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.

Start enquête

Vaste rubrieken

Cybercrime zal voorlopig niet apart in de Nationale Veiligheidsindex (NVI) worden opgenomen, zo blijkt uit onderzoek van het Wetenschappelijk Onderzoek- en Documentatie Centrum (WODC) van het ministerie van Veiligheid en Justitie.

Cybercrime voorlopig niet in Nationale Veiligheidsindex

Het WODC heeft de NVI ontwikkeld om de ontwikkeling in criminaliteit, overlast en onveiligheidsgevoelens in Nederland en op regionaal niveau in kaart te brengen.

In de NVI is criminaliteit opgesplitst naar elf soorten delicten, zoals moord en doodslag, geweldsdelicten en zedendelicten. Cybercrime ontbreekt echter, ook al heeft het onderwerp de afgelopen jaren steeds meer aandacht gekregen in het maatschappelijke en wetenschappelijke debat. Ook op de Veiligheidsagenda 2015-2018 van het ministerie van Veiligheid en Justitie neemt de bestrijding van cybercrime een prominente positie in.

Voor het onderzoek wilden de onderzoekers kijken hoe cybercrime het beste gedefinieerd worden, alsmede of cybercrime als los delict type in de NVI moet worden meegenomen of dat er onderscheid moet worden gemaakt tussen verschillende vormen van cybercrime. Ook zochten de onderzoekers naar databronnen die beschikbaar en bruikbaar zijn om de ontwikkeling in cybercrime in Nederland weer te geven.

Opnemen

Uit het onderzoek blijkt dat cybercrime niet op korte termijn kan worden meegenomen in de NVI. Momenteel wordt cybercrime al meegeteld in de bestaande delict typen van de NVI. Eerst zal er een manier ontwikkeld moeten worden om cybercrime los te koppelen van de bestaande soorten misdrijven. Een mogelijke methode is door aangiften en meldingen bij de politie nader te analyseren met behulp van textmining. Textmining heeft echter grote gevolgen voor de methode van de NVI. Nu worden politiedata gebruikt die voor iedereen zijn op te vragen via het CBS. Bij textmining dient data te worden gebruikt die niet vrij toegankelijk zijn.

Daarnaast zal de criminaliteitsindex van de NVI een ander beeld geven dan tot op heden wanneer de online gepleegde delicten losgekoppeld worden van de offlinedelicten. Ook is het afzonderlijk meenemen van cybercrime in de NVI op korte termijn niet opportuun, zo stellen de onderzoekers. Omdat politiecijfers slechts een beperkt beeld geven van cybercrime, zijn deze cijfers nog niet geschikt om de ontwikkeling in cybercrime betrouwbaar te beschrijven. Een alternatief is om de ontwikkeling in cybercrime te beschrijven aan de hand van de ontwikkelingen in verschillende verschijningsvormen, zoals: hacken, botnets, DDoS-aanvallen, malware en defacing. Deze verschijningsvormen kunnen worden gemeten met een combinatie van data van politie en justitie, slachtofferenquêtes, meldpunten en aanbieders van cybersecuritysoftware. Eerst zal echter een lijst moeten worden opgemaakt van databronnen die een betrouwbaar beeld geven van de verschijningsvormen. Hierover is namelijk nog veel onbekend. "Gezien de verschuiving van offline criminaliteit naar online criminaliteit is het wenselijk om op korte termijn meer inzicht te krijgen in de ontwikkeling van cybercrime, naast de ontwikkeling van de offline criminaliteit", aldus de onderzoekers.

Bron: Security.nl

Index

Elke maand krijgt de Landelijke Eenheid van de politie ongeveer vierhonderd meldingen binnen over de vondst van beeldmateriaal van kinderporno op internet.

Meldingen kinderporno ruim verdubbeld

Het aantal meldingen is meer dan verdubbeld van 2240 in 2014 naar 4908 vorig jaar, vooral vanuit het buitenland. Dit jaar zal het aantal opnieuw sterk stijgen.

Dat is de verwachting van de politie en het Openbaar Ministerie (OM) in een rapport, dat minister Van der Steur van Justitie onlangs naar de Tweede Kamer stuurde.

De stijging komt vooral door Amerikaanse regels die internetbedrijven ertoe verplicht melding te maken van het aantreffen van strafbaar materiaal. Dat leidt ertoe dat iedere nieuwe internetdienst op de markt een nieuwe stroom meldingen oplevert. Die trend zal zich de komende jaren doorzetten, verwachten ze.

Verder is vorig jaar het aantal onderzoeken en interventies uitgekomen op 842. Dat zijn er 242 meer dan het streefcijfer van het kabinet. Dit komt onder meer doordat nu ook de eenvoudiger zaken worden meegeteld. Het blijkt steeds lastiger voor de politie om verdachten op te sporen via een IP-adres van de computer.

Dat komt omdat ze meer gebruik maken van internet via laptops, mobiele telefoons of via open netwerken of wifi-hotspots. Daarom moeten opsporingsmethoden verder worden ontwikkeld, bepleit de politie. Van der Steur wil de (internationale) aanpak van kinderporno en kindersekstoerisme de komende jaren verder versterken

Bron: Security.nl

Index

Uit de memorie van toelichting voor de nieuwe Wet Computercriminaliteit 3

De heling van gegevens

Algemeen

Het wetsvoorstel beoogt de strafrechtelijke bescherming van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen verder te verbeteren. Daartoe bevat het wetsvoorstel twee elementen:

- Het wordt strafbaar om niet-openbare gegevens die door middel van een geautomatiseerd werk zijn opgeslagen wederrechtelijk met een technisch hulpmiddel over te nemen (artikel 138c Sr).
- Het wordt strafbaar om niet-openbare gegevens die door misdrijf zijn verkregen voorhanden te hebben of bekend te maken (artikel 139f Sr).

Met de eerstgenoemde strafbaarstelling – betreffende het wederrechtelijk overnemen van gegevens – wordt een betere bescherming geboden tegen het overnemen van gegevens uit een geautomatiseerd werk, in die gevallen waarin de gegevens gekopieerd zijn en de rechthebbende dus de beschikking houdt over de gegevens. De rechthebbende heeft echter geen invloed op het gebruik dat vervolgens van de overgenomen gegevens kan worden gemaakt, waardoor hij benadeeld kan worden.

Met de als tweede genoemde strafbaarstelling wordt strafrechtelijke aansprakelijkheid gecreëerd van degene die dergelijke gegevens voorhanden heeft of bekend maakt. Langs deze weg wordt “heling” van de desbetreffende gegevens strafbaar gesteld. Hiermee wordt uitvoering gegeven aan een toezegging aan de Tweede Kamer om heling van gegevens strafbaar te stellen.

Strafbaarstelling van “heling” van gegevens is van belang in situaties waarin niet aangetoond kan worden dat de persoon die deze gegevens bekend maakt degene is die deze gegevens zelf heeft overgenomen, al dan niet na in een geautomatiseerd werk te zijn binnengedrongen (de computervredebreuk, strafbaar gesteld in artikel 138ab Sr).

De beide voorgestelde strafbaarstellingen waren opgenomen in een conceptwetsvoorstel dat reeds eerder in consultatie is gegeven. Zij zullen in hun onderlinge samenhang worden besproken.

De voorgestelde strafbaarstellingen

Met het voortschrijden van de informatie- en communicatietechnologie wordt het steeds eenvoudiger om gegevens uit een computer over te nemen en vervolgens op het internet te zetten. Daardoor kan het gebeuren dat vertrouwelijke gegevens snel worden verspreid en voor grote groepen mensen toegankelijk worden. Het is bovendien niet eenvoudig om via het internet verspreide gegevens daarvan volledig verwijderd te krijgen.

De technologische ontwikkelingen nopen tot een verdere strafrechtelijke bescherming van gegevens. Het uit een computer overnemen van gegevens over personen, en die gegevens vervolgens op het internet zetten, zijn verwerpelijke gedragingen waartegen adequaat strafrechtelijk moet kunnen worden opgetreden, vooral met het oog op bescherming van de persoonlijke levenssfeer van degene wiens gegevens het betreft. De personen die zich aan dergelijke handelingen schuldig maken, kunnen weten dat het hier om verwerpelijke gedragingen gaat.

Dit is niet alleen van belang voor de bescherming van de persoonlijke levenssfeer. De strafbaarstelling van het voorhanden hebben van door misdrijf verkregen gegevens is ook van belang voor gevallen waarin een verdachte waardevolle gegevens voorhanden heeft, zoals bankrekeningnummers of wachtwoorden, die eerder door misdrijf zijn verkregen. In veel gevallen is computercriminaliteit gericht op het wederrechtelijk vergaren van gegevens en het vervolgens gebruiken van deze gegevens bij het plegen van andere misdrijven. Het inbreken in computers van bedrijven om gegevens over creditcards te achterhalen of het door middel van het zogenaamde phishen (het opzetten van een valse website) ontfutselen van bancaire gegevens en pincodes zijn hier inmiddels bekende voorbeelden van.

Phishing is strafbaar als een vorm van oplichting (artikel 326 Sr). Vereist is dat een persoon door middel van – kort gezegd – misleiding wordt gebracht tot de afgifte van een goed of van gegevens. Het is niet (meer) vereist dat deze gegevens een geldswaarde in het handelsverkeer hebben.

Gebleken is dat het thans niet mogelijk is een persoon te vervolgen voor “heling” van gegevens die door dergelijke misdrijven zijn verkregen. Het College van procureurs-generaal heeft – bij gelegenheid van de consultatie over het ontwerp van het aan de Wet van 12 juni 2009, Stb. 245 ten grondslag liggende wetsvoorstel – aandacht gevraagd voor de onmogelijkheid iemand te vervolgen voor het “helen” van gegevens.

Bij verschillende gelegenheden is gebleken dat behoefte bestaat aan een dergelijke mogelijkheid. Dit betrof volgens het College onder meer een geval waarbij gegevens door computervredebreuk uit een e-mailbox waren gekopieerd, en vervolgens aan een derde doorgegeven. Deze derde heeft de gegevens, ondanks dat vrijwel vaststond dat hij moest weten dat zij door misdrijf waren verkregen, in ontvangst genomen en door middel van het internet gepubliceerd.

Omdat het in deze zaak om (gekopieerde) gegevens ging, en niet om een goed, kon deze derde niet strafrechtelijk aansprakelijk worden gesteld voor heling van een goed. De hacker kon worden vervolgd wegens computervredebreuk (artikel 138ab Sr). Inmiddels hebben ook andere gevallen in de media de nodige aandacht gekregen, zoals de publicatie op het internet van door computervredebreuk verkregen digitale naaktfoto’s van een bekende presentatrice.

Naar aanleiding van dit geval zijn Kamervragen gesteld over de noodzaak om “heling” van gegevens strafbaar te stellen. Bij de beantwoording van die vragen is aangegeven dat strafbaarstelling van heling van gegevens bij het onderzoek van de knelpunten in het juridisch instrumentarium zal worden betrokken en dat de mogelijkheden voor een juridische vormgeving van een dergelijke strafbepaling zullen worden onderzocht . Dit onderdeel van het voorliggende wetsvoorstel vormt het resultaat daarvan.

Burgers, bedrijven en de overheid zijn zich in toenemende mate bewust van de gevaren die aan het misbruik van gegevens verbonden zijn en investeren het nodige om hun gegevens tegen onrechtmatige toegang en gebruik te beschermen. Gelet op de maatschappelijke belangen die op het spel staan bij het onrechtmatige bezit of gebruik van gegevens is het van belang dat de strafrechtelijke bescherming tegen misbruik van gegevens verder wordt verstrekt.

Voor een vermindering van de prikkel om systemen goed te beveiligen behoeft niet te worden gevreesd, omdat burgers en bedrijven zich voldoende bewust zijn van het belang van een adequate gegevensbeveiliging. Bovendien is het ook voor het misdrijf van computervredebreuk – met de inwerkingtreding van de Wet computercriminaliteit II – niet langer vereist dat een beveiliging wordt doorbroken. De strafbepalingen van diefstal en verduistering van goederen – uit een woning of gebouw – zijn evenmin gebonden aan een dergelijk vereiste.

Met de Wet computercriminaliteit is er destijds voor gekozen om gegevens begripsmatig afzonderlijk te behandelen en niet gelijk te stellen aan een “goed”. Ook in de jurisprudentie van de Hoge Raad is de gelijkstelling van gegevens aan een goed afgewezen . Doorslaggevend argument is dat een “goed” individualiseerbaar is en dat degene die de feitelijke macht daarover heeft deze noodzakelijkerwijze verliest indien een ander zich de feitelijke macht erover verschaft.

Gegevens kunnen echter worden overgenomen zonder dat de rechthebbende de beschikkingsmacht over de gegevens verliest. De rechthebbende kan echter geen invloed uitoefenen op het gebruik dat vervolgens van de overgenomen gegevens wordt gemaakt, waardoor hij benadeeld kan worden als de gegevens worden geopenbaard of anderszins worden aangewend op een wijze waardoor zijn belangen worden geschaad.

Daar waar de gegevens buiten de beschikkingsmacht van de rechthebbende worden gebracht is strafvervolging op grond van diefstal volgens enkele uitspraken van feitenrechters niet uitgesloten. Een voorbeeld hiervan betreft de diefstal van een virtueel amulet en een virtueel masker uit een online computerspel.

Het onderscheid dat met de Wet computercriminaliteit is gemaakt tussen het begrip goed en het begrip gegevens heeft ertoe geleid dat in het Wetboek van Strafrecht en het Wetboek van Strafvordering specifieke bepalingen zijn opgenomen met betrekking tot gegevens. Zo kent het Wetboek van Strafrecht afzonderlijke strafbaarstellingen van computervredebreuk (artikel 138ab Sr), het wederrechtelijk aftappen of opnemen van gegevens (artikel 139c Sr), het beschikken over of bekend maken van gegevens die zijn afgetapt, opgenomen of afgeluisterd (artikel 139e Sr), het “vernielen” van gegevens (artikelen 350a en 350b Sr), het bekend maken of uit winstbejag gebruiken van gegevens over een onderneming (artikel 273 Sr), alsmede strafbaarstelling van de persoon die werkzaam is bij een aanbieder van een telecommunicatienetwerk of -dienst en die wederrechtelijk niet voor hem bestemde gegevens overneemt (artikel 273d Sr).

In lijn met de keuze die destijds bij de Wet computercriminaliteit en de Wet computercriminaliteit II is gemaakt, is ervoor gekozen de benodigde verbeteringen in de strafrechtelijke bescherming van gegevens door te voeren in de strafbepalingen die in de Vijfde Titel van het Tweede Boek van het Wetboek van Strafrecht zijn opgenomen. Het – in het algemeen – strafbaar stellen van het wederrechtelijk overnemen van gegevens die zijn opgeslagen door middel van een geautomatiseerd werk sluit aan bij de in die titel opgenomen strafbaarstelling van het wederrechtelijk aftappen of opnemen van dergelijke gegevens (artikel 139c Sr).

Bovendien is het overnemen van gegevens uit een geautomatiseerd werk door iemand die daarin wederrechtelijk is binnengedrongen ook reeds in die titel strafbaar gesteld (artikel 138ab, tweede lid, Sr). Het wederrechtelijk overnemen van gegevens is voorts, zoals hierboven werd aangestipt, strafbaar gesteld voor zover dit gebeurt door een persoon die werkzaam is bij een aanbieder van een telecommunicatienetwerk of –dienst (artikel 273d Sr).

De door het voortschrijden van de informatie- en communicatietechnologie wenselijke versterking van de strafrechtelijke bescherming van gegevens brengt mee dat het wederrechtelijk overnemen van gegevens in het algemeen strafbaar wordt gesteld.

Voor strafbaarheid van het wederrechtelijk overnemen van gegevens is niet – zoals in artikel 138ab, tweede lid, Sr – vereist dat het geautomatiseerde werk waaruit de gegevens worden overgenomen, is binnengedrongen. Met andere woorden: de gegevens behoeven niet door computervredebreuk te zijn verkregen.

De voorgestelde strafbepaling is, in aanvulling op de strafbaarstelling van computervredebreuk, vooral van belang voor gevallen waarin de dader rechtmatige toegang heeft tot niet-openbare gegevens van een computer, en deze gegevens wederrechtelijk overneemt. Daarbij kan worden gedacht aan de werknemer die gegevens waartoe hij uit hoofde van zijn functie toegang heeft, kopieert met de bedoeling deze voor zichzelf of voor een ander te gebruiken.

Om deze reden wordt artikel 139c Sr in dit wetsvoorstel zo gewijzigd dat niet alleen het opnemen van gegevensoverdracht (stromende gegevens) maar ook het wederrechtelijk overnemen van opgeslagen gegevens – in het algemeen – strafbaar wordt. Hiermee wordt tegemoet gekomen aan situaties waarin personen gegevens van een computer waartoe zij rechtmatige toegang hebben, bijvoorbeeld vanwege hun functie bij een overheidsinstelling, zonder daartoe gerechtigd te zijn voor zichzelf of voor een ander overnemen. Er is dan als het ware sprake van “verduistering” van gegevens, met dien verstande dat de rechthebbende de beschikkingsmacht over de gegevens behoudt, in welk geval strafvervolging op grond van artikel 321 Sr niet mogelijk is omdat in een dergelijk geval van een goed geen sprake is.

Met het gebruik van de term “overnemen” wordt tot uitdrukking gebracht dat niet is vereist dat de gegevens buiten de beschikkingsmacht van de rechthebbende worden gebracht. Het opzettelijk en wederrechtelijk overnemen van de gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, vormt daarmee een zelfstandige strafbare gedraging.

Samenvattend: met de voorgestelde artikelen 138c en 139f Sr wordt de rechthebbende van gegevens een betere bescherming geboden tegen personen die de gegevens waar zij rechtmatig toegang toe hebben overnemen, zonder dat er sprake is van computervredebreuk. Tevens wordt voorzien in een strafbaarstelling van een gedraging die zou kunnen worden aangemerkt als “heling” van dergelijke gegevens.

Bron: Rijksoverheid

Index

Uit de memorie van toelichting voor de nieuwe Wet Computer-criminaliteit 3

Cybercrimeverdrag begripsomschrijvingen

Secure Computing

Gegevens:

‘Een weergave van feiten, begrippen of instructies op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of door automatische middelen’.

Opgemerkt wordt nog dat onder ‘feiten’ zowel reële als denkbeeldige gebeurtenissen worden begrepen. Onder deze definitie vallen niet alleen gegevens die zijn opgeslagen of worden overgedragen met het oogmerk om de mens informatie ter beschikking te stellen, maar ook programmatuur, ongeacht de vraag of deze auteursrechtelijk is beschermd .

Geautomatiseerd werk :

‘Elke inrichting die met technische middelen geschikt is gemaakt voor de opslag, verwerking of overdracht van gegevens’.

Het begrip ‘geautomatiseerd’ duidt op een functioneren van het werk voor een deel onafhankelijk van menselijk ingrijpen. Hieronder vallen dus computers, netwerken van aan elkaar verbonden computers en geautomatiseerde inrichtingen voor telecommunicatie. Hieronder vallen dus niet werken die uitsluitend bestemd zijn voor de opslag van gegevens of eenvoudige werken die in beginsel slechts bestemd zijn om te functioneren zonder interactie met hun omgeving, zoals een elektronisch klokje. Bij de huidige stand van de techniek gaat het om het omgaan met elektronische of optische middelen. In de naaste toekomst zullen wellicht ook biotechnische ontwikkelingen hieronder vallen.

Aftappen:

‘elke momentane kennisneming van gegevens’

Opnemen:

‘het vastleggen van gegevens op enige gegevensdrager’

Ook het enkel visueel kennis nemen van gegevens op bijvoorbeeld een beeldscherm is al een vorm van (eventueel strafbaar) ‘aftappen’.

Verder:

- **a.**„computersysteem", ieder apparaat of geheel van onderling verbonden of samenhangende apparaten, waarvan een of meer overeenkomstig een programma geautomatiseerde gegevensverwerking uitvoert;
-
- **b.**„computergegevens", iedere weergave van feiten, informatie of begrippen in een vorm die geschikt is voor verwerking in een computersysteem, met inbegrip van een programma dat geschikt is om een computersysteem een functie te laten verrichten;
-
- **c.**„serviceprovider":
- **i.**iedere publieke of private instelling die aan de gebruikers van haar diensten de mogelijkheid biedt te communiceren met behulp van een computersysteem, en
-
- **ii.**iedere andere instelling die computergegevens verwerkt of opslaat ten behoeve van een zodanige communicatiedienst of van de gebruikers van een zodanige dienst;
-
-
- **d.**"verkeersgegevens", computergegevens die
- –verband houden met een met behulp van een computersysteem gevoerde communicatie, en
-
- –worden voortgebracht door een computersysteem dat een onderdeel vormt van de communicatieketen, en
-
- –de herkomst, de bestemming, de route, de tijd, de datum, de omvang, de duur of de aard van de betrokken dienst aanduiden.

Het onbruikbaar maken, veranderen of anderszins aantasten van gegevens is strafbaar gesteld in de artikelen 350a en 350b Sr.

Onbruikbaar maken, veranderen of aantasten van gegevens

Deze artikelen beschermen het ongestoorde gebruik van computergegevens tegen onder meer onbevoegde verandering of het ontoegankelijk maken van die gegevens .

Het Wetboek van Strafrecht onderscheidt de situatie waarin iemand opzettelijk gegevens onbruikbaar maakt of verandert (art. 350a Sr) van de situatie dat dit niet opzettelijk gebeurt, maar er wel sprake is van schuld (art. 350b Sr).

In de artikelen 350 a en 350 b Sr. zijn twee gedragingen strafbaar gesteld: het aantasten van gegevens (lid 1 en 2) en het ter beschikking stellen en verspreiden van gegevens die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, zoals computervirussen, wormen en andere malware (lid 3).

Artikel 350a: opzet

Op basis van artikel 350a Sr zijn de criteria voor strafbaarstelling van het opzettelijk onbruikbaar maken en veranderen van gegevens:

1. Er is sprake van gegevens.

2. De gegevens zijn via een geautomatiseerd werk opgeslagen, of worden door een computer verwerkt of overgedragen.

3. De gegevens worden opzettelijk en wederrechtelijk veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, of er worden opzettelijk andere gegevens aan toegevoegd.

Naast het opzettelijk veranderen of onbruikbaar maken van gegevens is expliciet strafbaar gesteld het ter beschikking stellen en verspreiden van gegevens die schade aanrichten door zichzelf te vermenigvuldigen. Dit artikel is specifiek gericht op computervirussen en andere vormen van malware.

Voor strafbaarheid is het voldoende dat iemand de malware ter beschikking stelt of verspreidt, ongeacht of de malware ook daadwerkelijk schade aanricht. Merk op dat spyware hier niet onder valt; dergelijke software is niet bestemd om schade in de computer aan te richten. Op spyware is mogelijk wel het eerste lid van art. 350a Sr van toepassing.

Artikel 350b: schuld

Het artikel beschermt niet alleen gegevens die op het moment van handelen van de dader in een geautomatiseerd werk aanwezig zijn (opgeslagen). Ook de gegevens diegedurende de handeling van de dader worden verwerkt of overgedragen (waaronder het verzenden) vallen hieronder.

Gegevens die worden verwerkt of overgedragen zijn bijvoorbeeld gegevens die van een disc naar een beeldscherm, van een computer naar een printer en van een computer naar een andere computer worden overgezet.

Het ‘onbruikbaar maken’ van gegevens kan bijvoorbeeld plaatsvinden door het wijzigen, veranderen, toevoegen, wissen of ontoegankelijk maken van de gegevens, zoals het wijzigen van een toegangscode. Het ontoegankelijk maken kan leiden tot het onbruikbaar maken van gegevens.

Veranderen of wissen van gegevens is een andere vorm van onbruikbaar maken. Ook het toevoegen van gegevens is strafbaar, omdat het de integriteit van de verzamelingcomputergegevens als geheel aantast.

Opzettelijk betekent dat de verdachte:

• de bedoeling moet hebben gehad om gegevens ter

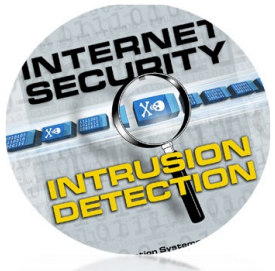
beschikking te stellen en te verspreiden, en

• wist dat de gegevens bestemd zijn om schade aan te

richten.

De criteria voor de ‘culpoze’ (aan schuld te wijten) malwareverspreiding zijn hetzelfde als bij de opzettelijke variant, behalve dat het nu gaat om verwijtbare nalatigheid. Een dader is niet strafbaar in het geval hij de gegevens verspreidt met de bedoeling om de schade, die veroorzaakt werd door een eerder (door een ander) verspreid programma, te beperken (art.350a, lid 4 Sr).

Veranderen, wissen, onbruikbaar of ontoegankelijk maken en/of toevoegen van andere gegevens wordt aangemerkt als schade. Ernstige schade is bijvoorbeeld schade die grote financiële gevolgen heeft en/of schade die moeilijk te herstellen is. De rechtspraak noemt als voorbeeld als (een deel van) een computersysteem van een bedrijf meer dan 12 uur ontoegankelijk is.



Bron: Rijksoverheid

Index

Diefstal of verduistering is het wederrechtelijk wegnemen van een goed zodanig dat de rechtmatige eigenaar er niet meer over kan beschikken.

Diefstal en verduistering cybergerelateerd

Diefstal van gegevens is nu niet als zodanig strafbaar omdat de eigenaar de gegevens feitelijk niet kwijt raakt. Een wezenlijke eigenschap van een 'goed' is dat er niet meer over kan worden beschikt als een ander ermee vandoor gaat. Gegevens of informatie zijn geen goed. Als een persoon een computerbestand kopieert en doorsluist, raakt de eigenaar de gegevens niet kwijt: ze staan nog in de computer. Er is uiteraard wel sprake van diefstal als het fysieke medium waarop de gegevens staan opgeslagen, wordt ontvreemd.

Toch kunnen virtuele objecten onder sommige omstandigheden als goederen gekwalificeerd worden. Bij twee zaken werd succesvol aangevoerd dat ook in de virtuele wereld goederen kunnen voorkomen omdat het om unieke zaken ging.

In de Habbo-hotel en RuneScape-uitspraken beriep de verdediging zich erop dat men slechts informatie ("eentjes en nulletjes") had gekopieerd, wat geen diefstal is. De uitspraak was revolutionair: voor het eerst werd geaccepteerd dat het in deze specifieke gevallen niet alleen ging om gegevens maar dat deze gegevens een uniek identificeerbare virtuele zaak vormden. Als men na het overnemen van gegevens vervolgens deze gegevens verwijdert, is er sprake vernieling van gegevens, wat een aparte handeling is onderartikel 350a Sr.

Het is niet strafbaar om (onrechtmatig verkregen) computergegevens, bijvoorbeeld gegevens afkomstig van gecompromitteerde computers, wachtwoorden of toegangscodes van gebruikers, door te verkopen of te verhandelen (heling).

Onder de huidige wetgeving is het wel verboden om een wachtwoord of andersoortige toegangsinformatie door te sluizen als je daarmee beoogt een misdrijf te plegen (zie voorbereidingshandelingen onder 2.2.3 en 2.2.4 bij artikelen 161sexies en 139d Sr). Personen die wederrechtelijk verkregen digitale informatie zonder een zodanig specifiek oogmerk doorsluizen aan een derde, zijn nu niet strafbaar omdat ook bij heling sprake moet zijn van een 'goed'.

Dit laatste wil men in de nieuwe Wet Computercriminaliteit III aan gaan passen.

Bron: Rijksoverheid

SQL-injectie is een aanvalstechniek waarbij via invoervelden op een website extra of aangepaste instructies worden opgegeven met als doel om de achterliggende database van een website bepaalde instructies te laten uitvoeren.

SQL-injectie

Op deze wijze kan een aanvaller bijvoorbeeld ongeautoriseerd toegang krijgen tot de website, gegevens uit de database opvragen (zoals gebruikersnamen en wachtwoorden) of opdrachten door de website laten uitvoeren. Webapplicaties maken vaak gebruik van databases voor het opslaan en oproepen van allerhande informatie. Structured Query Language (SQL) is de taal die elke database ondersteunt om toegang tot deze informatie mogelijk te maken.

Elke database biedt de mogelijkheid om informatie uit de database op te vragen (SELECT), te verwijderen (DELETE) en te wijzigen (UPDATE). Daarnaast is het uiteraard mogelijk om nieuwe informatie aan de database toe te voegen (INSERT). Deze functionaliteiten vormen de basis van elke database.

Vaak is het mogelijk om via de aanroep van in de database opgeslagen scripts (stored procedures) extra taken te laten uitvoeren zoals het versturen van e-mail. Sommige databases bieden zelfs de mogelijkheid om direct opdrachten en programma's op besturingsniveau aan te roepen.

SQL-injectie wordt veroorzaakt door onvoldoende controles op de invoer van gebruikersdata en onveilige programmeergewoonten. Is de kwetsbaarheid voor SQL-injectie aanwezig, dan kan een aanvaller op het internet SQL-verzoeken die een webapplicatie verstuurt naar de database manipuleren.

Daarbij heeft de aanvaller vaak toegang tot het brede scala aan functionaliteiten dat de database biedt. De gevolgen van deze kwetsbaarheid zijn in grote mate afhankelijk van de programmalogica.

Technische verschijningsvormen en herkenbaarheid

Misbruik via SQL-injectie kan in de logbestanden worden teruggevonden. Dan is te zien of via HTTP GET- of HTTP POST-opdrachten ongewenste informatie wordt meegestuurd.

Kenmerken van pogingen tot SQL-injectie zijn:

• SQL-commando's zoals CAST, DECLARE, SELECT, WHERE

in de communicatie;

• logische instructies in antwoordvelden die worden

aangeboden aan de website

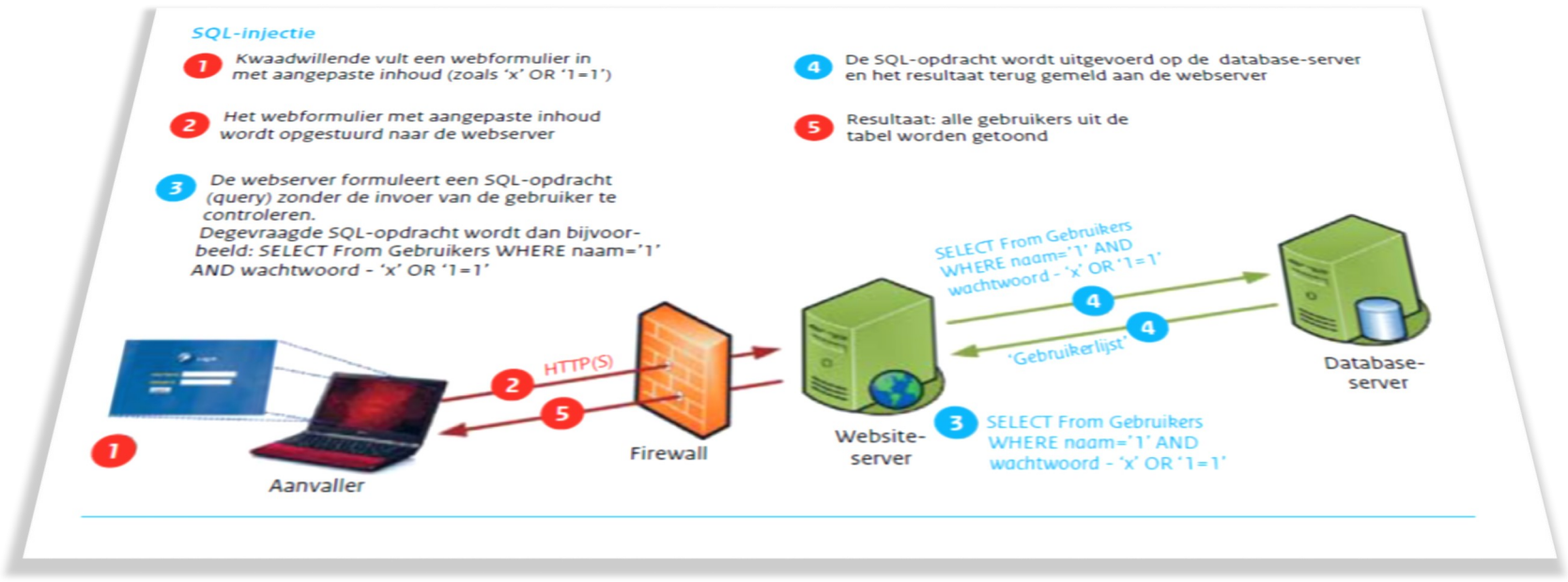
(zoals AND, OR, =, > operators);

• extreem lange waarden van een parameter, getypeerd

door meer dan 500 karakters;

• de aanwezigheid van de keywords IFRAME en SCRIPT SRC

in verschillende velden in de database.



Bron: Rijksoverheid

Index

Benodigde gegevens voor vaststelling Vooral de logbestanden van de webserver, proxyserver en/of databaseserver zijn nodig, met hieruit de relevante gedeelten waarin de HTTP-verzoeken met geïnjecteerde data te vinden zijn. Daarnaast kunnen alle afwijkende gedragingen van de computer een aanwijzing zijn, zoals onbekende meldingen in een firewall/IDS-log, trager wordende prestaties (internetverbinding), foutmeldingen of veelvuldige storingen bij specifieke webapplicaties.

Strafbaarstelling

Wordt er binnengedrongen? Mogelijk. Door SQL-injectie worden onverwachte gegevens ingebracht op of aangeboden aan een webserver. Er worden gegevens verstuurd aan een webserver om te worden verwerkt, om zo zonder toestemming gegevens van de website te ontfutselen. Daarnaast wordt SQL-injectie bijvoorbeeld toegepast om met valse signalen of een technische ingreep de beveiliging van een systeem te omzeilen. Meestal is bij SQL-injectie sprake van een vorm van wederrechtelijk binnendringen.

Wordt stoornis in het geautomatiseerde werk veroorzaakt?

Mogelijk.

Een webserver aangevallen via SQL-injectie kan onbedoeld opdrachten uitvoeren die stoornis veroorzaken in een geautomatiseerd werk, bijvoorbeeld doordat onderliggende procedures (commando's) worden gestart of omdat gegevens worden aangetast.

Worden gegevens veranderd, onbruikbaar gemaakt, vernield of toegevoegd?

Ja.

Door SQL-injectie kunnen gegevens worden verwijderd, gewijzigd of toegevoegd. Het is bijvoorbeeld via SQL-injectie mogelijk om gegevens aan een database toe te voegen, te veranderen of te wissen.

Worden gegevens afgetapt of afgeluisterd?

Nee.

Het is wel mogelijk door SQL-injectie ongeautoriseerd gegevens op te vragen en te kopiëren, zoals toegangsgegevens van gebruikers (overnemen van gegevens).

Strafbaarheid

Het aanbieden van een kwaadaardige code gebeurt bijnaaltijd met opzet, bijvoorbeeld door het aanbieden van een gemanipuleerd HTTP-verzoek aan een website. De dader wil binnendringen, gegevens overnemen of schade als gevolg van vernieling veroorzaken in het computersysteem of de gegevens in het computersysteem aantasten. Als er eerst onrechtmatig gegevens moeten worden toegevoegd aan een database om meer rechten te kunnen krijgenom verdere acties te ondernemen, is artikel 350a lid 1 Srvan toepassing. Hierbij kan tevens sprake zijn van het overnemen van gegevens nadat is binnengedrongen in het geautomatiseerde werk (artikel 138ab lid 2 Sr).

Bron: Rijksoverheid

Index

Stichting Brein heeft officieel toestemming gekregen om ip-adressen van torrentgebruikers te verzamelen: een belangrijke stap in het bestrijden van online piraterij.

Zo verzamelt Brein ip-adressen (en misschien wel die van jou)

Als je veel uploadt, kan je ip-adres in het systeem van Brein terechtkomen. Maar wat betekent dit precies?

Brein-directeur Tim Kuik introduceerde eind vorig jaar een systeem dat ip-adressen (het telefoonnummer van je internetverbinding) verzamelt van mensen die auteursrechtelijk beschermd materiaal op grote schaal uploaden. Dat systeem is vandaag officieel goedgekeurd door de Autoriteit Persoonsgegevens, de privacywaakhond van Nederland. Na die goedkeuring is Brein direct begonnen met het verzamelen van ip-adressen.

1. Wat is uploaden precies?
Als je iets downloadt, haal je bijvoorbeeld een film binnen. Bij het uploaden wordt dit proces omgedraaid: dan verstuur je juist die film. Bij het downloaden via torrents gaat dit proces meestal hand in hand: je downloadt de film en stuurt (stukjes van) deze film direct weer door naar andere mensen die dezelfde film downloaden. Dit is het hele idee achter het torrent-netwerk, waar mensen onderling bestanden uitwisselen.

2. Wanneer ben je een grote uploader?
Dat hangt af van hetgeen dat je downloadt. Stel: je downloadt op illegale wijze een nieuwe game. Als je de game enkel downloadt en vervolgens verwijdert uit het downloadprogramma, dan is de kans klein dat Brein je ip-adres gebruikt. De auteursrechtenwaakhond zegt alleen achter de grote aanbieders aan te gaan, en niet de individuele downloader.

Maar als je de torrent voor een langere tijd in je downloadprogramma aan hebt staan, en zo'n game voor een langere tijd naar andere downloaders verstuurt, kan je ip-adres wel door Brein worden geregistreerd. Je hebt er dan voor een lange periode auteursrechtelijk materiaal gedeeld, en dat maakt je een illegale aanbieder van auteursrechtelijk beschermd materiaal.

3. Komt uploaden ook bij streamen voor, zoals bij Popcorn Time?
Ja. Popcorn Time kan het beste worden gezien als een normaal downloadprogramma voor torrent-bestanden, maar in plaats van te wachten op de download kun je een film of serie direct bekijken.

Het Europees Hof moet zich nog buigen over de kwestie of het 'illegaal streamen' van auteursrechtelijk beschermd materiaal, zoals met Popcorn Time, ook daadwerkelijk onrechtmatig is. Deze uitspraak wordt binnen één tot anderhalf jaar verwacht.

4. Hoe komt Brein aan jouw ip-adres?
Als je iets via het torrent-netwerk downloadt, ben je zichtbaar met jouw ip-adres. Brein heeft een systeem ontwikkeld dat veel torrentwebsites, zoals The Pirate Bay en KickAss Torrents, afspeurt naar illegaal aangeboden materiaal van één van zijn klanten. Dat kunnen films en series zijn, maar Brein vertegenwoordigt ook muzikanten en gameontwikkelaars.

Het systeem kijkt vervolgens naar de ip-adressen die het meeste hebben geüpload. Als hier een Nederlands ip-adres tussen zit, wordt dit adres in het systeem van Brein opgenomen.

5. Je staat met je ip-adres in het systeem van Brein. Wat dan?
Met de ip-adressen die Brein verzamelt, stapt de stichting naar de internetproviders die de ip-adressen hebben uitgegeven. De provider weet wie de rekening betaalt van de internetverbinding die een bepaald ip-adres gebruikt. Maar daar bevindt zich nog een obstakel voor Brein, want de providers staan de NAW-gegevens die bij een ip-adres horen niet vrijwillig af.

Daarom moet Brein eerst naar de rechter stappen, om de providers zo proberen te dwingen om de NAW-gegevens af te staan. De rechter beslist dan of Brein voldoende heeft aangetoond dat de persoon daadwerkelijk inbreuk op het auteursrecht heeft gepleegd. Brein wil de uploader aanspreken op zijn gedrag en een 'schikkingsvoorstel' aanbieden, dat volgens de stichting kan oplopen tot de 12.500 euro.

In een eerdere soortgelijke zaak, waarin Brein bij Ziggo de NAW-gegevens van een illegale aanbieder vorderde, verloor de auteursrechtenclub. Volgens de rechter kon Brein niet voldoende aantonen dat de klant van Ziggo daadwerkelijk inbreuk op de auteursrechten pleegde.

6. Hoe reëel is het dat je een schadeclaim aan je broek krijgt?
De hierboven genoemde zaak laat zien dat het voor Brein best lastig is om de NAW-gegevens van een ip-adres te vorderen. Als de rechter een internetprovider verplicht om de NAW-gegevens af te staan, krijg de inbreukmaker een schadeclaim op de deurmat. Maar dan nog heb je de kans om de claim aan te vechten in de rechtbank.

Er zijn tal van situaties te bedenken waarin de rechter moet beslissen of jij ook daadwerkelijk degene was die de inbreuk heeft gepleegd. Denk bijvoorbeeld aan een studentenhuis, waar meerdere mensen gebruikmaken van één ip-adres, wie is dan de schuldige? Het wordt ook lastig als je een open wifi-netwerk aanbiedt waar mensen gebruik van mogen maken. Of wanneer je je huis verhuurt via Airbnb, en een huurder de inbreuk pleegt. Dat zijn vraagstukken waar een rechter zich over kan buigen.

Maar voordat het zover is, moet Brein eerst bij de provider de NAW-gegevens van zo'n 'grote uploader' vorderen. Het is dan wachten op de volgende rechtszaak tussen Brein en een internetprovider, waarin de rechter mag oordelen of de privacy van de internetgebruiker zwaarder weegt dan de vermeende inbreuk op het auteursrecht.

Bron: RTL-Z

Index

Het is sinds kort mogelijk om jezelf online te identificeren met iDIN, een soort iDeal om je identiteit bij een website te bevestigen. Hoe werkt deze technologie precies?

Zo gaan we ons online identificeren: iDIN

Identiteitsfraude is een groot probleem in Nederland. Mensen kopen bijvoorbeeld op naam van iemand anders spullen, maar laten het wel op hun adres bezorgen. Om identiteitsfraude te bestrijden, introduceert de Betaalvereniging Nederland in samenwerking met de Nederlandse banken een nieuw systeem waarmee je jezelf bij websites kunt identificeren. Het systeem heet iDIN en is deze week in gebruik genomen door de Belastingdienst.

Werkt nauw samen met iDEAL

iDIN maakt het mogelijk dat een website zeker weet dat jij het bent. Handig voor de Belastingdienst, een verzekeringsmaatschappij, zorginstelling of webwinkel. Als je inlogt met iDIN, vertelt je bank aan de betreffende website dat jij het ook daadwerkelijk bent. Een bank is hiertoe in staat omdat het de identiteit van klanten bij het openen van een rekening verifieert.

Het inlogvenster van iDIN lijkt als twee druppels water op die van iDEAL. Dat is niet vreemd, want iDIN maakt gebruik van de technologie achter iDEAL. Daarnaast maakt iDIN het mogelijk om persoonlijke gegevens met een derde partij te delen. Als je met iDIN inlogt bij een webshop, worden - als jij daarmee instemt - bijvoorbeeld je naam en adresgegevens automatisch ingevuld. Zo kun je sneller een product bestellen.

ING en Rabobank doen al mee

Het hele proces wordt uitgevoerd door je bank die je gegevens in kan zien. Het verschilt per website om welke gegevens wordt gevraagd. Een verzekeraar kan bijvoorbeeld om je burgerservicenummer vragen, een webshop waar je bier kunt kopen zou aan de bank kunnen vragen of je ouder bent dan achttien.

Bij beide gevallen geldt opnieuw: je geeft eerst altijd expliciet toestemming voor het delen van je gegevens, en je weet ook altijd welke gegevens je met welke partij deelt. Je financiële gegevens, zoals je saldo, kunnen niet worden opgevraagd.

iDIN is al beschikbaar voor klanten van de ING en Rabobank. De banken ABN Amro, SNS en Triodos volgen in april. In de tweede helft van dit jaar kunnen meer partijen van de dienst gebruikmaken, zodat iDIN ook daadwerkelijk actief in gebruik kan worden genomen.

Bekijk de video

Bron:

Index

Een beveiligde usb-drive of SD-kaart is lastig te wissen. Hier leggen we uit hoe je de beveiliging kunt opheffen zodat je de drive kunt leegmaken of formatteren.

Zo kun je een beveiligde usb-drive wissen

Sommige SD-kaarten of usb-drives bevatten een switch die je kunt omzetten zodat de inhoud niet gewist kan worden. Dit is handig, want zo raak je niet zomaar per ongeluk je bestanden kwijt, maar het kan gebeuren dat Windows de drive of kaart als beveiligd blijft herkennen ook al heb je de switch weer omgezet om de beveiliging op te heffen. Het kan ook dat je SD-kaart of usb-drive helemaal geen switch heeft en toch als beveiligd wordt aangemerkt. Wat kan je dun?

Als een SD-kaart of usb-drive tegen schrijven beveiligd is kun je de inhoud ervan lezen en kopiëren, maar het is niet mogelijk om bestanden te wissen, toe te voegen of de drive te formatteren. Het kan ook dat je de bestanden wel weg lijkt te kunnen gooien, maar als je de drive volgende keer in je computer plugt staan ze er weer.

Je kunt de Register-editor tool van Windows 10 gebruiken om ervoor te zorgen dat Windows de drive niet langer als beveiligd beschouwt. Om dit te doen moet je naar Regeditzoeken en het programma openen. Navigeer naar:

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies

Dubbelklik in het rechterpaneel op de waarde WriteProtect en verander de waarde onderValue van 1 naar 0. Klik op OK om de nieuwe waarde op te slaan.

Als je de drive weer in de computer stopt zal Windows deze als niet beveiligd beschouwen. Je kunt hem dan weer zoals altijd gebruiken.

Als je de registersleutel StorageDevicePolicies niet kunt vinden, kun je er eentje aanmaken.

Om dit te doen moet je met de rechtermuisknop in de map

Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\

in de lege ruimte in het rechterpaneel klikken en New > Key selecteren. Voer de naam StorageDevicePolicies precies zo in, met de hoofdletters op de juiste plaats.

Dubbelklik op de nieuw aangemaakte sleutel, klik opnieuw met de rechtermuisknop in de lege ruimte en kies New > DWORD (32-bit) Value. Geef de waarde de naam WriteProtect en kies als waarde 0. Klik op OK om de wijzigingen op te slaan. Sluit de Register-editor af en start de computer opnieuw op.

Als de oplossing hierboven niet werkt, kun je Opdrachtprompt gebruiken om de beveiliging van de drive op te heffen en alle inhoud te wissen.

Zorg dat je Opdrachtprompt opent als administrator. Dit kun je doen door met de rechtermuisknop op het programma te klikken en Als administrator uitvoeren te kiezen.

Typ het commando diskpart en druk op Enter. Typ vervolgens list disk en druk weer opEnter. Typ select disk X (waarbij X het nummer van je drive is) en druk op Enter. Typ nuattributes disk clear readonly en druk op Enter.

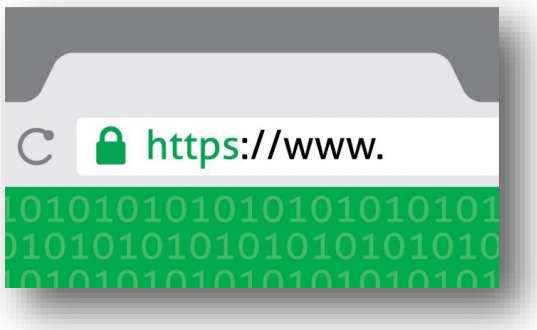
Typ clean en druk op Enter. Typ vervolgens create partition primary en druk op Enter. Typcreate partition primary en druk op Enter. Typ nu format fs=fat32 (je kunt ook format fs=ntfs kiezen als je de drive alleen op Windows computers zult gebruiken) en druk opEnter. Typ exit en druk op Enter, en Opdrachtprompt zal worden afgesloten.

Je drive is nu geformatteerd en Windows zal hem voortaan als onbeveiligd herkennen.

Bron: ComputerTotaal

Index

Het internet een veiliger plek maken. Dat is het doel van de non-profitorganisatie Let's Encrypt, die gratis beveiligde verbindingen voor websites beschikbaar maakt.



Let's Encrypt maakt het internet veiliger (en dat gratis)

In de adresbalk van je browser verschijnt regelmatig een icoon van een slotje. Zo'n slotje betekent dat je veilig met een website communiceert. Dit is bijvoorbeeld belangrijk bij het invullen van je adres- of creditcardgegevens: informatie die alleen de website mag inzien. Het slotje verschijnt bij websites die gebruikmaken van een ssl-certificaat. Normaal gesproken moet je zo'n certificaat kopen, maar Let's Encrypt geeft ze gratis weg.

Let's Encrypt is een zogeheten certificaatautoriteit en geeft sinds december van vorig jaar ssl-certificaten uit aan websites. Deze week is de non profit organisatie het magische getal van één miljoen certificaten gepasseerd. "Dat is nog maar het begin", zegt Josh Aas, de initiatiefnemer van Let's Encrypt. Aas begon zijn loopbaan bij Mozilla, het bedrijf achter de Firefox-browser, en richtte in 2013 de Internet Security Research Group op. Deze non profit organisatie wil de veiligheid van het internet verbeteren, en Let's Encrypt is hun eerste grote project.

Beveiligen en verifiëren van een website
Om het doel van Let's Encrypt goed uit te leggen, is het belangrijk om te weten wat een ssl-certificaat precies doet. Een ssl-certificaat heeft twee functies: het opzetten van een beveiligde verbinding tussen jou en de website, en het verifiëren van de identiteit van de website. Door het beveiligen van de verbinding wordt de connectie tussen jou en de website versleuteld, waardoor anderen niet kunnen zien welke data jij uitwisselt. Dat proces is volgens Aas relatief simpel, de lastigheid zit hem in het verifiëren van de identiteit van een website.

Het verificatieproces wordt in gang gezet zodra je een website met slotje - ook wel via https - bezoekt. Jouw browser bekijkt het certificaat en controleert vervolgens bij een vertrouwde certificaatautoriteit of de website echt is wie hij zegt dat hij is. "Het systeem hierachter is traditioneel gezien vrij complex, waardoor ontwikkelaars hun sites niet beveiligen. Met Let's Encrypt maken we het verificatieproces binnen een beveiligde verbinding veel simpeler", zegt Aas.

Niet meer betalen voor veiligheid
Let's Encrypt is een nieuwe en inmiddels vertrouwde certificaatautoriteit, maar dan zonder winstoogmerk. Andere bekende commerciële certificaatautoriteiten zijn Comodo, Symantec, GoDaddy en GlobalSign, waar je een ssl-certifcaat kunt kopen. De kosten variëren van een tientje tot enkele honderden euro's. Een duurder certificaat bevat bijvoorbeeld ook gegevens over de Kamer van Koophandel-inschrijving van het bedrijf. Let's Encrypt richt zich op de basiscertificaten die alleen de identiteit van de website verifiëren en een beveiligde verbinding opzetten.

"Zonder een certificaat is de communicatie tussen een website en zijn bezoekers voor iedereen in te zien", waarschuwt Aas. "Dat is onacceptabel en het duurt veel te lang om al die niet-https-verbindingen weg te werken." Uit onderzoek van Mozilla blijkt dat zo'n 40 procent van alle websites geen beveiligde verbinding ondersteunt en dat maar 65 procent van alle gevoelige transacties via een beveiligde https-verbinding wordt verwerkt. "In beide gevallen zou dat aantal 100 procent moeten zijn, om de privacy en veiligheid te bieden die mensen verwachten."

Van DirectAdmin tot WordPress
Het is voor gebruikers van een eigen webserver, hetgeen waar een website op draait, mogelijk om Let's Encrypt te installeren en een certificaat aan te vragen. Binnen enkele minuten kun je dan een beveiligde https-verbinding voor je website gebruiken. Het doel van Aas voor dit jaar is om Let's Encrypt om meer systemen beschikbaar te maken, zodat ook mensen zonder eigen server maar wel met een eigen website een ssl-certificaat aan kunnen vragen.

Onder andere CPanel en DirectAdmin, twee diensten om websites mee te beheren, bieden al ondersteuning voor Let's Encrypt. Je kunt dan de betreffende website selecteren en automatisch een certificaat instellen. "Ook de WordPress-community is enthousiast over het ondersteunen van Let's Encrypt", zegt Aas. Dit kan bijvoorbeeld met een plugin die WordPress-gebruikers installeren, waarna ze een gratis ssl-certificaat voor hun website kunnen aanvragen. "Maar ik kan nog niets zeggen over zo'n plugin of de release daarvan."

Waar doen ze het van?
Let's Encrypt wordt gesteund met donaties van grote bedrijven, zoals Mozilla, Google en Facebook. Zij betalen tussen de 350.000 en 150.000 dollar per jaar om Let's Encrypt te steunen. Met de donaties betaalt de non-profit zijn werknemers en de kosten om certificaten uit te delen en een lijst met alle uitgegeven certificaten bij te houden.

"Het is een belangrijke stap voor het internet om het voor websites gemakkelijker te maken een https-verbinding te gebruiken", aldus Alex Stamos, hoofd beveiliging van Facebook. "Daarom is Facebook trots om Let's Encrypt te steunen."

Nederland is vooralsnog maar goed voor een klein deel van het aantal uitgegeven ssl-certificaten. Van de miljoen door Let's Encrypt verstrekte ssl-certificaten zijn er enkele tienduizenden uitgegeven voor websites met een .nl-domeinnaam. Dat aantal moet omhoog, vindt Haas: "Nu het voor iedereen zo simpel is om via Let's Encrypt een certificaat te krijgen, is er geen reden meer om websites niet te beveiligen."

Bron: Let's Encrypt

Index

Als je je online leven sterk wilt beperken, zal je aan de slag moeten om her en der accounts te verwijderen. Dat is echter lang niet zo eenvoudig als het er uit ziet. Soms zelfs onmogelijk.

Je online leven opruimen met Just Delete Me

Stel dat je helemaal klaar bent met een online dienst of service en er graag weg wilt, dan is het nodig om je account te verwijderen. Vaak gebruiken bedrijven zogenaamde dark patterns, een speciale manier van het ontwerpen van de gebruikersinterface, om te voorkomen dat je weggaat. Zo'n ontwerp kan bijvoorbeeld een onlogische en onoverzichtelijke indeling zijn, door gebruik te maken van hoe wij mensen in elkaar zitten.

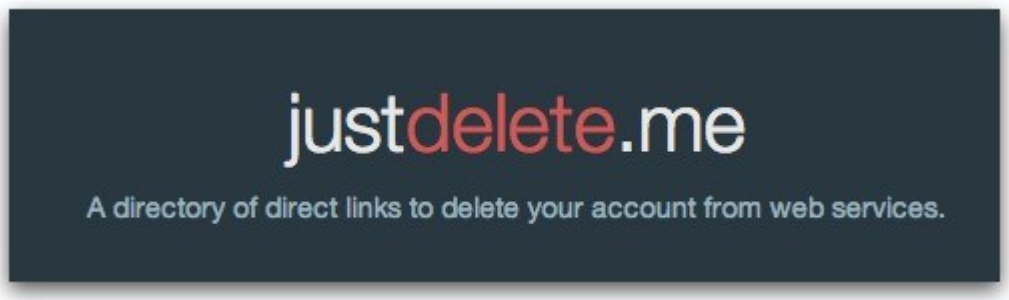
Een dienst die je erbij helpt om je online accounts te verwijderen, is justdelete.me. De website bevat een verzameling van websites met instructies hoe je je account kunt verwijderen, indien dat mogelijk is. Bij elke website is bovendien aangegeven hoe eenvoudig het verwijderen van je account is. Dat is gedaan in de vorm van de kleurcodes groen, geel, rood en zwart, waarbij groen eenvoudig is en zwart letterlijk onmogelijk.

Wil je bijvoorbeeld je Skype-account verwijderen, dan is het nodig om contact op te nemen met de klantenservice van Microsoft. Hetzelfde geldt voor het verwijderen van je Adobe ID. Het verwijderen van je account voor Parkmobile, dat ook in Nederland actief is, wordt door Justdelete.me als lastig bestempeld. Het is hiervoor nodig een e-mail te sturen naar de klantenservice met je naam, mobiele telefoonnummer en kenteken of de laatste vier cijfers van je bankrekeningnummer of creditcard.

Het verwijderen van een Evernote-account is bijvoorbeeld dan weer niet mogelijk. Evernote-accounts kunnen alleen gedeactiveerd worden, maar dan blijft alle data wel gewoon nog aanwezig. Het is dan vereist om handmatig alle notities en persoonlijke informatie te verwijderen, vervolgens al deze gegevens te synchroniseren met de Evernote-servers en dan je account te deactiveren. Alleen zo is het mogelijk enigszins je data van de servers te verwijderen. Andere websites waarvoor er instructies beschikbaar zijn, zijn onder andere WhatsApp, Telegram, TeamViewer, Todoist, Zoho, Wunderlist, Vimeo en Snapchat. Van bijvoorbeeld Wikipedia, Steam, YouTube, PlayStation Network, Netflix, League of Legends en Kik zal je overigens nooit je gegevens kunnen verwijderen.

Die kennis kan ook preventief werken. Als je je wilt registreren op een site waar het lastig, zo niet onmogelijk, is om je gegevens ooit weer te verwijderen, dan is het misschien nodig even twee keer na te denken voordat je je gegevens aan zo'n dienst of website zomaar afgeeft.

Om tijdens het surfen direct in te zien hoe websites omgaan met hun verwijderbeleid, is er voor Justdelete.me een Google Chrome-extensie beschikbaar. Bij het bezoeken van een website die wordt ondersteund verschijnen de instructies om je account te verwijderen automatisch in beeld. Bovendien verschijnt er in de adresbalk direct hoe eenvoudig het is je account te verwijderen, aan de hand van een bolletje met de betreffende kleurcode van die website. Je vindt de Justdelete.me-extensie voor Google Chrome hier.



Bron: PCMweb

Index

Onderzoekers van het Slowaakse anti-virusbedrijf ESET hebben naar eigen zeggen unieke en gevaarlijke usb-malware ontdekt die in staat is om offline computers te infecteren en ontwikkeld is om allerlei gegevens van besmette systemen te stelen.

Unieke usb-malware kan offline computers infecteren

De malware wordt USB Thief genoemd.

Om computers te infecteren maakt USB Thief gebruik van plug-ins of dll-bestanden. Volgens de onderzoekers spelen de malwaremakers hierbij in op de trend dat usb-sticks vaak "draagbare" applicaties bevatten die zonder installatie werken, zoals Firefox, Notepad++ en TrueCrypt. Zodra gebruikers een dergelijke applicatie starten wordt ook de malware in de achtergrond geladen. Het is echter onbekend hoe een besmette usb-stick bij het beoogde doelwit terechtkomt.

Hardware

USB Thief is ook opvallend omdat het alleen op een enkele usb-stick werkt. De malware is zo ontwikkeld dat die niet op andere usb-apparaten dan het originele apparaat kan werken. Voor elk exemplaar is er dan ook een andere usb-stick. Hiervoor maakt USB Thief gebruik van encryptie. De encryptiesleutel is afgeleid van het hardware-id van de usb-stick en bepaalde schijfeigenschappen. Daardoor kan de malware alleen vanaf de betreffende usb-stick worden geladen. Dit maakt het lastiger voor onderzoekers om de malware te analyseren.

Het belemmert echter ook de verspreiding van USB Thief. Aan de andere kant voorkomt het wel dat de malware buiten de aangevallen omgeving terechtkomt, aldus de onderzoekers. Dit was bijvoorbeeld het geval met de Stuxnetworm, die systemen ook via usb-sticks infecteerde. Stuxnet infecteerde echter ook usb-sticks die op de besmette computer werden aangesloten, waardoor de malware zich uiteindelijk buiten de aangevallen omgeving verspreidde.

Onderzoek

Omdat de onderzoekers niet over de besmette usb-sticks beschikten maar alleen de malware-bestanden, besloten ze het hardware-id van het oorspronkelijke usb-apparaat via brute force te achterhalen en gebruikten daarbij veelvoorkomende schijfeigenschappen. Hierdoor kon uiteindelijk de werking van de malware worden achterhaald. USB Thief blijkt alle databestanden op besmette computers te stelen, zoals afbeeldingen en documenten.

Ook verzamelt USB Thief informatie uit het Windowsregister, bestandslijsten van alle harde schijven en informatie die via het programma WinAudit wordt verzameld. Hierbij laat de malware geen enkel spoor achter. "Nadat de usb-stick is verwijderd kan niemand meer zien dat er gegevens zijn gestolen", zegt onderzoeker Tomas Gardon.

Usb-poorten uitschakelen

Om infecties door USB Thief te voorkomen adviseert ESET om usb-poorten uit te schakelen. In het geval dit niet mogelijk is wordt aangeraden om beleid op te stellen voor het gebruik van usb-apparaten en is het raadzaam om het personeel te trainen. "Mensen moeten de risico's kennen van usb-apparaten die van onbetrouwbare bronnen afkomstig zijn. Uit verschillende onderzoeken blijkt dat er een grote kans is dat mensen gevonden usb-sticks in hun computer steken", stelt onderzoeker Peter Stancik.

Bron: Security.nl

Index

Als je een e-mail stuurt, wordt het bericht beveiligd met een technologie die al bijna veertig jaar oud is. Het is daarom tijd om aan een nieuwe technologie te werken, en Google en Microsoft nemen het voortouw.

Google en Microsoft willen jouw e-mails beter beveiligen

Het versturen van een e-mail gebeurt lang niet altijd op een veilige manier. Berichten worden in veel gevallen niet versleuteld en het is voor de verzender niet altijd duidelijk of hij een e-mail naar de juiste persoon stuurt. E-mail kan hierdoor vrij gemakkelijk door een kwaadwillende worden onderschept en ingezien.

Zo werkt de technologie achter een e-mailtje
Om e-mails te versturen gebruiken e-maildiensten de technologie Simple Mail Transfer Protocol (SMTP), dat in de jaren tachtig is ontwikkeld. In 2002 werd deze technologie verbeterd met STARTTLS, dat de inhoud van e-mails tijdens het verzenden versleutelt. Maar STARTTLS wordt nog niet door iedereen gebruikt en beveiligt je niet tegen het onderscheppen van e-mail door een kwaadwillende.

Het onderscheppen gebeurt via een zogeheten man-in-the-middle-aanval, waarbij de kwaadwillende zich voordoet als de ontvanger van een e-mail.

De nieuwe technologie van Google en Microsoft
Google en Microsoft willen een nieuwe technologie introduceren, genaamd Simple Mail Transfer Protocol Strict Transport Security (SMTP STS), waarmee berichten tijdens het verzenden worden versleuteld en de identiteit van de ontvanger wordt geverifieerd.

SMTP STS forceert tijdens het verzenden van een e-mail een versleutelde verbinding, waardoor de inhoud van een e-mail niet voor bijvoorbeeld een internetprovider is in te zien. Daarnaast checkt de technologie de identiteit van de ontvanger. Dit gebeurt bijvoorbeeld door te controleren of je daadwerkelijk communiceert met de servers van Google als je een e-mail naar een Gmail-adres verstuurt - en dat je niet communiceert met de malafide server van een internetcrimineel.

Het voorstel voor SMTP STS te promoveren tot standaard is ingediend bij de Amerikaanse Internet Engineering Task Force, de organisatie die zich bezighoudt met internetstandaarden. Binnen zes maanden reageert de organisatie op het voorstel.

PGP
Bedrijven als Google en Microsoft kunnen hun e-mail nog beter beveiligen, bijvoorbeeld met Pretty Good Privacy (PGP). Met deze technologie wordt de inhoud van een e-mail op een specifieke manier versleuteld waardoor alleen de ontvanger het bericht in kan zien, en bijvoorbeeld niet de e-mailprovider.

Deze krachtige vorm van encryptie voeren bedrijven als Google niet in omdat zij dan niet meer jouw e-mails kunnen scannen en op basis daarvan je gepersonaliseerde advertenties kunnen voorschotelen.

Bron: RTL-Z

Index

Iedereen kent het probleem van virussen, Trojaanse paarden, ransomware en overige vormen van malware. Minder bekend zijn de beweegredenen van malwareontwikkelaars. Wie zijn deze cybercriminelen en waarom steken ze zoveel tijd in het schrijven van kwaadaardige programma's?

Waarom hacken hackers?

Vandaag de dag zijn er maar liefst 500 miljoen unieke malwarescripts bekend bij de gerenommeerde producenten van antivirussoftware. Een duizelingwekkend getal, zeker als je bedenkt dat er iedere maand 14 miljoen geïnfecteerde scripts bij komen. Overigens vormt niet alles een serieuze bedreiging, aangezien een deel is gericht op verouderde besturingssystemen als MS-DOS, Windows 95 en XP. Toch is het einde van cybercriminaliteit lang niet in zicht, gezien het feit dat recente Windows-versies nog altijd een populair doelwit zijn van malwareontwikkelaars. Bovendien duiken er ook voor Android in toenemende mate nieuwe bedreigingen op.

Herkomst digitale boeven

Net als alle reguliere vormen van criminaliteit is cybercrime een wereldwijd probleem en komt het dus overal voor. Veelal blijven de verantwoordelijke personen anoniem omdat ze hiervoor diverse voorzorgsmaatregelen nemen. Er is wel een duidelijke trend zichtbaar. De meeste malware is afkomstig uit Rusland, China, Brazilië en Verenigde Staten. Een verklaring hiervoor is dat het stuk voor stuk technologisch ontwikkelde landen zijn waar veel mensen wonen. Aangezien bepaalde virussen zich specifiek richten op Nederlandse gebruikers, mag je ervan uitgaan dat cybercriminelen ook dichtbij huis te vinden zijn. Kortom, ze zitten overal en kunnen in theorie iedere computer bereiken die is aangesloten op internet.

Beweegredenen malwareontwikkelaars

Interessant is om te weten waarom cybercriminelen op grote schaal veel tijd en geld steken in het ontwikkelen van malware. Volgens Bogdon Botezatu bestaan er hiervoor twee belangrijke redenen. “Allereerst is er natuurlijk een commercieel belang waarbij hackers geld via geïnfecteerde computers stelen. Dat kan door rechtstreeks in te breken op online bankaccounts of het onderscheppen van betaaltransacties. Daarnaast zijn er ook indirecte methoden om mensen geld af te troggelen, door bijvoorbeeld vanaf geïnfecteerde computers honderdduizenden spamberichten te verzenden. Een tweede reden is het zogeheten hacktivisme. Deze mensen zijn het ergens niet mee eens en gebruiken hun computerkennis om een protestactie te starten. Een bekend voorbeeld is het internationale hackerscollectief Anonymous. Zij zetten in een jong verleden via malware DDoS-aanvallen op om in te breken op betaalsystemen en het PlayStation Network. Ook overheden zijn vaak het doelwit van dergelijke aanvallen.”

Minder virussen!

Hoewel malwarebesmetting nog altijd een serieuze bedreiging is voor iedere pc, is het aantal virussen de afgelopen jaren afgenomen. Virussen verspreiden zichzelf als zelfstandige programma’s door bestanden te infecteren, maar malwareontwikkelaars gebruiken tegenwoordig minder vaak deze technologie. Sality en Ramnit zijn momenteel de grootste virusfamilies die in omloop zijn, maar ook die zijn inmiddels flink op leeftijd. Cybercriminelen doen tegenwoordig vaker een beroep op Trojaanse paarden en ransomware. Een Trojaans paard zit meestal in andere software verscholen of bereikt via een e-mailbijlage je pc. Ransomware is een programma dat je pc kaapt, waarbij er voor ontgrendeling meestal losgeld geëist wordt.

Overheid en malware

Ook overheden faciliteren de ontwikkeling van malware. Dat gebeurt zelfs op grote schaal. De reden hiervoor is meestal het beschermen van de staat. Botezatu legt uit: ”Overheden gebruiken malware als cyberwapens om binnen bepaalde organisaties te infiltreren of bepaalde activiteiten te blokkeren. Denk hierbij bijvoorbeeld aan nucleaire systemen, elektrische centrales en verzoersbedrijven van de vijand. Andere overheden gebruiken malware om in het kader van de rechtshandhaving burgers te bespioneren. Onder meer Duitsland maakte zich daar in het verleden schuldig aan”.

Toekomstperspectief

Nog altijd is het relatief eenvoudig om voor Windows-systemen malware te ontwikkelen en dus zijn we voorlopig nog niet af van kwaadwillende cybercriminelen. Botezatu denkt dat malwareontwikkelaars zich in toenemende mate gaan specialiseren op het verspreiden van ransomware. “Ransomware is eigenlijk een programma dat je computer volledig versleutelt. Je kunt nergens meer bij komen, dus het programma gijzelt feitelijk je pc inclusief alle persoonlijke bestanden. Meestal moet de gebruiker een bedrag aan losgeld betalen. Als de bezitter van de pc het verzoek honoreert, wordt er een decryptie-sleutel opgestuurd om het systeem te ontsleutelen. Ik denk dat deze malware-trend in de komende jaren steeds nadrukkelijker in beeld komt, aangezien de verantwoordelijke personen genoeg geld hebben voor de ontwikkeling van kersverse ransomware”.

Bron: Bogdon Botezatu, Bitdefender.

Index

Naast Apple wil het Amerikaanse Ministerie van Justitie nu achter WhatsApp aan. De versleuteling van die app zou namelijk voor problemen zorgen in de opsporing van criminelen.

Hoe veilig is WhatsApp nou eigenlijk?

Hoe zat het ook alweer met de beveiliging van WhatsApp? Hoe veilig en anoniem is 's werelds meest gebruikte chat-app eigenlijk?

Slechte resultaten uit het verleden

WhatsApp heeft in het verleden nogal eens beveiligingsproblemen gehad, inclusief accountkapingen en onveilige opslag van berichten. De overname door Facebook heeft de zorgen om privacy vergroot, waarna veel gebruikers leken over te stappen naar het veiliger geachte Telegram. Die beveiligde open source chat-app gebruikt eigen encryptie, waar experts al zo hun twijfels over hadden. Het versleutelen van informatie is namelijk een complex geheel, waarbij zowel de wiskundige ondergrond voor het versleutelingsalgoritme meespeelt als ook de zorgvuldigheid van de ingebruikname daarvan.

De ingebruikname betreft niet eens de inzet door de daadwerkelijke eindgebruiker, maar de manier waarop versleuteling is doorgevoerd in de software. Zoals dus een app voor beveiligde communicatie. Dit heet in ICT-termen de implementatie. Fouten daarin kunnen de gebruikte encryptie - hoe krachtig die wiskundig gezien ook is - ondermijnen.

Implementatiefouten of -slordigheden hebben eerder al de Amerikaanse inlichtingendienst NSA veel van zijn kraakwerk laten verrichten. Onmogelijk geachte decodering van versleutelde informatie bleek vaak doenbaar via een ‘zijdeur’, niet via het bruut kraken van wiskundig goed onderbouwde encryptie. Zijdeuren bestaan in diverse vormen en maten. Een voorbeeld is de categorie van man-in-the-middle aanvallen zoals diepgaand onderzocht en al vaak gedemonstreerd door de beruchte securityhacker Moxie Marlinspike. Het gevaar van implementatiefouten speelt niet alleen bij relatieve nieuwkomers zoals Telegram, maar ook voor het in 2009 opgerichte WhatsApp. Die chat-app is begin 2014 voor 19 miljard dollar opgekocht door Facebook en heeft later dat jaar end-to-end encryptie ingevoerd. Daarvoor heeft het aangeklopt bij het door Moxie Marlinspike opgerichte Open Whisper Systems, dat open source software voor beveiligde communicatie maakt.

Stapje voor stapje

Whisper is bekend van communicatie-app Signal, die de opvolger is van de beveiligde telefonie-app RedPhone en de beveiligde chat-app Textsecure. WhatsApp heeft laatstgenoemde geïntegreerd, maar eerst alleen in zijn Android-app. Ondersteuning in de iOS-app moet nog volgen. Hierdoor is WhatsApp-communicatie met iPhone-gebruikers dus niet end-to-end beveiligd.

Vóór de invoering van deze begin-tot-eind versleuteling had het bedrijf de mogelijkheid om berichten in te zien wanneer die door zijn servers werden ontvangen en doorgestuurd. WhatsApps servers bewaren namelijk berichten terwijl ze ‘onderweg’ zijn van verzender naar ontvanger. Dit is een tijdelijk bewaren; totdat het bericht bezorgd is. Van een ware back-up is dus geen sprake, daarvoor moet een gebruiker zelf andere middelen aanwenden. Telegram daarentegen is puur een clouddienst en bewaart dus niets lokaal.

Vingers in de dijk

Na de invoering van Whisper Systems’ end-to-end encryptie leek WhatsApp een stuk veiliger. Begin vorig jaar hebben Duitse onderzoekers echter kwetsbaarheden gevonden in deze beveiliging. Concreet: in de implementatie. Het bleek mogelijk berichten te onderscheppen via een zogeheten man-in-the-middle aanval. Het kernprobleem was volgens de onderzoekers dat het niet duidelijk was wannéér WhatsApp-conversaties echt met end-to-end encryptie zijn beveiligd. Sinds deze maand toont de WhatsApp-app een melding dat berichten op deze manier zijn beveiligd.

Toch is het daarmee niet honderd procent gegarandeerd dat WhatsApp volledig veilig is. De chat-app scoort relatief slecht ophet overzicht van de digitale burgerrechtenbeweging EFF. Telegram scoort daar weer beter, hoewel in november expertsopnieuw kritiek hadden op dit WhatsApp-alternatief. Het feit dat het open source is, is geen garantie dat het veilig is. Dit is wel aangetoond door recente grote gaten in bekende open source-producten, waaronder ook juist encryptiesoftware. Er blijft werk aan de winkel, wat ook geldt voor een closed source-product als WhatsApp.

Bron: Security.nl

Index

WhatsApp is een superhandige chat-app op je Android-, iOS- of Windows-smartphone, maar wist je dat er ook een webversie bestaat ?

In 3 stappen WhatsApp op je pc of laptop

Stap 01: Koppelen

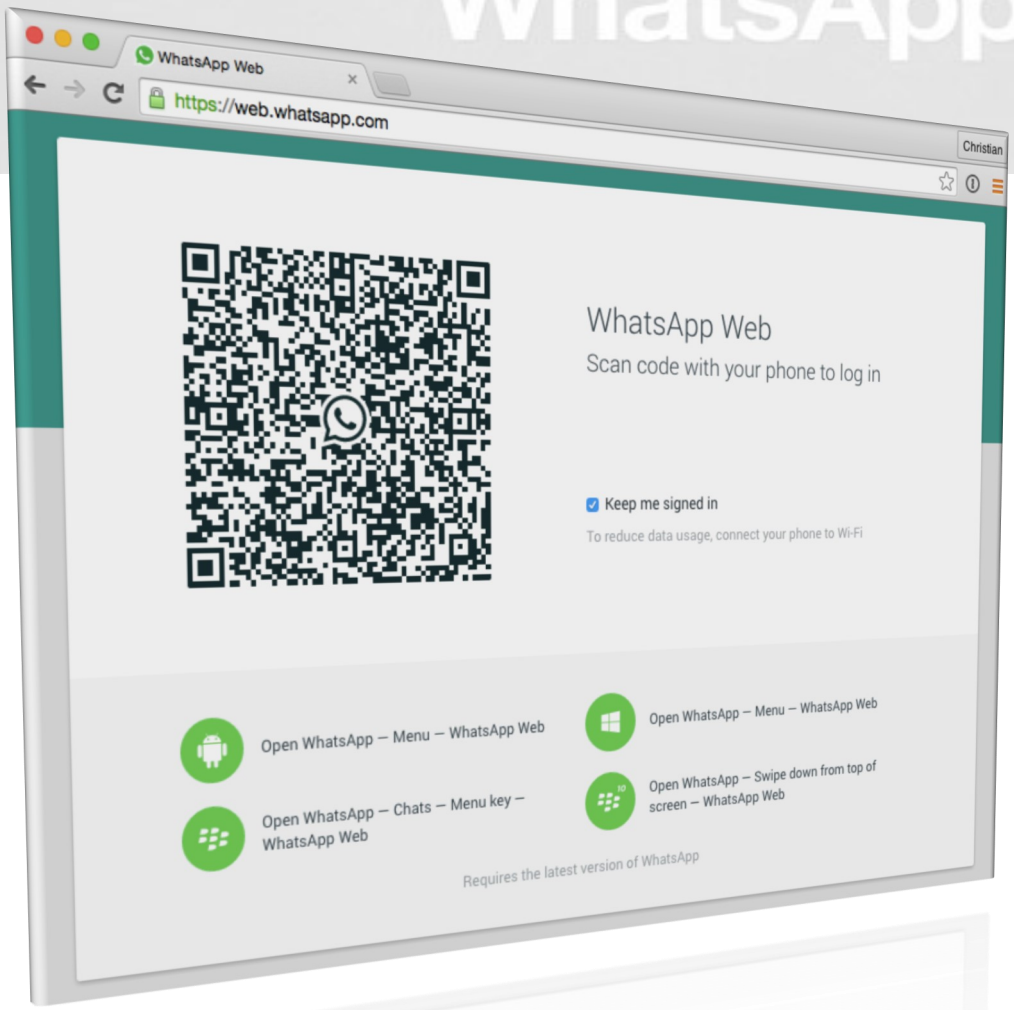
Controleer in eerste instantie of je de meest recente versie van WhatsApp op je telefoon hebt en voer eventueel een update uit. Open vervolgens de browser op je computer en ga naar https://web.whatsapp.com. Let wel, enkel Google Chrome, Firefox en Opera worden momenteel ondersteund. Om je computer en telefoon aan elkaar te koppelen, genereert WhatsApp een QR-code. Gebruik de groene knop Klik om QR-code te herladen om de code te zien. Ga op je telefoon naar Whatsapp / Menu / WhatsApp Web en scan de code. Vervolgens krijg je onmiddellijk een lijst van de laatste gesprekken op je computer te zien.

Stap 02: Versturen via computer

WhatsApp Web maakt verbinding met je telefoon om berichten te synchroniseren. Dat wil zeggen dat je telefoon sowieso in de buurt moet zijn, ingeschakeld moet blijven en verbonden moet zijn met internet via wifi of een mobiel netwerk. In principe werkt WhatsApp Web net zoals de app. In de linkerkolom kies je een gesprek of start je een nieuwe chat. Je kunt gewoonweg typen of gebruikmaken van emoji's. Door toegang te geven tot de microfoon van je computer kun je zelfs gesproken berichten opnemen en versturen. Hiervoor klik je op de knop met het microfoontje rechts onderaan in beeld. Met de knop met de paperclip bovenaan kun je foto's versturen of de webcam starten.

Stap 03: Bureaubladmeldingen

Dankzij WhatsApp Web kun je (ook op het werk!) ongestoord chatten zonder de hele tijd op je telefoon te zitten tokkelen. Als je ook nog bureaubladmeldingen inschakelt, kan jesmartphone zelfs in je tas of broekzak blijven zitten. Kies links bovenaan in de browser voor Bureaubladmeldingen inschakelen en klik in het pop-upvenster op OK, begrepen. Klik vervolgens op Toestaan bovenaan in de balk om meldingen te ontvangen. Je kunt de browser nu gewoon minimaliseren. Zodra er een nieuw bericht is, krijg je een subtiele melding op je bureaublad.



Bron: Security.nl

Index

Onderzoekers van het bedrijf Endgame hebben ontdekt dat kwaadwillenden websites opzetten, waarbij er een letter ontbreekt in het topleveldomein.

Malware verstopt zich achter typefouten in topleveldomein

Daarmee hopen ze mensen te lokken die per ongeluk een typefout in een url typen.

Een van de voorbeelden die wordt genoemd is netflix.om, waarbij er dus een c ontbreekt in het TLD. Er zijn meer dan 300 van dergelijke sites geïdentificeerd, waaronder ook youtube.om en twitter.om.

Endgame ontdekte dat het vrij simpel is om zo'n .om-domein op te zetten. Dat komt mede doordat deze domeinen eigenlijk bedoeld zijn voor sites uit Oman, een land in West-Azië.

Overigens waarschuwen browsers in sommige gevallen al dat er iets mis lijkt, als je zo'n adres intypt. Chrome geeft bijvoorbeeld de melding dat 'een misleidende site is gedetecteerd'. 'Typosquatting' is dan ook niet nieuw, maar nog wel alive and kicking.

Adware

Kom je op zo'n .om-site terecht, dan laten de sites je een Flash Installer downloaden die in werkelijkheid je computer infecteert met adware. Het virus in kwestie is door de onderzoekers tot 'Genieo' gedoopt.

Bron: PCMweb

Index

Cybercriminelen zijn erin geslaagd een designfout in iOS te misbruiken om zonder het medeweten van hun slachtoffers kwaadaardige apps naar iPhones en iPads te downloaden.

Nieuwe malware misbruikt designfout in iOS

De meeste iOS-malware misbruikt enterprisecertificaten alvorens het zichzelf op het toestel van een slachtoffer kan installeren. Palo Alto heeft echter een Trojaans paard, AceDeceiver genaamd, ontdekt dat misbruik maakt van designfouten in het digital rights managementsysteem van Apple. Hierdoor lopen niet alleen gebruikers van jailbroken toestellen, maar eenieder met een iPhone of iPad gevaar.

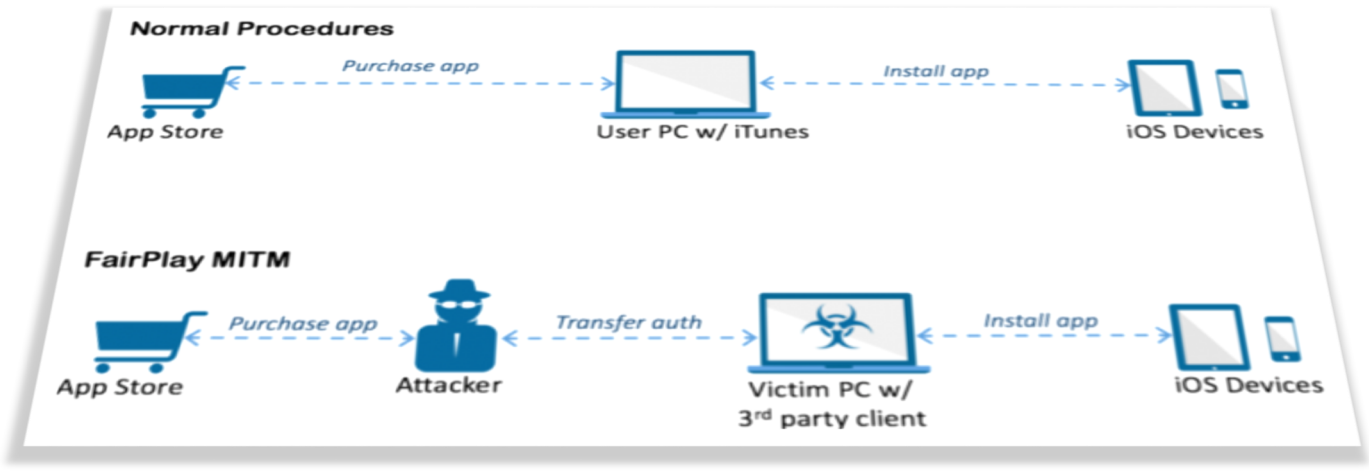
Aisi Helper

AceDeceiver maakt gebruik van de techniek 'FairPlay Man-In-The-Middle (MITM)', welke al sinds 2013 wordt gebruikt voor het verspreiden van gepirateerde apps. Eerst kochten de cybercriminelen een app van de App Store aan om de autorisatiecode te onderscheppen. Hierna hebben ze pc-software ontwikkeld die het gedrag van iTunes-clients nabootst. Met deze software kunnen apps naar iOS-toestellen verbonden met de pc worden gedownload, zonder het medeweten van het slachtoffer.

De software die werd gebruikt voor het uitvoeren van de Fairplay MITM-aanvallen werd Aisi Helper genoemd en deed zich voor als een programma dat diensten verleende voor iOS-toestellen, zoals backups nemen en jailbreaking. Behalve deze onschuldige services houdt de software zich echter eveneens bezig met het installeren van kwaadaardige apps op de toestellen van het slachtoffer. Deze apps verzorgen een connectie met een third party-app store, welke door de cybercriminelen werd beheerd. In deze app store worden bezoekers ertoe aangezet hun Apple ID en paswoord op te geven, met alle gevolgen van dien.

Kwaadaardige apps

Tussen juli 2015 en februari 2016 werden er drie verschillende iOS-apps van de AceDeceiver-familie naar de App Store geüpload, welke zich alle drie voordeden als wallpaper apps. De apps omzeilden meermaals de beveiliging van Apple, maar werden ondertussen door het softwarebedrijf offline gehaald. De cybercriminelen kunnen echter nog steeds nieuwe slachtoffers maken, aangezien de apps slechts eenmalig op de App Store aanwezig hoeven te zijn. De aanvaller heeft immers slechts één kopie van de autorisatie van Apple nodig om zijn apps te verspreiden.



Bron: Security.nl

Index

Terwijl de VS willen dat Apple zijn eigen iPhone kraakt, reageert de rest van de techsector door betere en geavanceerde encryptietechnieken uit te rollen.

Facebook, Google en WhatsApp steunen Apple met veiligere encryptie

Apple ligt onder vuur omdat het weigert z'n eigen iPhones te kraken. De VS willen dat Apple een achterpoortje maakt zodat onderzoekers een iPhone van een terrorist kunnen uitlezen. Apple weigert omdat een dergelijk poortje per definitie op alle iPhones zou werken. Toegeven zou een gevaarlijk precedent betekenen, niet alleen omdat onderzoekers dan veel meer iPhones zouden kunnen binnendringen maar vooral omdat een achterpoortje nooit gesloten blijft: de opzettelijk gemaakte sleutel zou onvermijdelijk uitlekken.

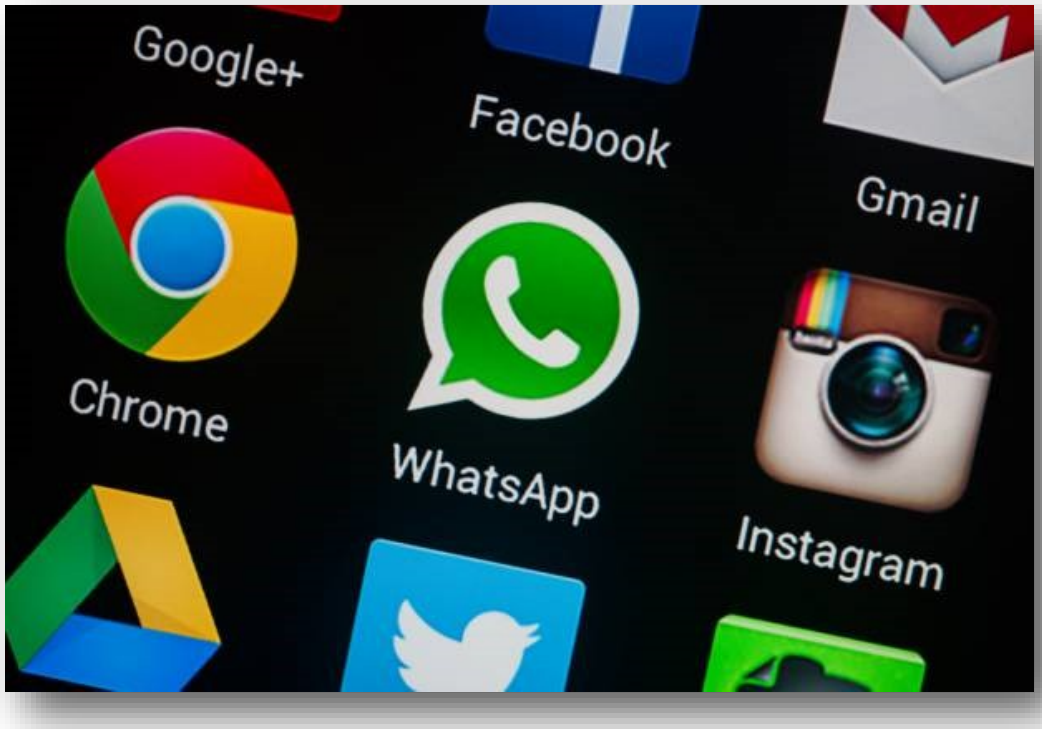
Zowat de hele technologiesector schaart zich achter de redenering van Apple. Onder andere Google, WhatsApp en Facebook dragen beveiliging naar eigen zeggen hoog in het vaandel. Ze spraken al openlijk hun steun uit voor Apple en lijken dat verbale hart onder de riem nu ook om te zetten naar daden.

The Guardian vernam uit goede bron dat zowel Facebook en WhatsApp als Google werken aan nieuwe en betere encryptiemethodes. Daarmee beveiligen ze jouw en mijn communicatie maar dus ook die van terroristen. WhatsApp zelf is al erg veilig voor wie één op één berichtjes stuurt. Die berichten zijn zodanig versleuteld dat zelfs WhatsApp zelf er niet aan kan. De dienst wil diezelfde encryptie nu uitrollen naar groepsgesprekken en telefoongesprekken.

Facebook van zijn kant wil een gelijkaardige beveiliging inbouwen in zijn berichtendienst. Moeilijk kan dat niet zijn: WhatsApp is eigendom van Facebook. Snapchat, vooral populair bij jongeren, wil dan weer een eigen beveiligde berichtendienst lanceren. Google kijkt ten slotte naar manieren om zijn diensten over de ganse lijn beter te beveiligen. De zoekgigant werkte enige tijd geleden al aan End-to-End, een maildienst die waterdicht moet zijn. De Guardian weet nu dat er binnen Google onderzocht wordt of de technologie achter dat project kan dienen voor de beveiliging van andere aspecten van het Google-portfolio,

Het is niet de eerste keer dat grote namen zich achter encryptie zetten. Bedrijven hopen dat potentiele klanten vandaag klaar zijn om eventueel een centje extra te betalen voor een app of dienst die hun bedrijfsgeheimen vrijwaart. WhatsApp van zijn kant spreekt niet te luid over zijn beveiligingsfuncties ook al is de dienst nu al één van de veiligste ter wereld. Stichter Jan Koum, die opgroeide in Oekraïne toen dat land nog (helemaal) deel was van de Sovjet Unie, vindt beveiliging geen feature maar een minimumvereiste.

De grote namen in de technologiewereld lijken zich dus lijnrecht tegen overheid en justitie te keren. In de VS woedt het debat het hardst, maar overal ter wereld klagen beveiligingsdiensten dat nieuwe technologieën hun werk moeilijk maken. Uiteindelijk gaat het debat niet over of Apple al dan niet toegeeft. Het probleem is veel ruimer en heeft zelfs repercussies buiten de technologiewereld: hoeveel privacy ben jij bereid om op te geven in ruil voor meer veiligheid? En in welke mate betrouw je diensten zoals de NSA om daar op een verantwoorde manier mee om te gaan?



Bron: ZDnet

Index

Smartphones lijken er steeds op de verkeerde momenten de brui aan te geven. Jammer genoeg zal het regelmatig sluiten van ongebruikte apps dit probleem niet van de baan helpen.

Apps sluiten om batterij te sparen heeft averechts effect

Wie zijn apps na gebruik volledig sluit om de batterij van zijn smartphone te sparen, zal bedrogen uitkomen. Zowel Apple als Google hebben recentelijk bevestigd dat dit proces geen invloed heeft op de tijd dat je batterij meegaat. Volgens Hiroshi Lockheimer van Android kan het sluiten van apps zelfs de levensduur van je batterij verslechteren.

De reden waarom het sluiten van apps geen effect heeft op de batterij van je smartphone, is omdat een app verschillende toestanden kan hebben. In iOS kan een app in de eerste plaats actief of inactief zijn. Verder kan een app op de achtergrond werken en heeft een app een overgangsfase. Tijdens deze fase is de app zichtbaar op het scherm, maar doet het niets. Dit gebeurt bijvoorbeeld wanneer je van scherm aan het wisselen bent.

Als laatste is er een ‘Suspended’ status. Een app is in deze toestand wanneer het niet op je scherm zichtbaar is en ook niets in de achtergrond doet. Het programma zal slechts ruimte innemen in het geheugen van je smartphone, maar zal geen invloed hebben op je batterij.

Bovendien hebben zowel iOS als Android algoritmes die aan geheugenmanagement doen. Wanneer het algoritme merkt dat een suspended app gedurende enige tijd niet is gebruikt, of dat een app erg veel geheugen en stroom verbruikt, zal het de app automatisch sluiten. Wanneer je een app uit geheugen opent, zal deze echter een stuk sneller starten. De app moet immers niet volledig worden heropgestart.

Bron: PCMweb

Index

Kaspersky Cleaner is misschien wel het eenvoudigste gratis schoonmaakprogramma op het net. De tool brengt je computer in tiptop vorm in letterlijk twee muisklikken.

Verlos je pc van overtolligheden

Na verloop van tijd vult je pc zich onvermijdelijk op met allerlei overtolligheden: je prullenbak puilt uit, tijdelijke bestanden blijken toch niet zo tijdelijk en je laat allerlei sporen na die je misschien liever 's opgeruimd zag: cookies, cachebestanden, recente documenten, logs, enz. Nu kun je die augiasstal wel manueel opruimen, maar Kaspersky Cleaner doet dat net zo lief voor jou.

Comfort

Bij Kaspersky Cleaner is alles gericht op gebruikscomfort. Met letterlijk twee muisklikken (één op Start scan en één op Fix) laat je de tool naar overbodige bestanden en naar systeeminstellingen speuren die het niet zo goed begrepen hebben op je privacy én maak je daar meteen komaf mee.

Het gaat heel concreet over de volgende items: System Cleanup (leegmaken van caches, tijdelijke bestanden, lijst van recente documenten, prullenmand en installatielogs; circa 35 items), System Settings (bestandsassociaties herstellen, bepaalde applicatie-instellingen, enz.; circa 75 items), Private Browsing (cache clearing, Windows 10 privacy-instellingen, Windows logging; circa 10 items), Remove activity traces (zoekgeschiedenis opschonen, cookies verwijderen, TEMP-map en Windows logs leegmaken; circa 20 items).

Selectief schoonmaken

Je hoeft gelukkig niet zonder meer alle suggesties van Kaspersky Cleaner te accepteren. Je kunt namelijk doorklikken naar elke rubriek en zelf aangeven welke items de tool effectief mag aanpakken. Jammer wel dat je over deze items geen verdere informatie krijgt, ook niet via tooltips.

Na afloop van de opschoonronde – die je overigens ook altijd kunt onderbreken – kun je nog een detailoverzicht van de uitgevoerde operaties opvragen, waarna je wellicht wordt gevraagd je systeem even te herstarten om alle uitgevoerde wijzigingen effectief te kunnen doorvoeren.

Gebruikersvriendelijker dan Kaspersky Cleaner kun je het nauwelijks verwachten, maar het is duidelijk dat dit programma vooral toch op de beginnende gebruiker (of de gebruiker met weinig zin of tijd) mikt.

(download: klik start scan)

Bron: Kaspersky.nl

Index

Snapshots

Omdat persoonsgegevens niet meer zo interessant zijn, proberen cybercriminelen nu met een DDoS-gijzeling geld te verdienen. Bij zo'n gijzeling wordt een site net zo lang aangevallen of versleuteld totdat de eigenaar losgeld betaalt. Beveiligers van Kaspersky zagen eind 2015 dat een bepaalde site maar liefst vijftien dagen lang werd aangevallen. De nieuwe methode is een gevolg van de 'gekelderde' prijzen voor data.

———————————————————-

Om de effectiviteit van virusscanners buiten een testomgeving om te testen voert het Oostenrijkse testlab AV-Comparatives elke maand een "real-world protection test" uit, waarbij anti-virusprogramma's voor consumenten met echte besmette links en drive-by downloads op internet worden getest. Op deze manier kan worden gekeken hoe beveiligingsproducten presteren met dreigingen waar gebruikers echt mee te maken hebben. Voor de test van februari werd er met 394 besmette links gewerkt. F-Secure, Kaspersky Lab en Trend Micro weten 100% van de malware te detecteren. Microsoft Security Essentials eindigt met een score van zo'n 92% onderaan. Naast de detectie van malware werd er ook naar 'false positives' gekeken, het onterecht alarm slaan bij schone bestanden. Trend Micro zet hierbij de slechtste prestaties neer en gaat 13 keer in de fout, gevolgd door BullGuard met 11 onterechte waarschuwingen. Van de drie virusscanners die 100% van de malware detecteerden maakt alleen Kaspersky Lab geen fout als het om false positives gaat. AV-Comparatives zal uiteindelijk de prestaties van verschillende maanden bij elkaar nemen om zo tot een eindoordeel te komen, aangezien de prestaties van anti-virusprogramma's per maand kunnen verschillen.

——————————————————

Er is een daling van het aantal geregistreerde misdrijfzaken, maar veel vormen van criminaliteit zijn minder zichtbaar geworden, met name op het internet, aldus Marc van Nimwegen, hoofdofficier van het parket in Rotterdam. Van Nimwegen laat dit weten over de cijfers van het afgelopen jaar van het OM in Rotterdam. "Het internet heeft ongekende communicatiemogelijkheden geopend, maar ook ongekende mogelijkheden gecreëerd voor allerlei soorten van criminaliteit", aldus het Openbaar Ministerie in het jaarrapport . Het parket Rotterdam heeft vorig jaar meerdere strafrechtelijke onderzoeken naar cybercriminaliteit gestart of afgerond. Het parket had de doelstelling 23 cybercrime-onderzoeken te doen. "Die hoeveelheid zaken hebben we, mede door vergrote inzet van de politie, gehaald." Volgens het OM wordt het op het oog geringe aantal verklaard door de strenge officiële definitie van cybercrime: criminaliteit gericht tegen de computerapparatuur. Criminaliteit die wordt gepleegd met behulp van computers, zoals internetoplichting, valt hier buiten. "Omdat deze vorm van criminaliteit meestal internationaal georganiseerd is, is het erg lastig om de daadwerkelijke plegers van de cybercrime op te sporen en te vervolgen." Voor dit jaar is het de bedoeling tenminste 25 strafrechtelijke onderzoeken uit te voeren. Ook zal er speciale aandacht komen voor kwetsbare groepen op het gebied van cybercriminaliteit, zoals ouderen. Er lopen op dit moment onderzoeken naar onder meer het 'mijnen' van bitcoins met behulp van gestolen stroom, het uitvoeren van DDoS-aanvallen op een gemeente en voor hacking.

——————————————————

Cybercriminelen verdienen momenteel goed hun brood met ransomware. De geniepige malware versleutelt alle documenten op een systeem, waarna het slachtoffer wordt gechanteerd tot het betalen van losgeld. Beveiligingsspecialisten hebben gelukkig manieren gevonden om bepaalde ransomware te kraken en de malware te detecteren alvorens het kattenkwaad kan uithalen.

Jammer genoeg heeft dit in het geval van TeslaCrypt net averechts effect gehad. De cybercriminelen die achter de kwaadaardige software zitten, hebben hun ransomware namelijk van een update voorzien, waardoor deze onkraakbaar is geworden. Wie getroffen wordt door TeslaCrypt zal hierdoor niet anders kunnen dan het losgeld te betalen of voorgoed dag te zeggen tegen zijn kostbare documenten.

De vorige versie van TeslaCrypt bevatte een zwakte in de manier waarop de sleutel werd bewaard. Hierdoor slaagden onderzoekers erin een tool te ontwikkelen, waarmee een slachtoffer zijn bestanden gratis kon decrypteren. Voortaan wordt de sleutel echter lokaal gegenereerd, waarna deze onmiddellijk naar de cybercriminelen wordt doorgestuurd en verwijderd van het slachtoffer zijn pc. Hierdoor is het onmogelijk geworden de sleutel te achterhalen met een tool.

——————————————————

Het vergt wat tijd en handigheid met computers, schrijft Het Parool maar 'iedereen kan online drugs kopen'. Niet alleen middelen die niet onder de Opiumwet vallen: de krant kocht online 4-fa en synthetische weet, gewoon via google gevonden, via iDeal betaald en per post thuisbezorgd. Maar ook illegale middelen als coke en xtc: te koop op het dark web, met een tor-browser en wat bitcoins. Onderzoekers van het Trimbos-instituut signaleren twee trends: behalve nieuwe middelen die de Opiumwet omzeilen, de groeiende handel via internet. Onbekend is het aandeel van internet in de drugshandel. Volgens Trimbos-onderzoeker Daan van der Gouwe gaat het in Nederland om vijf tot tien procent. 'Dat aandeel zal stijgen, want internethandel biedt consumenten voordelen. De pakkans is klein, je ontmoet geen agressieve dealers, je kunt prijzen vergelijken en je kunt via recensies achterhalen wie betrouwbaar is'. Het ergste wat je kunt gebeuren, zegt Van der Gouwe, is dat je je geld kwijt bent. 'Maar dan schrijf je een slechte recensie. Op de onlinemarkt is de klant koning, op de fysieke markt is het andersom'. Op internet zou de kwaliteit van de drugs beter zijn dan op straat en de prijs vaak lager. Het oprollen van Silk Road, in 2013, heeft niet veel veranderd: een paar arrestaties maar vooral veel nieuwe sites. 'Het is ondoenlijk alle sites te verbieden. Er is vraag naar drugs en dus ook aanbod'.

Index

Cops in Cyberspace

Hoe de politie Amsterdam facebook inzet, met een klikbare advertentie, is volstrekt veilig. Een politiewoordvoerster zegt dat mensen die informatie willen geven, niet bang hoeven te zijn dat deze informatie bij kwaadwillenden terecht komt. Onduidelijk is hoe groot het bereik van de advertentie is. ‘Wij kunnen uiteindelijk ook niet controleren hoeveel tips wij dankzij facebook hebben gekregen’. Ze benadrukt dat het vanwege de privacy niet te achterhalen is wie er reageert. ‘Wij zitten nergens aan, alles gaat via facebook zelf’. De advertentie wordt alleen getoond aan facebookgebruikers die in de buurt wonen van de plaatsen delict, de twee plekken waar de uitgebrande auto’s stonden én natuurlijk de plek waar ‘het hoofd’ lag.

———————————————————-

De politie is bezig met het opzetten van een database met de locaties van particuliere beveiligingscamera's. Steeds meer particulieren gebruiken camera's om hun eigendommen te beveiligen. De politie maakt naar eigen zeggen in haar dagelijkse werk veel gebruik van deze camerabeelden. Om te weten waar de beveiligingscamera’s zich bevinden en wat zij 'zien', alsmede wat de beeldkwaliteit is, is de politie het project 'Camera in Beeld' gestart. Wanneer er bijvoorbeeld een overval, straatroof of een inbraak is geweest, kan de politie op een interactieve plattegrond zien of er camerabeelden van het incident zijn. Als dat zo is, neemt de politie contact op met de eigenaar van de betreffende camera. In dit geval zullen de beelden volgens de politie altijd met een machtiging van het Openbaar Ministerie worden gevorderd. De beelden kunnen vervolgens als bewijs worden gebruikt. De politie kan niet met de camera's meekijken en de gegevens van mensen die aan het project meewerken zijn alleen voor politiemedewerkers inzichtelijk.

———————————————————-

Waar de misdaadcijfers ‘in real life’ al jarenlang dalen, gebeurt er online steeds meer ‘waar de politie maar moeilijk zicht op krijgt’. Het OM Rotterdam meldt in het jaarbericht over 2015 dat veel vormen van criminaliteit, ‘met name op het internet’, minder zichtbaar en grijpbaar zijn geworden. ‘Er groeit een nieuwe generatie op die van nature de weg weet in cyberspace; sommigen zoeken bij uitstek de slinkse wegen’, aldus hoofdofficier van justitie Marc van Nimwegen.

———————————————————

De relatie tussen politie en Whatsapp is vanaf het begin een lastige geweest. Het succes van de vele honderden, zo niet duizenden Whatsapp -groepen in wijken en buurten, is overduidelijk. Maar hoe agenten die app moeten gebruiken? In de week dat wijkagenten het advies kregen vooral met de beheerders van de groepen in contact te blijven (en niet in de groepen zelf mee te doen), werd in de eenheid Zeeland-West -Brabant het ‘Politie WhatsApp’ nummer 06-52528336 geopend. Het gaat om een landelijke proef, in de regio weliswaar, om via WhatsApp vragen te stellen of meldingen te doen. Als de proef, die tot eind juni duurt, goed loopt, wordt het mogelijk een landelijk nummer. Sectorhoofd Wiebe Leverman van het Regionale Service Centrum (RSC) in Roosendaal ziet twee voordelen: ‘het is goed voor de veiligheid en het is een snelle, laagdrempelige manier om met ons in contact te komen’. Appjes naar het nummer worden gelezen door iemand op het RSC, die direct kan reageren of andere actie kan ondernemen. De berichtjes worden dagelijks uitgelezen tussen 07 en 22 uur.

———————————————————

In samenwerking met de National Crime Agency heeft de Nederlandse politie drie mannen aangehouden voor het witwassen van bitcoins. De hoofdverdachte is een Brit (36, uit Amsterdam). Hij zou de bitcoins van criminelen hebben gekregen. Met hulp van geldezels zou hij deze hebben omgezet in contact geld, tegen een flinke commissie. Zulke ‘exchangers’ worden tegenwoording vaker ingezet omdat ‘normale’ manieren van bitcoins cashen traceerbaar kunnen zijn. In deze zaak zou de verdachte miljoenen hebben verdiend. ´Op één rekening alleen al werd in zeven maanden tijd negen miljoen euro gestort’, zegt THTC-chef Gert Ras. Bij zoeking werd 90 mille in contacten, een boot en een dure auto in beslag genomen.

———————————————————

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

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

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