Bestanden voor het onderzoek kunnen bovendien het beste ook nog eens apart worden versleuteld.

Bron: Rijksoverheid

Index

Uit onderzoek blijkt dat t RAT's in Nederland vaker worden ingezet voor een nieuwe vorm van digitale betaalfraude.

RAT: remote acces trojan

RAT's zijn relatief gemakkelijk te verkrijgen en te gebruiken. Het plegen van bijvoorbeeld digitale fraude wordt daardoor laagdrempelig en toegankelijk voor verschillende dadergroepen. De inzet van een RAT voor betalingsfraude is nieuw en lijkt zich vooralsnog op het mkb te richten. Besmetting komt door zakelijke (spear)phishing-e-mails. De criminelen gebruiken de RAT om toegang te krijgen tot verschillende betaalomgevingen van het bedrijf, bijvoorbeeld de internetbankieromgeving of de financiële administratie. Vervolgens proberen zij geld weg te sluizen naar geldezels en volgt een witwasproces. Het is op dit moment nog niet bekend hoe groot de omvang en de schade van deze nieuwe vorm van digitale fraude is. De implicaties kunnen echter aanzienlijk zijn. De impact van deze fraudevorm kan groot zijn in de zin van economische en reputatieschade. Bovendien is de integriteit van het zakelijke betalingsverkeer in het geding. Het gaat om een relatief laagdrempelige vorm van cybercrime, die door een brede groep fraudeurs gepleegd kan worden. De gebruikte malware is goedkoop, makkelijk te krijgen en met beperkte digitale kennis te gebruiken.

Wat is een RAT?

Een Remote Access Trojan (RAT) is een aggresieve vorm van spyware. Het geeft de aanvaller de mogelijkheid zijn slachtoffers te bespioneren en hun computers op afstand te bedienen, alsof hij fysiek ter plaatse is.

Een RAT wordt zonder medeweten van het slachtoffer geïnstalleerd en blijft stilletjes op de achtergrond actief. Daarnaast zorgt deze spyware ervoor dat het onzichtbaar blijft voor antivirussoftware, waardoor slachtoffers niet weten dat iemand stiekem op de computer meekijkt. Het biedt de aanvaller meer heimelijke functies, zoals:

- maken van beeldschermafdrukken
- meekijken en meeluisteren via de webcam en microfoon
- stelen van documenten en persoonlijke foto's

onderscheppen van toetsaanslagen om persoonlijke informatie te stelen, zoals inloggegevens of inhoud van belangrijke en vertrouwelijke e-mails

installeren van andere kwaadaardige software

Het gebruiken van een kwaadaardig remote access programma valt onder computervredebreuk en wordt bestraft volgens huisvredebreuk.

Hoe blijft een RAT onzichtbaar voor antivirussoftware?

Cybercriminelen, hackers en andere aanvallers maken net als hun slachtoffers ook gebruik van antivirussoftware, zodat ze zeker zijn dat hun aanval ongezien langs de verdediging komt. Door de RAT middels versleuteling of verhaspeling (obfuscatie) te camoufleren worden virushandtekeningen buiten spel gezet en zal de RAT niet door antivirussoftware worden opgemerkt.

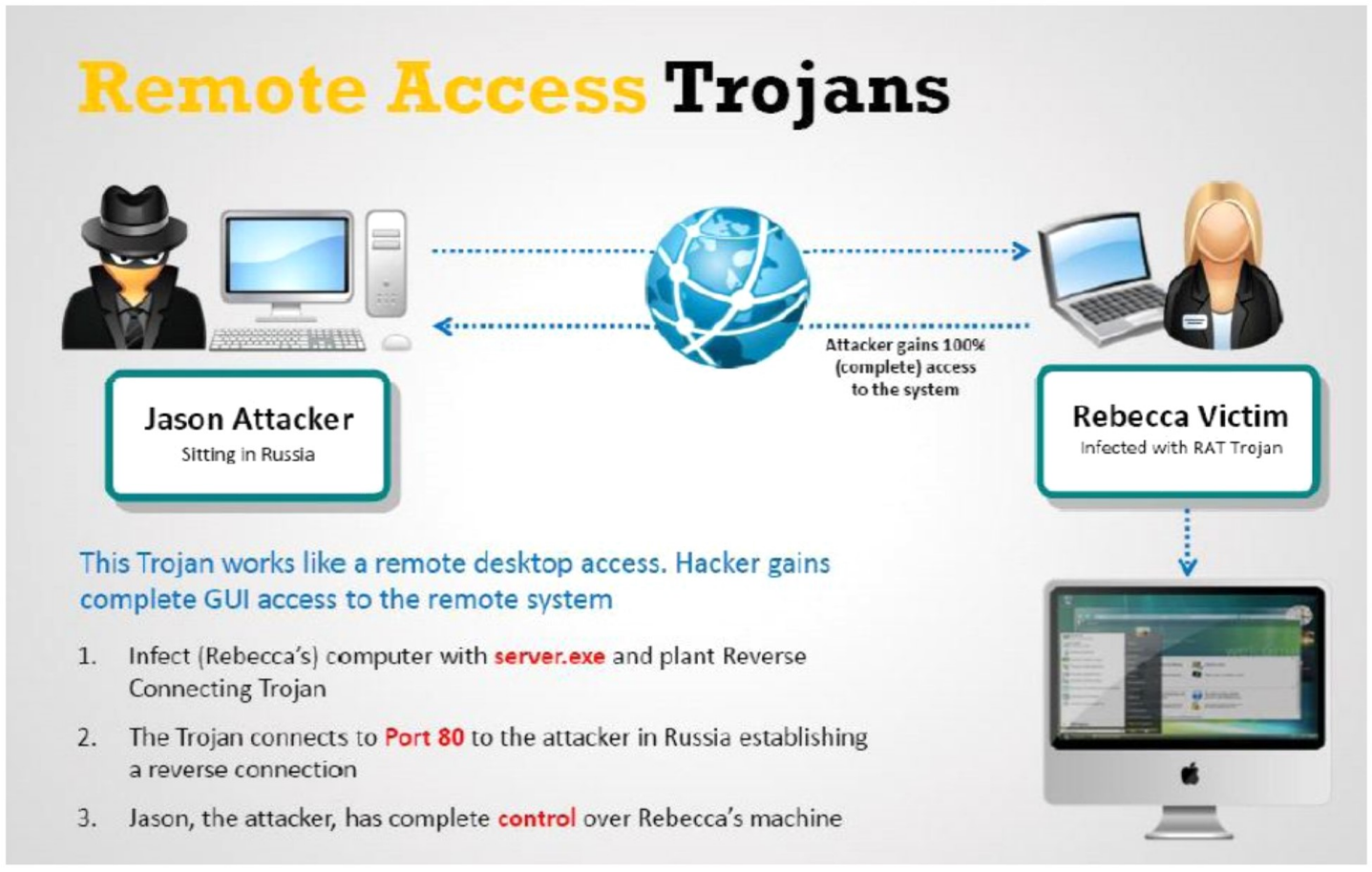
Een aanvullende techniek waarmee een actief RAT-proces onopgemerkt blijft heet hollow process. Hierbij wordt een reeds aanwezig legitiem programma misbruikt om de kwaadaardige code van de RAT uit te voeren; het legitieme geheugenproces wordt uitgehold en voorzien van de kwaadaardige code. De RAT neemt dus de identiteit van het legitieme proces over waardoor het niet opvalt in bijvoorbeeld de proceslijst van Windows Taakbeheer en het veelal vrije doorgang heeft in de Windows Firewall. Deze truc maakt het virusonderzoekers en gerenommeerde antivirussoftware nog lastiger een RAT op te merken.

Een virusbestrijder zal een exemplaar van deze specifieke RAT moeten bemachtigen om een virushandtekening te kunnen maken. Echter, omdat een RAT in de regel slechts een beperkte groep slachtoffers heeft worden deze besmettingen niet snel opgemerkt. Daarnaast is het niet zeker of de bedreiging ooit door antivirussoftware zal worden opgeruimd. Het onderzoeken van virusexemplaren en het maken van een goede virushandtekening kost tijd, waarbij virusbestrijders eerder voorrang geven aan veelvoorkomende bedreigingen dan uniek gerichte exemplaren. Slachtoffers hebben een bijzondere virusscanner nodig om een gecamoufleerde RAT op te kunnen sporen.

Bron: CSBN 2015

Index

Remote Acces Trojan



Bron: NSBN 2015

Index

Eind jaren zestig van de twintigste eeuw is bij de ontwikkeling van het internet een protocolsuite ontstaan die TCP/IP wordt genoemd. Deze protocolsuite maakte het voor het eerst mogelijk om op brede schaal verschillende systemen met elkaar te laten communiceren. Als basis voor deze communicatie dient het Internet Protocol (IP).

IPv6

Elk apparaat dat is aangesloten op het Internet of een netwerk heeft een uniek nummer om zich te identificeren (IP-adres). Er is een verschil tussen interne IP-adressen die alleen geschikt zijn om te communiceren op een intern netwerk en publieke IP-adressen die nodig zijn voor communicatie op het Internet. De Interne IP-adressen worden verstrekt door systemen op het interne netwerk. De publieke IP-adressen worden verstrekt aan bedrijven door Internet Service Providers (ISP).

IPv4 bestaat uit adressen van 32 bits waardoor theoretisch bijna 4,3 miljard adressen mogelijk zijn. In de praktijk ligt dit aantal lager omdat een aantal reeksen gereserveerd zijn voor bijvoorbeeld het gebruik in interne en private netwerken of omdat ze gereserveerd zijn voor een andere toepassing. Doordat het aantal en de dichtheid van Internetaansluitingen en dus de uitgifte van IPv4 adressen toeneemt, komt het totale aantal beschikbare adressen in het gedrang. Ook door een enorme toename van aan Internet gekoppelde consumentenelektronica, het zogenaamde ‘Internet of things3 ’, die allemaal een of soms zelfs meerdere publieke Internetadressen nodig hebben, is IPv4 uiteindelijk niet meer toereikend.

De Internet Engineering Task Force (IETF)5 , met als taak de standaardisatie van protocollen voor Internet, heeft in 1994 besloten een opvolger voor IPv4 te ontwikkelen6 . Deze werd in eerste instantie IP Next Generation (IPng) genoemd en later IP versie 6 (IPv6).

Een van de belangrijkste redenen om over te stappen op IPv6 is het geringe adressenbereik van het huidige IPv4-protocol. Nieuwe publieke IPv4-adressen worden in zeer beperkte mate uitgegeven. Zeker als de volgende “disruptive technology” zijn opwachting maakt: het “Internet of Things, anything connected”. Het koppelen van bijvoorbeeld koelkasten, auto’s, elektriciteitsmeters en dergelijke aan het internet zal een grote vlucht nemen naarmate steeds meer apparaten op afstand uitgelezen en/of bediend moeten kunnen worden. Al deze apparaten moeten kunnen communiceren met achterliggende Internetdiensten, bijvoorbeeld om informatie uit te wisselen of nieuwe firmware te laden, waardoor een unieke kans ontstaat voor vernieuwende businessmodellen.

In een groot deel van Azië en Australië zijn IPv4-adressen op en worden bijvoorbeeld nieuwe gebruikersdiensten gekoppeld via IPv6. Raadplegen van de ‘oude’ IPv4 websites en diensten is daardoor moeilijk. Als een bedrijf of organisatie zaken doet met deze regio is het zeker van belang om een migratie in gang te zetten. Business partners in deze regio’s zullen al grotendeels overgeschakeld zijn. Nieuwe technische ontwikkelingen worden waarschijnlijk primair op IPv6 gebaseerd en ondersteuning voor IPv4 zal dan worden afgebouwd. Echter zullen ook oudere applicaties of apparatuur, die niet met IPv6 overweg kunnen, voorlopig in gebruik blijven. De meeste migraties bevatten daarom het plan om een periode ‘dual stack’ te acteren waarmee bedoeld wordt dat IPv6 en IPv4 naast elkaar gebruikt worden.

Bron: NCSC

IPv6 heeft niet alleen technische consequenties voor beveiliging maar ook gevolgen voor de organisatie van beveiliging.

IPv6 en beveiliging

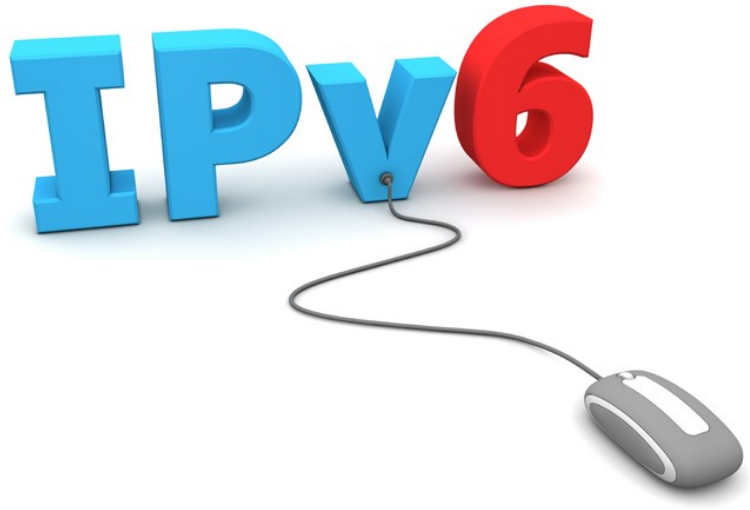
Dreigingen waaraan netwerken, internet diensten en apparatuur bloot gesteld worden veranderen niet bij het gebruik van IPv4 of IPv6 en dat geldt ook voor de beveiliging. Aanvallen zoals sniffing, flooding en man-in-the-middle-aanvallen, zijn voor beide versies relevant. Ook aanvallen op de applicatielaag en het gebruik van illegale apparatuur op het netwerk (rogue devices) zijn in IPv6 net zo goed mogelijk als in IPv4. In het gebruik van IPv6 schuilen echter een aantal gevaren die niet spelen bij IPv4. Niet alle in gebruik zijnde firewalls ondersteunen op dit moment volledig IPv6 of zelfs helemaal niet. De vraag is dan wat er met IPv6-verkeer gebeurt, met andere woorden wat is de standaard instelling van de firewall voor IPv6?

Er bestaan voorbeelden van firewalls die IPv6 niet ondersteunen maar het IPv6-verkeer wel doorlaten. Daarnaast bestaan er beveiligingssystemen die IPv6 wel ondersteunen en ook standaard aan hebben staan. In dat geval is het van belang te weten wat de standaard instellingen zijn en op welke wijze dit verkeer wordt bewaakt en gefilterd. Een gerelateerd probleem is dat veel systemen, waaronder werkstations, al IPv6 ondersteunen. Het is in dit geval wellicht mogelijk om IPv6-verkeer te ‘verpakken in een versleutelde tunnel die op het IPv4 netwerk door de beveiligingssystemen naar buiten en naar binnen communiceert.

De firewall en andere beveiligingssystemen kunnen dan de inhoud van het verkeer niet beoordelen waardoor een open verbinding naar het internet gerealiseerd wordt. Beveiligingsvoordelen Een van de voordelen van IPv6 is dat geëist wordt dat IPv6-systemen met IPsec-encryptie en tunneling kunnen omgaan. Dit leidt tot een bredere toepassing van IPsec. Dit IPsec-protocol zorgt voor betere beveiliging tegen aanvallen als ‘IP-spoofing’ en ‘TCP sequence number prediction’. Echter, het is niet zo dat IPsec een algemene oplossing is voor alle beveiligingsproblemen, hoewel het wel vaak gezien wordt als zodanig.

Een van de belangrijkste factoren die de sterkte van een op vercijfering gebaseerde oplossing bepalen is het sleutelbeheer. Voor IPsec in IPv6 zijn geen eisen vastgelegd. IPsec zelf beschrijft wel een aantal methoden voor sleutelbeheer die gebruikt kunnen worden. Bij het implementeren van IPsec op basis van IPv6 moet het sleutelbeheer dus op een goede manier geïmplementeerd worden10. Daarnaast bestaan talloze andere beveiligingsprotocollen die veel gebruikt worden zoals SSL/TLS en Kerberos. Deze zijn hetzelfde gebleven aangezien ze geïmplementeerd worden bovenop het Internet Protocol.

Het belangrijkste aandachtspunt ten aanzien van de veiligheid van IPv6 is dat het nog relatief nieuw is. Hoewel veel onderzoeken naar kwetsbaarheden in IPv6-implementaties hebben plaatsgevonden, waarbij ook kwetsbaarheden zijn gevonden, is de kans groot dat in de nabije toekomst nog nieuwe fouten worden ontdekt zoals dat bij iedere nieuwe technologie gebeurt.



Bron: NCSC

Index

Er is een groep cyberspionnen die al enkele jaren zeer actief is en allerlei technieken inzet om toegang tot organisaties en vertrouwelijke gegevens te krijgen. Toch zijn er maatregelen die organisaties kunnen nemen om de kans op een succesvolle aanval door deze spionagegroep te verkleinen, aldus Microsoft.

Microsoft geeft advies tegen cyberspionage

Secure Computing

De groep wordt onder andere 'Sofacy', 'Sednit', 'Pawn Storm', 'APT28' en 'Strontium' genoemd. Vorig jaar gebruikte de groep vijf zero day-exploits in Microsoft Office, Oracle Sun Java, Adobe Flash Player en Windows. Op het moment van de aanvallen waren er nog geen beveiligingsupdates beschikbaar. De groep heeft het vooral voorzien op defensiebedrijven die aan NAVO-landen leveren, journalisten, politieke adviseurs en politieke organisaties, maar ook overheidsinstellingen zijn regelmatig het doelwit geweest.

Om doelen aan te vallen wordt er een combinatie van phishingaanvallen en malware gebruikt. Zo wordt er eerst een verkenningsfase uitgevoerd, om potentieel interessante doelen in kaart te brengen. De volgende stap is het infecteren van deze doelwitten via malware. Hiervoor worden drive-by downloads of besmette documenten met een exploit gebruikt.

"Gezien de technische mogelijkheden en vastberadenheid om aanvallen maanden of jaren uit te voeren totdat het lukt, vormt deze groep een grote dreiging die lastig is om tegen te verdedigen", stelt Microsoft.

Advies

Er zijn echter maatregelen die organisaties volgens de softwaregigant kunnen nemen. Het gaat dan om het snel uitrollen van beschikbare beveiligingsupdates. Ervoor zorgen dat rechten van gebruikers en beheerders zijn gescheiden. Het trainen van personeel, aangezien de cyberspionnen social engineering gebruiken om werknemers bestanden of links te laten openen. Ook wordt het gebruik van multi-factor authenticatie aangeraden, alsmede het loggen van wachtwoordaanpassingen en andere belangrijke gebeurtenissen op het netwerk. Als laatste adviseert Microsoft om voorzichtig te zijn met informatie op social media, zoals e-mailadressen. De spionagegroep gebruikt informatie van dit soort bronnen voor het uitvoeren van aanvallen.

Bron: Microsoft

Index

De afgelopen dagen is er een sterke stijging geweest van het e-mails die via besmette zip-bijlagen de Locky-ransomware proberen te verspreiden.

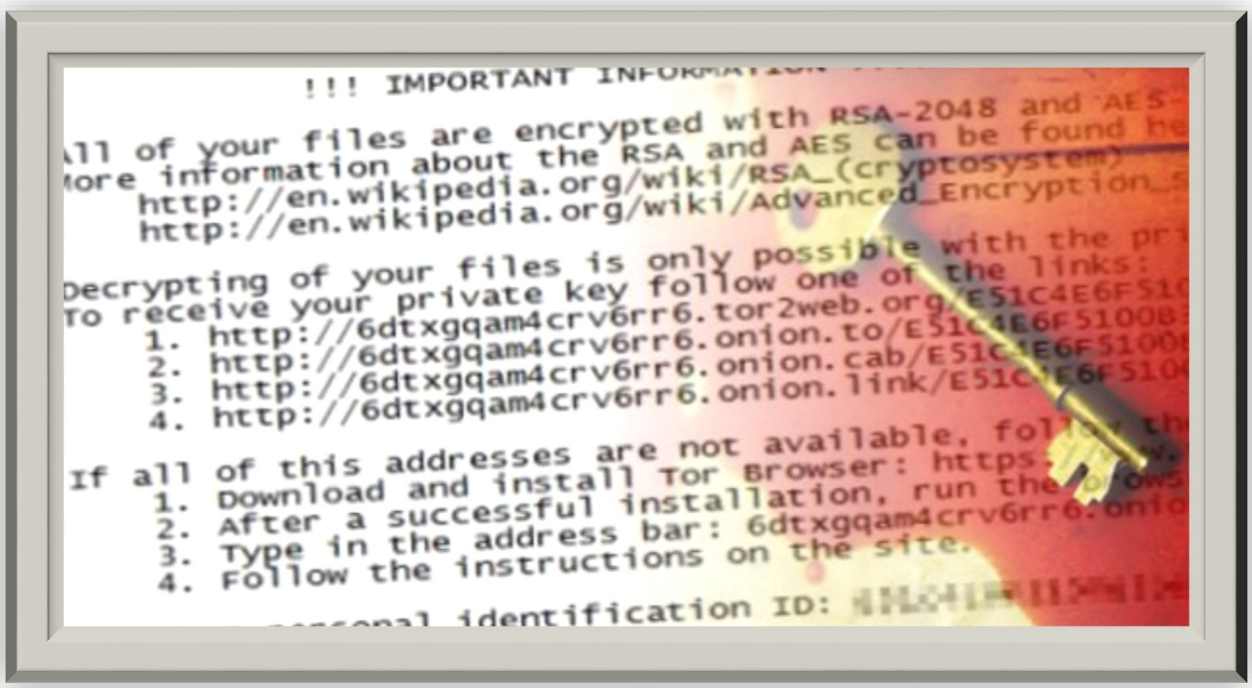
Sterke stijging van zip-bijlagen met ransomware

Secure Computing

De e-mails hebben onder andere als onderwerp "invoice notice", "attached image" en "attached document themes".

Volgens het bericht heeft de ontvanger bijvoorbeeld een bestelling geplaatst of een rekening niet betaald. Meer informatie zou in het meegestuurde zip-bestand zijn te vinden. Dit zip-bestand bevat weer een JavaScript-bestand dat de Locky-ransomware op de computer downloadt. De e-mails worden wereldwijd verspreid, waaronder ook in Nederland. Locky is een vrij nieuwe ransomware-variant, die net als andere ransomware bestanden voor losgeld versleutelt.

In het begin gebruikte de Locky-ransomware nog kwaadaardige macro's in Excel- en Word-bestanden om systemen te infecteren, maar is nu op JavaScript-bestanden overgestapt. Een mogelijke reden hiervoor is dat het eenvoudig is om het script te obfusceren en nieuwe varianten uit te rollen, en zo traditionele op signatures-gebaseerde virusscanners te omzeilen, aldus beveiligingsbedrijf FireEye. Uit cijfers van VirusTotal blijkt dat de ransomware slecht door anti-virussoftware wordt herkend. Recentelijk werd een Amerikaans ziekenhuis nog door de Locky-ransomware getroffen, waarop het ziekenhuisbestuur intern de noodtoestand afkondigde.



Bron: Security.nl

Index

Het Centre for International Governance Innovation heeft eind vorig jaar een internationaal onderzoek gedaan onder 24.000 personen om te kijken hoe men denkt over privacy en encryptie.

Meerderheid wil geen onkraakbare encryptie

Daaruit komt naar voren dat 60 procent van de respondenten tegen de ontwikkeling van encryptie is die ervoor zorgt dat de overheid geen toegang meer kan verkrijgen tot privédata.

De deelnemers uit het onderzoek kregen verschillende stellingen voorgelegd waarbij ze moesten aangeven hoe eens of oneens ze het waren met de stelling. Daarbij werd ook de volgende stelling gebruikt: "Bedrijven moeten geen technologie ontwikkelen die voorkomt dat opsporingsdiensten toegang kunnen krijgen tot online gesprekken", de meerderheid was het met deze stelling eens. Van de 24 landen waar de respondenten vandaan komen waren alleen ondervraagden uit Zuid-Korea het niet eens met de stelling.

De ondervraagden komen vanuit de hele wereld, waaronder uit Duitsland, Frankrijk en het Verenigd Koninkrijk, maar helaas niet uit Nederland of België. Nu staat Duitsland bekend als een land dat extreem voor privacy is, maar ook hier zijn ze dus geen voorstander van onkraakbare encryptie. De uitslag zal in Nederland en België waarschijnlijk ook niet anders zijn.

Verder werd er een stelling voorgelegd dat de politie recht moet hebben om toegang te krijgen tot de inhoud van online gesprekken, als dat nodig is voor de nationale veiligheid. Een grote meerderheid van 70 procent is het hier mee eens, behalve in Duitsland daar is slechts 55 procent voorstander van deze stelling.

Ook uit andere soortgelijke stellingen kwam eenzelfde antwoord. Wat we hieruit kunnen concluderen is dat mensen wel bezwaar hebben tegen massasurveillance, maar dat als het echt nodig is er geen bezwaren zijn dat de politie toegang krijgt tot persoonlijke gegevens en correspondentie. Mensen lijken te snappen dat dit nodig is om de opsporingsinstanties goed te laten werken.

Het onderzoek werd eind vorig jaar gehouden en vond dus plaats voor de hele discussie tussen de FBI en Apple over het hacken van een iPhone. Aan de andere kant vond het ook plaats voor de aanslagen in Brussel. Het is moeilijk te zeggen wat voor effect deze gebeurtenissen hebben gehad op de mening van mensen. Wel laten steeds meer opsporingsinstanties weten moeite te hebben met het achterhalen van data door alle beveiligingen.

Bron: Techzine

Index

Een e-mailbericht bevat naast de standaardinformatie die je boven je e-mail ziet nog meer informatie die niet direct zichtbaar is. Dit zijn de e-mailheaders.

Volledige e-mailheaders weergeven

Secure Computing

In de headers van een e-mailbericht staat vanaf welke server het bericht wordt verzonden en via welke servers het bericht uiteindelijk bij de ontvanger uitkomt. Deze informatie is nuttig bij het analyseren van eventuele problemen en wordt ook gebruikt bij spambestrijding.

Microsoft Outlook 2010 & 2013 (voor Windows)

1. Open de e-mail in een nieuw venster door erop te dub-belklikken.
2. Klik linksboven op de oranje ‘File’-knop.
3. Klik op ‘Info’.
4. Klik op ‘Properties’.
5. Hier ziet u de headers in het veld ‘Internet headers’.

Apple Mail

1. Selecteer de e-mail waarvan u de headers wilt opvragen.
2. Klik vervolgens in het menu op ‘View’.
3. Klik op ‘Message’.
4. Kies voor ‘Long Headers’.

Windows Live Mail

1. Klik met de rechtermuisknop op de e-mail waarvan u de headers wilt opvragen.
2. Kies ‘Properties’.
3. Klik op het tabblad ‘Details’.

Mozilla Thunderbird

1. Open de e-mail waarvan u de headers wilt opvragen.
2. Klik op ‘View’.
3. Klik op ‘Message Source’.

Gmail

1. Open de e-mail waarvan u de headers wilt opvragen.
2. Klik op het pijltje rechts van de ‘reply’-knop.
3. Klik op ‘Origineel weergeven’.

Hotmail

1. Klik met de rechtermuisknop op het bericht waarvan u de headers wilt opvragen.
2. Kies ‘Berichtbron weergeven’.

Bron: is.nl

Index

Door de technologische ontwikkelingen zijn we van de Koude Oorlog vrijwel ongemerkt in een andere manier van oorlogvoering beland die het best valt te omschrijven als de Cool War.

Cool war

Geen ouderwets geopolitiek ellebogenwerk, maar dwarsbomen met elektronen in plaats van met bommenwerpers. Het nieuwe front is online.

We bevinden ons in een situatie die je de Cool War zou kunnen noemen, de opvolger van de Cold War. Hij lijkt op zijn voorganger doordat zich geen conflicten op het slagveld voordoen, maar verschilt ervan in het soort heimelijke manoeuvres waarmee deze oorlog wordt gevoerd.

Deze oorlog is om twee redenen eerder ‘cool’ dan ‘cold’. Ten eerste is hij iets warmer dan koud, omdat het waarschijnlijk lijkt dat hij vrijwel voortdurend uit offensieve maatregelen zal bestaan die, zonder dat ze tot echte veldslagen leiden, tot doel hebben de tegenstander schade toe te brengen of te verzwakken, of voordeel te behalen door schendingen van de soevereiniteit en het binnendringen van defensiesystemen. Daarbij is deze oorlog ook ‘cool’ in de zin dat hij gebruik maakt van de modernste technologieën.

Dat gebeurt op manieren die het concept van wat een conflict precies is veel ingrijpender veranderen dan de Koude Oorlog. Die ging immers veel meer over ouderwets geopolitiek ellebogenwerk, in afwachting van een mogelijke totale oorlog van het oude stempel.

De Cool War is bovendien ook anders dan de Cold War omdat hij voor onbepaalde tijd kan worden gevoerd – permanent zelfs – zonder tot een regelrechte oorlog te leiden. Zo luidt althans de theorie.

Het jongste signaal dat erop wijst dat deze oorlog gaande is, is het artikel uit The New York Times van 19 februari, dat gaat over de onthullingen van de Amerikaanse beveiligingsfirma Mandiant over Eenheid 61398 van het Chinese Volksbevrijdingsleger, een in Shanghai gevestigde operationele eenheid die naar verluidt betrokken zou zijn geweest bij veel van de recente aanvallen op de computersystemen van Amerikaanse bedrijven en overheidsinstellingen.

Opvallend aan het artikel is het hoge man-bijt-hond-gehalte. Iedereen die een beetje oplet, weet dat de Chinezen ermee bezig zijn, net als andere landen, van Rusland tot Iran, terwijl niemand gelooft dat dergelijke aanvallen een breuk in de Amerikaanse-Chinese betrekkingen zullen veroorzaken van de aard die men in een vorig tijdperk van spionageschandalen had mogen verwachten.

Via deze aanvallen willen de Chinezen toegang verkrijgen tot waardevol Amerikaans intellectueel eigendom, inzicht in hoe de Amerikaanse economie werkt en een steeds verder groeiend vermogen om het functioneren te belemmeren van individuele bedrijven, belangrijke delen van onze cruciale infrastructuur en voorname bronnen van de Amerikaanse macht en veiligheid. En hoewel we de aanvallen in het openbaar veroordelen, matigen we onze kritiek omdat wijzelf in de hele wereld hetzelfde doen.

Het beroemdste voorbeeld hiervan is het computervirus dat is ingezet tegen het Iraanse nucleaire programma – bekend als Stuxnet – dat werd ontworpen door de VS en bondgenoten om met behulp van elektronen te doen wat we niet met commandotroepen of bommenwerpers wilden doen: het dwarsbomen van de Iraanse voortgang op de weg naar het maken van een kernbom. De opvolger van Stuxnet is nu vrijwel zeker onderweg, terwijl we de Iraniërs tegelijkertijd onder druk zetten en proberen te ‘verleiden’ tot gesprekken.

Computerworm

En omdat wij hun dat aandoen, zullen zij ook proberen ons dat aan te doen. Als men een bom op een doel werpt, verwoest die bom niet alleen het doel, hij ontploft, en vernietigt dus ook zichzelf. Maar als men een computerworm op een doel loslaat, blijft die worm – of de elementen waaruit hij is opgebouwd – intact en dus bruikbaar voor het slachtoffer van de aanval. Met andere woorden: hoewel cyberconflicten wellicht ‘hetere’ gevechten voorkomen, zorgen ze tot nu toe ook voor een vrijwel onophoudelijke escalatie.

Daarnaast zullen cyberaanvallen steeds effectiever worden en we zullen ons er steeds minder goed tegen kunnen beschermen in de wereld van ‘big data’ en ‘het internet der dingen’ die we nu betreden. Door de combinatie van alomtegenwoordige sensoren en gegevens verzamelende mechanismen, onbeperkte geheugens en enorme verwerkingscapaciteiten, wordt de oceaan van bits en bytes steeds groter en wordt vrijwel elk bedrijf een databedrijf. Elk bedrijf zal steeds meer gegevens willen beschermen, en elk bedrijf zal steeds grotere risico’s lopen wanneer het daar niet in slaagt. Dat is de reden dat zo veel bedrijven die nooit iets met deze zaken te maken hebben gehad, er nu niet alleen op uit zijn om firma’s als Mandiant in te schakelen, maar ook steeds meer belangstelling aan de dag leggen voor de toekomst van de cyberpolitiek.

De Cool War is uiteraard niet louter beperkt tot de mogelijkheid van het voeren van permanente ‘spookoorlogen’ via cyberaanvallen. Hij gaat verder dan dat, tot en met de aanhoudende discussie over het gebruik van onbemande toestellen voor observatie en vernietiging zoals drones. Al deze nieuwe technologieën maken het voor technologisch machtige landen makkelijker om tegenstanders aan te vallen en te overheersen zonder mensen-levens of militair materiaal op het spel te zetten, of om hun traditionele strijdkrachten speciale voordelen te geven als ze een conflict aangaan, zodat de risico’s worden verkleind. Het doel van de Koude Oorlog was het verkrijgen van een voordeel voordat de volgende ‘hete oorlog’ zou uitbreken, of zo mogelijk het uitstellen van dat moment. Het doel van de Cool War is om in staat te zijn voortdurend toe te slaan zonder een ‘hete oorlog’ te veroorzaken en tegelijkertijd dat soort oorlogen minder wenselijk te maken (zoals de nucleaire technologie dat deed in de tijd van de Koude Oorlog).

Bron: David Rothkopf / 360 Magazine

Index

De Amerikaanse toezichthouder FTC waarschuwt voor een nieuwe tactiek die telefoonoplichters toepassen bij het oplichten van internetgebruikers.

FTC waarschuwt voor nieuwe tactiek telefoonoplichters

De oplichters zijn al jaren actief en doen zich vaak voor als personeel van Microsoft en bellen mensen thuis vanwege "computerproblemen" of "malware".

Vervolgens moeten gebruikers een programma downloaden waarmee de oplichters toegang tot de computer krijgen. De oplichters gebruiken nu een nieuwe tactiek, aldus de FTC. Ze bellen mensen nog steeds op, maar doen zich nu voor als medewerker van het Global Privacy Enforcement Network en claimen dat het e-mailaccount van de gebruiker is gehackt en voor het versturen van frauduleuze berichten wordt gebruikt.

Vervolgens stelt de oplichter dat er juridische stappen tegen de gebruiker zullen worden genomen, tenzij de gebruiker hem het probleem laat oplossen. Als gebruikers vragen stellen voeren de oplichters de druk op. Zo geven ze echte telefoonnummers van de FTC en wijzen mensen naar de website van het Global Privacy Enforcement Network, een echt bestaande organisatie die overheden met privacyzaken helpt.

De FTC waarschuwt om mensen die bellen om de computer te "repareren" nooit toegang tot de computer te geven. Ook wordt afgeraden om financiële en gevoelige informatie te verstrekken aan mensen die contact opnemen. In het geval de beller druk uitoefent om meteen actie te ondernemen is het volgens de FTC zo goed als zeker een scam en moet er worden opgehangen. Gebruikers die zich toch zorgen maken moeten via bekende contactgegevens zelf contact met hun beveiligingsleverancier opnemen en geen informatie gebruiken die de beller geeft.

Bron: Security.nl

Index

WhatsApp voegt volledige versleuteling toe in alle chats. Daarmee zijn gesprekken tussen iOS- en Android-gebruikers en groepsgesprekken volledig beveiligd. WhatsApp gebruikt daarvoor de versleuteling van Open Whisper Systems, die ook wordt gebruikt voor de chat-app Signal.

Eind-tot-eind encryptie voor Whats App

De nieuwe encryptie werd 5 april jl doorgevoerd. WhatsApp werkt al een tijdje aan volledige versleuteling van alle berichten, maar had dat tot nu toe nog niet overal ingesteld.

Overal

Voorheen werkte WhatsApps beveiliging alleen op iOS, maar dat was niet compatibel met Android-apparaten. Nu zijn ook daar de chats beveiligd, net als op kleinere platformen als Windows Phone en Blackberry. Niet alleen chats zijn versleuteld, maar ook foto's, video's en documenten.

De encryptie is gebouwd door Open Whisper Systems, dat ook de encryptie maakt voor de beveiligde chat-app Signal. WhatsApp werkt al langer met dat bedrijf samen voor versleuteling.

Extra veilig

Met de eind-tot-eind-encryptie is WhatsApp in één klap één van de veiligste chat-apps die er zijn. Een gesprek is namelijk alleen te lezen door de verzender en de ontvanger die de sleutel hebben. Berichten die worden onderschept of opgeslagen kunnen zelfs door WhatsApp niet worden gelezen. Toch zijn critici ook skeptisch over de beveiliging. Die is namelijk niet volledig open source en dus niet te controleren. Bovendien wordt nog steeds je adresboek naar WhatsApp gestuurd - dat bovendien inmiddels eigendom is van Facebook.

Bron: PCM web

Index

Nederland is wekelijks het doelwit van cyberspionage, zo stelt de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) in het jaarverslag van 2015 dat onlangs werd gepresenteerd. Volgens de MIVD zijn vooral de ministeries van Buitenlandse Zaken en Defensie het doelwit, maar ook het internationale bedrijfsleven en toeleveranciers van Defensie.

Nederland wekelijks doelwit cyberspionage

"Met name enkele niet-westerse landen met grote militaire ambities maken zich hier schuldig aan", zo laat het rapport weten, maar landen worden niet genoemd. Naast het verzamelen van informatie biedt de toegang tot netwerken en systemen ook de mogelijkheid de functionaliteit ervan te beïnvloeden. De MIVD stelt dat er binnen militaire inlichtingendiensten een trend zichtbaar is om zich in toenemende mate te specialiseren in het binnendringen van Industriële Controle Systemen of SCADA-systemen. Deze systemen worden onder andere voor de vitale infrastructuur gebruikt.

Aanvalsmiddelen

De meest gebruikte aanvalsmiddelen zijn volgens de MIVD spear phishing en 'watering holes', waarbij websites die potentiële slachtoffers uit zichzelf bezoeken worden gehackt, om zo vervolgens bezoekers met malware te infecteren. De MIVD heeft echter ook infecties via usb-sticks en wifi waargenomen. Bij een geslaagde hack gaan daders van cyberspionage vooral op zoek naar intellectueel eigendom, politieke inlichtingen en informatie om hun eigen krijgsmachten of nucleaire capaciteiten sneller te kunnen ontwikkelen of technologische kennis om het nationale bedrijfsleven te bevorderen.

Uit onderzoeken van de MIVD naar cyberspionage rijst een beeld van enkele staten die met zeer aanzienlijke middelen trachten "ongeëvenaarde grote hoeveelheden" data te stelen om daarmee hun belangen te dienen, zo laat de inlichtingendienst weten. "Sommige staten zetten op dagelijkse basis naar schatting meer dan honderdduizend personen in ten behoeve van digitale spionage."

Opmerkelijk is volgens de MIVD dat de scheiding militair-civiel in het digitale domein vervaagt. Een militaire inlichtingendienst van een vreemde mogendheid beperkt zich niet per definitie tot militaire doelen. Militair relevante doelwitten worden ook aangevallen door civiele statelijke actoren. Ook maken civiele inlichtingendiensten in militaire zin gebruik van het digitale domein.

Toekomst

De MIVD concludeert dat digitale aanvallen in het informatietijdperk helaas een gegeven zijn. "Digitale landsverdediging in combinatie met Forward Defence capaciteiten, waarbij de inlichtingendiensten actief op zoek gaan naar bedreigingen voor dat deze zich daadwerkelijk manifesteren, kunnen effectief tegenwicht bieden aan een van de meest agressieve en succesvolle vormen van spionage, sabotage en oorlogsvoering die de wereld ooit gekend heeft."

De inlichtingendienst pleit dan ook voor verdere ontwikkeling van de capaciteiten en mogelijkheden om Nederland beter tegen dit soort activiteiten te wapenen. Daarbij wil het ook ongericht internetverkeer via de kabel kunnen aftappen, iets dat nu nog niet is toegestaan. "De MIVD wil zijn taken voor de bescherming van de krijgsmacht goed kunnen blijven uitvoeren en haar verantwoordelijkheden voor een veiliger Nederland in het samenspel met haar nationale veiligheidspartners naar behoren kunnen invullen. Daarvoor is toegang tot de kabel essentieel."

Bron: MIVD

Index

Nieuwe ransomware saboteert ook werking computer

Nieuwe ransomware: Manamecrypt

De meest ransomware versleutelt alleen bestanden en laat de werking van de computer ongemoeid, maar onderzoekers waarschuwen nu voor een nieuw exemplaar dat naast het versleutelen van bestanden ook verschillende programma's saboteert, waaronder browsers, virusscanners en Windowstools.

De ransomware wordt Manamecrypt genoemd en valt ook op vanwege de manier waarop de ransomware zich verspreidt. De meeste ransomware gebruikt e-mailbijlagen of exploits om zich te verspreiden, maar Manamecrypt is gebundeld met legitieme software, zo meldt het Duitse anti-virusbedrijf G Data. Het gaat in dit geval om een softwarebundel die uit het torrentprogramma uTorrent bestaat, aangevuld met de ransomware.

Eenmaal actief kopieert de ransomware allerlei bestanden naar een rar-bestand en voorziet die van een wachtwoord. De originele bestanden worden daarna verwijderd. Vervolgens blokkeert de ransomware allerlei programma's op de computer. Het gaat dan om anti-virusprogramma's, Windowstools zoals Systeemherstel, Taakbeheer en de Register-editor en monitoringsprogramma's, maar ook software zoals Steam en browservensters met daarin woorden als Amazon, YouTube, Facebook, Twitter en Vimeo.

Bron: G-Data

Index

Na jaren van afwezigheid krijgt Firefox eindelijk een sandbox wat de veiligheid, stabiliteit en de prestaties van de browser moet verbeteren, zo heeft Mozilla laten weten. Firefox is nog de enige van de grote browsers die niet over een sandbox beschikt.

Firefox krijgt sandbox voor veiligheid en stabiliteit

Microsoft kwam begin 2008 met meerdere processen voor IE, gevolgd door Chrome zes maanden later. Safari volgde in de zomer van 2011, maar Firefox moest het zonder doen.

Een sandbox wordt als een zeer belangrijke beveiligingsmaatregel gezien, omdat het kan voorkomen dat via een kwetsbaarheid er meteen toegang tot het systeem kan worden verkregen. Vorig jaar blies Mozilla het "Electrolysis" of "e10s" project nieuw leven in. Hierbij gebruikt Firefox geen enkel proces meer voor de browser, maar meerdere. Dit heeft verschillende voordelen voor gebruikers, aldus Mozilla's Dan Callahan. In het geval een geopende browsertab bijvoorbeeld crasht zal dit niet meer betekenen dat heel Firefox crasht, zoals nu het geval is. Ook zorgt het scheiden van processen ervoor dat straks sandboxes voor webcontent kunnen worden gemaakt. Verder zou het ook de prestaties verbeteren, omdat de nieuwe architectuur van meerdere processen het mogelijk maakt om het werk over meerdere cpu-cores te verdelen.

Callahan merkt op dat sommige mensen zich zorgen maken dat het implementeren van een dergelijke architectuur het geheugenverbruik van Firefox drastisch zal vergroten. Dit is niet het geval, aldus de Mozilla-engineer. Hoewel meerdere processen een grotere geheugenafdruk hebben dan een enkel proces zou de impact beperkt moeten zijn. Zo blijkt een voorlopige testversie van Firefox 10% tot 20% meer geheugen te verbruiken. Dit zou echter de helft minder zijn dan wat Google Chrome op dezelfde website gebruikt. "Om ervoor te zorgen dat we niet teveel werkgeheugen verbruiken, zal de eerste versie van e10s alleen een enkel extra proces voor webcontent gebruiken", merkt Callahan op. Naarmate de architectuur efficiënter met het werkgeheugen omgaat zullen er meerdere processen worden toegevoegd.

Wanneer de sandbox in de uiteindelijke versie van Firefox zal verschijnen is onbekend. "De overstap op meerdere processen is een investering in de toekomst. We lossen een technische schuld af en herontwerpen de architectuur van Firefox op een fundamenteel niveau. Net zoals elke verandering van deze omvang brengt dit allerlei uitdagingen met zich mee", aldus Callahan. Zo zullen veel add-ons moeten worden aangepast.

Bron: Mozilla

Index

Er wordt recent heel wat aandacht besteed aan ransomware, terwijl we over andere malware nauwelijks iets horen. Wat maakt ransomware zo bijzonder?

Wat maakt ransomware zo bijzonder?

Als vaste lezer van dit magazine kan het geen nieuws zijn voor u: het internet en alle bedrijven en personen die eraan gekoppeld zijn met een pc of een smartphone zitten diep in de problemen door de monsterlijke opkomst van ransomware. Helemaal sinds cryptoware een stevig percentage van ransomware uitmaakt, is de beer los. Iedereen zal vroeg of laat slachtoffer worden van een stuk malware dat de pc en alle bestanden daarop gijzelt tegen betaling van losgeld. Althans: zo lijkt het. Sinds het I Love You-virus is er in de media niet meer zoveel aandacht geweest voor één bepaald soort malware. Als je niet over verregaande inzichten in de malware-industrie beschikt, zou je geloven dat er vandaag de dag alleen nog maar ransomware is. Malware die iets anders doet, daar hoor of lees je nooit meer iets over.

Als je naar wat statistieken hierover kijkt, kom je al snel tot de conclusie dat ransomware slechts een klein percentage van alle malware in de wereld uitmaakt. In 2015 minder dan 1%. Het lijkt erop dat dat aandeel groeiende is, maar het is zeker dat 'gewone' malware nog altijd ruimschoots in de meerderheid is. Toch hebben IT-beheerders bij bedrijven en bij automatiseerders schijnbaar alleen nog maar oog voor ransomware en zijn er veel klachten over het feit dat niet alle ransomware door alle beveiligingsproducten goed wordt tegengehouden.

Verklaring?

Een verklaring voor dit verschijnsel zou kunnen worden gevonden in een hoger besmettingspercentage van ransomware. Maar is dat wel zo? Nee, zeggen de malware-experts. Ransomware maakt gebruik van dezelfde (social engineering) technieken, zwakke plekken en exploits als alle andere malware. Uiteraard bestaat er simpele malware, die gemakkelijk kan worden tegengehouden. Maar er bestaat ook simpele ransomware die gemakkelijk wordt tegengehouden. Veel ransomware is relatief nieuw en maakt gebruik van relatief nieuwe beveiligingslekken, waar veel andere malware relatief oud is en gebruik maakt van oude beveiligingslekken, die relatief vaker al gepatcht zijn. Maar er is ook heel veel nieuwe malware, die gebruik maakt van dezelfde nieuwe beveiligingslekken als ransomware. Daar kunnen we de verklaring dan ook niet vinden.

Misschien heeft het te maken met het aantal mensen dat weet dat een infectie heeft plaatsgevonden. Meestal wanneer er een trojaan of keylogger op het bedrijfsnetwerk wordt aangetroffen, weet alleen de systeembeheerder van de infectie af. De meeste malware heeft immers tot doel om eerst ongemerkt kopietjes te maken van alle interessante bestanden op het systeem om die naar het moederschip te sturen en vervolgens zo lang mogelijk onopgemerkt op het netwerk te blijven rondhangen. Dan kan de malware de pc's van het netwerk inzetten in een botnet, waarmee DDoS-aanvallen kunnen worden gepleegd, waarmee spam kan worden verspreid en waarmee wachtwoorden kunnen worden gekraakt. Hoe langer de malware daar kan blijven zitten, hoe lucratiever de oorspronkelijke tijdsinvestering van het schrijven en verspreiden van de malware.

Het is om die reden dat (succesvolle) malware-infecties nauwelijks opvallen. De medewerkers van een bedrijf zullen er in de regel niets van merken. Dat ligt uiteraard anders bij ransomware. Bij een besmetting met ransomware, kan niemand binnen het bedrijf nog bij zijn bestanden en in de regel kan niemand zijn werkzaamheden nog uitvoeren. De kans dat het nieuws over een dergelijke besmetting uiteindelijk 'uitlekt', is uiteraard veel groter.

Sociaal aanvaard.

Toch is daarmee het verschijnsel nog niet volledig verklaard. Het meeste nieuws dat openbaar wordt over ransomware-besmettingen, wordt niet zozeer door loslippige medewerkers de wereld ingebracht. Het zijn meestal ook echt de IT-afdelingen die dergelijk nieuws met derden bespreken. Ik denk dat dat te maken heeft met sociale acceptatie.

Het werkt ongeveer zo: je hoort niemand erover dat een bepaalde banktrojaan op een zakelijk netwerk is aangetroffen. Als je als IT Manager ziet dat die banktrojaan op jouw systeem staat, kan dat eigenlijk maar één ding betekenen: je bent laks geweest. Je hebt een bepaalde patch niet op tijd uitgevoerd en nu is die banktrojaan uitgerekend op jouw netwerk binnengekomen. Je concurrenten en mede-ondernemers zijn veel verstandiger, want die hebben geen last van deze banktrojaan. Uit pure schaamte en angst voor een slechte reputatie besluit je de besmetting dood te zwijgen. En zo ondergaat de volgende die een besmetting met die banktrojaan ondergaat, hetzelfde denkproces.

Bij ransomware is deze spiraal doorbroken, wellicht met behulp van minder discrete medewerkers die het nieuws aan de grote klok hebben gehangen. In ieder geval lijkt het nu nog nauwelijks een issue te zijn om ervoor uit te komen dat je netwerk door ransomware is gegijzeld. Er zijn al zoveel voorbeelden van dit soort infecties bij andere bedrijven, dat we ons niet meer de enige sukkel voelen. En dat terwijl er precies dezelfde fouten aan ten grondslag liggen, zoals te late installatie van patches, het niet effectief filteren van e-mailbijlages en onvoldoende informeren van de medewerkers over de gevaren van links in e-mails, valse facturen en zip-files als bijlagen.

Bron: Eddy Willems / ZDnet

Index

Encryptie is één van de beste manieren om je bestanden te beschermen tegen diefstal. Met een tooltje als EncryptOnClick kost het niet eens veel moeite.

Bestanden encrypteren met een muisklik

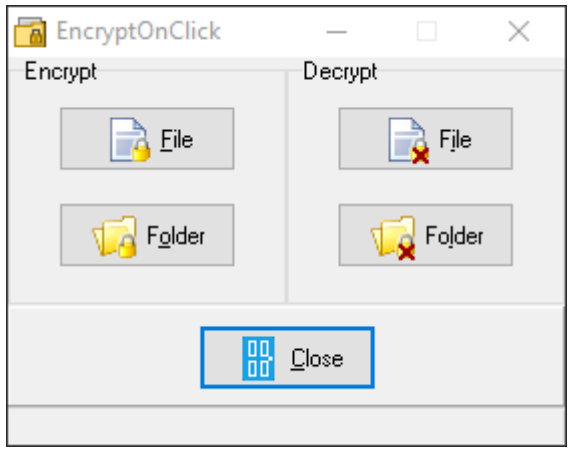
Datadiefstallen zijn tegenwoordig schering en inslag, en dus is het cruciaal dat je gevoelige bestanden voldoende beschermd. Een goede manier om dat te doen, is door ze te versleutelen. Met EncryptOnClick kost dat niet eens veel moeite.

EncryptOnClick is gratis encryptiesoftware waarmee je in enkele klikken een bestand of verzameling bestanden in een map kan versleutelen of weer ontsleutelen. De interface stelt weinig voor: met de twee knoppen in de linkerkolom kan je kiezen om een bestand of map te encrypteren, in de rechterkolom heb je twee gelijkaardige knoppen om te decrypteren. De encryptie die wordt uitgevoerd is 256-bit AES.

Wanneer je een bestand encrypteert, moet je een wachtwoord opgeven. Dat is de encryptiesleutel waarmee je het bestand achteraf weer kan ontcijferen. Het is belangrijk dat je dat wachtwoord goed onthoudt, aangezien het nergens wordt bewaard door EncryptOnClick. Ben je het wachtwoord vergeten, dan is er geen manier om weer toegang te krijgen tot het bestand.

EncryptOnClick encrypteert niet alleen je bestanden, het comprimeert ze ook, waardoor ze minder ruimte in nemen op je harde schijf. De geëncrypteerde bestanden kunnen ook met externe software zoals bijvoorbeeld WinRAR of WinZip9 worden gedecrypteerd (en uitgepakt). EncryptOnClick kan bovendien vanaf een USB-stick worden gebruikt, zodat je het tooltje altijd bij de hand hebt.

Wil je wat meer gemoedsrust dat je belangrijke bestanden beschermd zijn tegen eventuele diefstal,
geef EncryptOnClick dan zeker eens een kans. Het tooltje is erg compact en zeer eenvoudig in gebruik.



Bron: ZDnet

Index

Beveiligingsbedrijf G-Data lanceert Secure Chat, een gratis app die sms'en en chatberichten op je Android-mobieltje versleutelt.

Gratis afluistervrij sms'en en mobiel chatten

De versleuteling gebeurt van apparaat tot apparaat en valt onder de strenge Duitse privacy-wetgeving.

De gratis app G Data Secure Chat voor Android versleutelt sms- en chatberichten met behulp van het onkraakbaar geachte Axolotl-protocol. Niet alleen tekst, maar ook foto's, video's en andere media worden versleuteld.

De versleuteling gebeurt van apparaat naar apparaat, zowel voor individuele als voor groepchats. Er wordt dus geen informatie opgeslagen op de servers van G Data. Bovendien valt G Data onder de zeer strenge Duitse privacywetgeving. Gebruikers behouden de rechten over hun bestanden en berichten en hoeven dus niet bang te zijn dat hun communicatie wordt ge- of misbruikt door derden.

Je kunt berichten ook versturen met een zogenaamde zelfvernietigings-timer. Dan worden ze na een tijdje automatisch gewist. Je kunt je lokale chatgeschiedenis eveneens versleutelen en beveiligen met een wachtwoord. De app maakt ook (versleutelde) back-ups van je lokale chatgeschiedenis op een sd-kaart. Je kunt er tevens voor kiezen om het maken van schermafdrukken uit te schakelen voor berichtjes.

Bron: Disk Idee

Index

Kaspersky Safe Kids laat kinderen op een veilige manier internetten, terwijl ouders voldoende controle houden. De software is grotendeels gratis bruikbaar en werkt op Windows, Mac, Android en iOS.

Kaspersky Safe Kids voor Windows, Mac, Android en iOS

Je beheert Kaspersky Safe Kids via het My Kaspersky portal waarmee je ook de gewone antimalwareproducten van het bedrijf instelt en gebruikt. Als je nog niet geregistreerd bent, moet je dat eerst doen. Vervolgens maak je een profiel aan voor het kind en download je de software voor het gewenste platform of installeer je de app op afstand via de App Store van Apple of Google Play.

Daarna kun je allerlei regels instellen en vervolgens bewaken en bepalen cq. beperken hoeveel tijd het kind gebruik maakt van zijn apparaten, de apps die hij of zij installeert, bekeken webpagina's, de locatie van een kind en zijn contacten. Je kunt ook e-mailmeldingen instellen die naar je gestuurd worden wanneer de software detecteert dat het kind geconfronteerd wordt met een bedreiging. Je moet dan zelf ook Safe Kids op je toestel installeren.

De tijdbeheerfunctie en het beperken van apps per categorie werkt om technische reden niet op iOS, wel op de andere ondersteunde platformen. De locatiefunctie werkt alleen voor Android en iOS wanneer de gps is ingeschakeld en het apparaat verbonden is met internet.

Als extra optie bieden Android-gebaseerde apparaten statistieken over de contacten door wie kinderen worden gebeld en van wie het sms-berichten ontvangt (om de privacy niet te schenden wordt de tekst van deze berichten niet weergegeven).

Kaspersky Safe Kids is grotendeels gratis, maar voor enkele functies moet je een kleine vergoeding betalen. In de gratis versie kun je de online activiteiten van je kinderen beheren, het applicatiegebruik beperken en het apparaatgebruik beheren.

De Apple-versie vereist iOS 7 of hoger of Mac OS X 10.9 / 10.10 met minstens 2 GB vrije ram; de Android-versie werkt vanaf Android 3.0 (maar nog niet op 6.0) en vereist een minimale schermresolutie van 320 x 480 pixels; de Windows-versie ten slotte werkt in principe op alle Windows-versies die minstens 120 MB vrije ruime op de harde schijf hebben. Een internetverbinding is in alle gevallen nodig voor de productinstallatie, de eerste configuratie en updates. De software werkt momenteel alleen in het Engels.

Bron: Kaspersky

Index

De zoekmachines StartPage en Ixquick, die beide de privacy van hun gebruikers centraal stellen, gaan voortaan samen verder, waardoor de grootste privacyzoekmachine van Europa ontstaat.

StartPage en Ixquick worden één privacyzoekmachine

Ixquick bestaat sinds 1998 als metazoekmachine en werd in 2006 de eerste privacyvriendelijke zoekmachine op het web.

StartPage bestaat sinds 2009 en biedt Google-zoekresultaten met 'gewaarborgde privacy'. Beide zoekmachines zijn eigendom van het Nederlandse Surfboard Holdings en slaan de ip-adressen van gebruikers niet op en geven die ook niet door. Verder wordt persoonlijke informatie van gebruikers niet bijgehouden. StartPage biedt verder bij iedere zoekopdracht een gratis proxydienst aan. Net als StartPage toont Ixquick.com nu actuele zoekresultaten van Google, waarbij de anonimiteit van de gebruiker volgens de ontwikkelaars volledig gewaarborgd is.

Via Ixquick.eu hebben bezoekers nog steeds de mogelijkheid om de klassieke Ixquick metazoekresultaten te bekijken. "Het aantal zoekopdrachten is de laatste jaren explosief gegroeid en we verwerken nu meer dan 6 miljoen zoekopdrachten per dag. Dat komt omdat we onze gebruikers privacy bieden en ze relevante, ongecensureerde zoekresultaten krijgen. Dat spreekt steeds meer mensen aan. Onder één naam kunnen we ons nog beter richten op verdere groei", zegt Robert Beens, directeur van StartPage.

Bron: Security.nl

Index

Snapshots

De Belgische antiterreurcoördinator Gilles de Kerchove voorspelt dat er binnen vijf jaar aanslagen via internet komen. Terroristen zijn dan in staat om in te breken in systemen van bijvoorbeeld kerncentrales, stuwdammen of het openbaar vervoer. De Kerchove wil daarom extra aandacht voor wat (potentiële) terroristen online doen. ‘Geïsoleerde personen kunnen gemakkelijk een aanslag beramen via internet’. Onlangs werden in de VS nog zeven Iraniërs aangeklaagd voor hackaanvallen op de VS. Bij een daarvan werd geprobeerd een stuwdam te hacken. Dat dit niet lukte, is een kwestie van tijd, vreest De Kerchove.

———————————————————

Het Korps Mariniers van het Amerikaanse leger kan door de lancering van een nieuwe eenheid voortaan ook missies in cyberspace uitvoeren. De Marine Corps Cyberspace Warfare Group heeft als doel om mariniers te trainen en voor te bereiden voor het uitvoeren van cyberpacemissies.

———————————————————

Er is een nieuwe versie van Firefox voor iOS verschenen, waarbij de wachtwoordmanager nu via een viercijferige pincode of Touch ID kan worden beveiligd. Op deze manier kunnen gebruikers op toestellen met Touch ID via een vingerafdruk hun wachtwoorden opvragen en op allerlei websites gebruiken.

———————————————————

Als het aan de Britse politietopman Gavin Thomas ligt worden 16-jarigen ingezet voor het bestrijden van cybercrime. Op dit moment is de minimale leeftijd voor politieagenten 18 jaar, maar Thomas wil dat ook 16-jarigen kunnen worden aangenomen.

———————————————————

Een terreurverdachte die vorig jaar augustus door de Franse autoriteiten werd aangehouden bleek het wachtwoord van zijn met TrueCrypt versleutelde usb-stick op een papiertje te hebben geschreven, dat hij in zijn tas bewaarde. Het gaat om een 29-jarige computertechnicus uit Parijs die zich bij terreurorganisatie IS had aangesloten. Als onderdeel van zijn training werd uitgelegd hoe hij het encryptieprogramma TrueCrypt moest gebruiken. Eenmaal in het Syrische Raqqa aangekomen ontving hij een usb-stick met TrueCrypt en het programma CCleaner om de surfgeschiedenis van zijn computer te wissen. Vervolgens moest hij naar Europa terugkeren om daar een aanslag te plegen.

Om met zijn contactpersoon in Syrië te communiceren moest de man een met TrueCrypt versleuteld bestand op een Turkse opslagdienst opslaan. Vervolgens werd het door zijn contactpersoon gedownload. Hij mocht het bestand niet via e-mail versturen, om zo geen metadata achter te laten. Eén van de kameraden van de man werd echter in Spanje aangehouden, waardoor de opsporingsdiensten hem op het spoor kwamen. Na te zijn ingelicht volgde de Franse politie de man naar de woning van zijn moeder in Parijs. Tijdens een huiszoeking werd hij aangehouden en vonden agenten achter een bank zijn usb-stick van IS en in zijn tas het bijbehorende TrueCrypt-wachtwoord.

———————————————————

Microsoft heeft strengere regels aangekondigd voor programma's die de werking van browsers aanpassen, zoals toolbars. Vorig jaar kwam Microsoft al met strengere regels voor agressieve adware en software die advertenties injecteert. Zo is het niet meer voor dit soort software toegestaan om beveiligingsmaatregelen van het systeem te omzeilen of man-in-the-middle-aanvallen uit te voeren.

———————————————————

Niet in het voetbal, maar wel in de drugshandel. Nederland is Europees kampioen drugshandel. Althans volgens een EU-rapport, op basis waarvan het AD Nederlands zelfs een narcostaat noemt, ‘een polderversie van Mexico en Colombia ineen’. Europeanen besteden jaarlijks 24 miljard aan drugs en een groot deel daarvan komt via Nederland de EU binnen dan wel wordt via Nederland verhandeld dan wel vloeit naar Nederland. Essentieel, zoals in elke sector, is innovatie, aldus het rapport: Nederlandse drugscriminelen tonen ambitie, zoeken naar slim gebruik van nieuwe technieken en kijken naar de toekomst. Ook de drugs die op het dark web, een aantal goed verborgen platforms op internet, worden verkocht, komen voor een flink deel uit Nederland. ‘Zo zet een lange Nederlandse handelstraditie zich onverminderd voort’.

———————————————————

Swipe right for #mdma! Drugsdealers hebben massaal bezit genomen van populaire apps als Instagram, Tinder en Kik om daar nieuwe klanten te vinden. Simpel: met een paar hashtags, bijvoorbeeld #weed4sale, zijn honderden advertenties te vinden. Je kunt de verkopers vervolgens direct benaderen, betalen gaat via Western Union, via bitcoins of via pre-paid gift cards. En de post doet de rest. Zelfs op Tinder werkt het: swipen totdat je een dealer vindt, daarmee matchen en vervolgens chatten. The Guardian schrijft dat de meeste kopers jongeren zijn. Logisch, dat zijn degenen die sociale media het vaakst gebruiken. Aan de risico’s lijken ze niet te denken, aldus de krant. Veel dealers bieden hun spul aan als ‘research chemicals’ en wanen zich onaantastbaar, net als de kopers. Voor zover mogelijk proberen de platforms illegale advertenties te verwijderen maar ja, met tientallen miljoenen foto’s per dag is dat een lastige zaak, bekent een woordvoerder van Instagram. En lang niet elke gebruiker maakt gebruik van de ‘report’ button. Een woordvoerder van de National Police Chiefs Council komt niet verder dan de opmerking dat de digitale wereld ‘de beschikbaarheid en de gevaren van drugs heeft veranderd’ en dat ‘we must adapt to these challenges’.

———————————————————

Een app die was ontwikkeld door de Taliban, is niet langer verkrijgbaar in Google’s Play Store. De app gaf toegang tot onder meer officiële verklaringen en videofilmpjes. Ze werd ontdekt door jihadmonitor Site, die direct Google inlichtte over de app. De Taliban heeft nog wel een website – in vijf talen! – en allerlei accounts op sociale netwerken.

Index

Cops in Cyberspace

Twee mannen (29 en 50, uit Hardenberg) hebben voorwaardelijke taakstraffen van dertig uur gekregen omdat ze een jeugdagente hadden beledigd op facebook. Onder een foto waarop de agente een dronken voetbalsupporter in een houtgreep neemt, schreven ze: 'het is blauw en het wurgt je'. De foto was al jaren oud, genomen in Vroomshoop na een WK-wedstrijd in 2010, maar de stiefvader van de gemangelde jongen bleef boos. Voorjaar 2015 zet hij de foto op facebook, met de bewuste tekst erbij. De jongste verdachte 'deelt' de foto, als hij in een kliniek afkickt van zijn ghb-verslaving. Hij vond het een lachwekkende foto. 'Op sociale media wordt iedereen in de zeik genomen'. Enfin, de agente doet aangifte, de advocaat beschuldigt de politie van 'hijgerigheid omdat het een collega betreft' en zegt dat de agente zélf het risico neemt dat 'lolbroeken haar foto bewerken en op internet plaatsen'. De officier spreekt van een grens die is overschreden 'als foto's worden geshopt' en de rechter … Die acht smaad bewezen. 'Dit zijn geen grappen meer'. Als burgers botsen met politiemensen, kunnen ze een klacht indienen, maar 'het mag niet onnodig grievend of beledigend zijn'.

———————————————————

Een medewerkster van de politie, bekend als 'seksagente', is terecht ontslagen, vindt de rechter. De vrouw, die adverteerde op internet, werkte in een illegale club, was beschikbaar voor gangbangs (maximaal acht mannen à 95 euro pp) in een bedrijfspand in Apeldoorn. Toen het politieteam mensenhandel en prostitutie in 2012 getipt werd over een seksadvertentie van de vrouw, werd een onderzoek gestart. De vrouw zelf vond dat het om privéactiviteiten ging en dat ze niet chantabel was, maar de politieleiding dacht daar anders over. De vrouw had geen vergunning, werkte in een crimineel milieu, verdiende zwart bij en dat is allemaal onverenigbaar met een baan bij de politie. De vrouw werd daarom voorgedragen voor ontslag. En daar is de rechter het mee eens. Agenten mogen prostituees bezoeken (wel 'buiten de regio waar zij werken', schrijft de krant) maar niet als zodanig actief zijn. De vrouw mag van de korpsleiding overigens wel weer parenclubs bezoeken.

———————————————————

De politie heeft zowel tijdens het tv-programma Bureau Brabant als op Politie.nl een verkeerde foto van een verdachte getoond. Voor de zoveelste keer, klinkt het op sociale media. De politie toonde in een pinpasfraudezaak de bewakingscamerafoto van een man die niets met de zaak te maken heeft. De foto was door de bank doorgestuurd, maar was op een andere dag gemaakt. De politie verzuimde de beelden 'voldoende te controleren', aldus een woordvoerder. Januari jl ging het bij Bureau Rijnmond al een keer fout, vorig jaar in het programma Team West.

———————————————————

'Ken jij iemand die nooit richting aangeeft? Tag hem/haar dan en misschien vergeet hij/zij het nooit meer!' De politie Apeldoorn heeft in 'een opmerkelijke' facebookpost haar volgers opgeroepen om mensen die verkeersovertredingen maken, te taggen. De post gaat over het gebruik van richtingaanwijzers bij inhalen of wegrijden. 'Een kleine moeite' om die te gebruiken, aldus het bericht dat niet bij iedereen goed viel. Veel mensen vragen zich hardop af of de politie dat zelf ook niet eens wat vaker moet doen, 'bijvoorbeeld als jullie weer eens door rood knallen om op tijd voor het eten op het bureau te wezen'. Eén facebookgebruiker tagde overigens 'alle BMW-rijders' …

———————————————————

Het is de politie 'een doorn in het oog' dat het steeds gemakkelijker wordt om software aan te schaffen waarmee cybercrime kan worden gepleegd. In De Telegraaf zegt Rob van Bree, portefeuillehouder Intensivering Aanpak Cybercrime van de Nationale Politie, dat het aanbod 'zorgen baart'. Software om te hacken, te phishen of ransomware – het is overal verkrijgbaar, steeds goedkoper en steeds makkelijker. 'Vroeger moest je die software zelf bouwen, nu kun je het op internet kopen'. Ook Inge Philips, plaatsvervangend hoofd van de landelijke recherche, noemt de situatie zorgwekkend. De politie pleit al langer voor meer opsporingsmogelijkheden voor cybercrime, die mogelijk worden geregeld met de Wet Computercriminaliteit III . Critici vrezen dat deze wet de politie de bevoegdheid zou geven om 'terug te hacken', maar dat is het niet, zegt Philips. 'Het is niets anders dan een reguliere inval van een arrestatieteam'.

———————————————————

Ook de Duitse politie is, net als de Nederlandse, 'bezorgd' over de toenemende internetactiviteiten tegen vluchtelingen en asielzoekers. En waar de Nationaldemokratische Partei Deutschlands (NPD) al in 2013 op facebook opriep tot een burgerwacht, ziet de Duitse politie vooral de laatste maanden een enorme toename van lokale of regionale facebookgroepen van Bürgerwehr- of Bürgerschutzinitiatieven. Het grootste probleem daarbij is de bemoeienis van neo-nazi's en andere rechtsextremisten. Veel groepen ontstaan omdat 'de politie te slap' optreedt tegen vluchtelingen, staat te lezen op de pagina's. Politie en OM zeggen bezorgd te zijn over de populariteit van de groepen. Alleen al op facebook zijn een stuk of vijftien groepen te vinden, met stuk voor stuk duizenden leden. In één van de groepen, Gemeinsam gegen Gewalt an Frauen und Kinder (drieduizend leden) staat een filmpje waarin de beheerder van de groep de Hitlergroet brengt. In andere groepen staat dat 'als de staat ons niet meer beschermt, wij ons zelf wel beschermen'. In álle groepen staat overigens netjes te lezen wat artikel 127 van de Duitse Strafwet behelst: iedere burger mag een crimineel op heterdaad staande houden en aan de politie overdragen.

Index

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

Doe jij het veilig online

Malware

WiFi ontvangst verbeteren

Internetfraude via de telefoon

Documentaire: Veiligheid en privacy

Herken een nep-hotspot

Gebruik wachtzinnen

Drive-by-downloads voorkomen

Hoe herken je een phishing mail

Beveiligd internetbankieren

Privacy—ik heb toch niets te verbergen

Webinar Computercriminaliteit

Mousejack

Gegijzeld door Ransomware. Wat nu?

Telefonische phishing

Nieuw:

Grooming

Sexting

Webcammisbruik

Bedreigd/gechanteerd

Kinderporno

Nepprofiel

Bron: YouTube/TekTok/Heplwanted

Index

Cybercrime wetsartikelen

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

Bron: Maxius

Overzichtstabel cybercrime

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: Rijksoverheid

Index

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

Actuele phishingmails:

klik hier

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

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

MARKTPLAATS: veilig handelen

opgelet op internet.nl

Computerwoordenboek

Index

OneDrive extra's

Naslag:

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

Muziek: DoubleYouAB

- Return to TubularBells
- FeddeLeGrand remix
- Faithless Insomnia remix
- ReeAnna2015
- 1.11 Armin
- SummerHardstyle2015
- Summermix2015
- TrancePhonic 2015
- Open Your Eyes 2015 rmx
- MikeOldfieldReborn
- MashedUp2011
- Heilig rmmstnmix

OneDrive

Index