Mijn geeltjes ? Kijk op compubuy.jouwpagina.nl

Februari—Maart 2015

JAARGANG 4

Secure Computing

In dit nummer oa:

Veel lees(r)plezier

(NB: met Ctrl+ scrolwieltje kunt u de pagina vergroten en verkleinen. U kunt dus zelf uw leesbaar formaat kiezen.)

W.Bosgra Taakaccenthouder Digitale Criminaliteit Basisteam Enschede

Snel index

Klik op een link voor snelle toegang tot het artikel.

Om terug te keren naar de snelindex klikt u onderaan de pagina op Index

Bronnen:

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

Identiteitsraude: artikel 231b Wetboek van Strafrecht

Definitie WODC : "Identiteitsfraude is het opzettelijk en wederrechtelijk of zonder toestemming verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedrahing of met de intentie om daarmee wederrechtelijke gedraging te begaan"

Uit ervaring van slachtoffers blijkt dat het soms lastig is daadwerkelijk aangifte te kunnen doen. Soms wordt deze vorm van criminaliteit niet als zodanig herkend. Soms speelt de ID-fraude zich af in het civiele gebied bijvoorbeeld tussen koper en verkoper.

Het artikel 231b Wetboek van Strafecht biedt uitkomst en de grondslag voor het opnemen van een aangifte als iemand aangifte komt doen omdat zijn identificerende gegevens zijn misbruikt en daardoor nadeel heeft geleden.

De verschijningsvormen van identiteitsfraude zijn divers:

-**overname van identiteitsgegevens**

Het overnemen en misbruiken van iemands identiteitsgegevens, zonder toestemming van de persoon. De fraudeur weet andermans identiteitsgegevens frauduleus te bemachtigen en lift vervolgens onrechtmatig op deze identiteit mee.

-**identiteitsdelegatie**

Medegebruik maken van iemands identiteit, met toestemming van die persoon. Bijv. iemand inschakelen die voor jouw een examen aflegt.

-**identiteitsruil**

Gebruik maken van de identiteit van een ander met toestemming van elkaar. Er is sprake van identiteitsruil als persoon A zich geheel kan uitgeven voor persoon B, omdat A alle identificerende gegevens van B gebruikt. Persoon B gaat hierbij als persoon A door het leven.

-**identiteitscreatie**

Het creëren van een fictieve identiteit, al dan niet met gedeeltelijke identiteitsgegevens van bestaande personen.

Artikel 231b

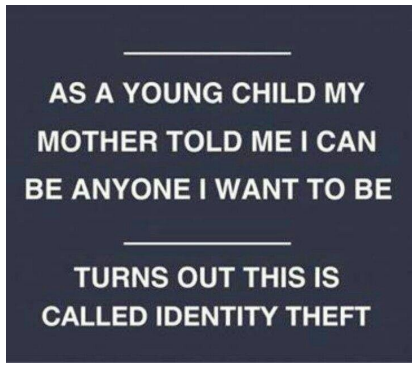
Hij die opzettelijk en wederrechtelijk identificerende persoonsgegevens, niet zijnde biometrische persoonsgegevens, van een ander gebruikt met het oogmerk om zijn identiteit te verhelen of de identiteit van de ander te verhelen of misbruiken, waardoor uit dat gebruik enig nadeel kan ontstaan, wordt gestraft met een gevangenisstraf van ten hoogste vijf jaren of geldboete van de vijfde categorie.

Identificerende gegevens is veel omvattend.

Bijv.: naam, adres, emailadres, bijnaam, artiestennaam enz.

Gebruik dit artikel dus bijvoorbeeld bij het op andermans naam bestellen van goederen, nepaccounts aanmaken op Facebook enz.

Uiteraard kan dit samen gaan met valsheid in geschrifte en oplichting.



Index

Bron:

CBP richt zich dit jaar op profiling en persoonsgegevens

Het College bescherming persoonsgegevens (CBP) gaat zich dit jaar op verschillende onderwerpen richten. Het gaat om profiling en de beveiliging van persoonsgegevens, alsmede het gebruik van dit soort data door overheden.

COLLEGE
BESCHERMING
PERSOONSGEGEVENS

Volgens het CBP worden via digitale apparatuur zoals smartphones, smartwatches, smarttelevisies en smartmeters voortdurend grote hoeveelheden gegevens vastgelegd over het gedrag van mensen. Bijvoorbeeld over hun locatie en hun surf- en kijkgedrag. Op basis van al die gegevens kunnen organisaties mensen indelen in profielen en anders behandelen dan anderen. Het CBP richt zich dit jaar vooral op de naleving van de eis dat mensen goed worden geïnformeerd. Ook kijkt de toezichthouder of op de juiste wijze toestemming is gevraagd voor het gebruik van hun gegevens.

Cameratoezicht

Een ander onderwerp dat aan bod zal komen is cameratoezicht in het lokale domein. Lokale overheden maken veel gebruik van cameratoezicht en passen hierbij nieuwe technieken toe. Zo zetten zij steeds vaker 'slimme' camera's en drones in om de openbare orde te bewaken. Bovendien is door een nieuw wetsvoorstel ook flexibel (mobiel) cameratoezicht in de openbare ruimte mogelijk. Deze nieuwe toepassingen van cameratoezicht zijn volgens het CBP niet altijd even zichtbaar, waardoor het des te belangrijker is dat mensen goed worden geïnformeerd op welke plaatsen er cameratoezicht is.

Verder zal er uitgebreid naar het gebruik en de beveiliging van persoonsgegevens worden gekeken. De privacywaakhond stelt dat de wijdverbreide toepassing van ICT en de omvang van de gegevensbestanden ervoor zorgen dat de impact van onvoldoende beveiliging van gegevens sterk is toegenomen. Het CBP publiceerde eerder al richtsnoeren voor de beveiliging van persoonsgegevens.

In 2015 treedt naar verwachting de meldplicht datalekken in werking. Organisaties worden dan verplicht om inbreuken op de beveiliging die leiden tot diefstal, verlies of misbruik van persoonsgegevens te melden. Dit moet aan de toezichthouder worden gemeld en in veel gevallen ook aan mensen van wie de gegevens zijn.

Het College bescherming persoonsgegevens (CBP) ziet er op toe dat persoonsgegevens zorgvuldig worden gebruikt en beveiligd en dat uw privacy ook in de toekomst gewaarborgd blijft.

Index

Bron:

42 privégegevens die van jou worden verzameld

De Europese Commissie wil 42 persoonlijke details van je weten als je een vliegtuig boekt voor een interne vlucht op ons continent. Die data worden vervolgens vijf jaar opgeslagen in een centrale database.

Waarom is dat? Nou, terrorisme en zo. Niet dat ooit is bewezen dat het massaal vergaren en opslaan van data van alle burgers iets heeft uitgehaald in de strijd tegen terrorisme, maar elke maatregel bekt zo lekker als daadkrachtig bestuur.

Maar welke data wordt dan opgeslagen?

Je paspoortnummer

Welk land je paspoort heeft uitgegeven

Wanneer je paspoort verloopt

Je doopnamen

Je achternaam

Je geslacht

Je geboortedatum

Je nationaliteit

Een zogeheten passenger name record locator code (code voor PNR-opslag)

Datum van ticketreservering

De data waarop je geboekte vlucht(en) gaat/ gaan

Je volledige naam

Andere namen die elektronisch verbonden zijn aan je naam

Je adres

Alle vormen van betaalinformatie

Het adres dat gebruikt wordt bij het bestellen/ betalen

Opgegeven telefoonnummers/ contactinformatie

Alle reisplannen voor dit specifieke PNR

Frequent Flyer-informatie

Reisbureau

Reisagent

Deelcode voor PNR-informatie

Reisstatus van de passagier

Op te delen PNR-informatie

E-mailadres

Informatie uit het ticketsysteem

Algemene opmerkingen

Ticketnummer

Stoelnummer

Datum waarop ticket is uitgegeven

Je no-show-verleden

De gegevens van je kofferlabel

Je go-show-verleden

Andere service-gerelateerde informatie

Speciale verzoeken, zoals voedselvoorkeuren

Informatie over waar deze informatie vandaan komt

Alle historische wijzigingen in deze PNR-data

Aantal reizigers in dit specifieke PNR-record

Stoelinformatie

Enkele reis-informatie

Alle API-systeeminformatie

De software die gebruikt is om de ticket aan te maken

Veel van de data heeft een zeer hoog "aha, dat is herkenbaar"-gehalte. Daarnaast is er een aantal technische data, bedoeld voor gebruikers van het PNR-systeem. PNR staat voor Passenger Name Records, een systeem dat al jaren wordt gebruikt door vliegmaatschappijen. In het rijtje komt verder de afkorting API voor, dat staat voor Advance Passanger Information en dat gebruikt wordt door vooral de Amerikanen om vooraf al te weten wie er aan komt vliegen.

Sommige specifieke punten zijn minder duidelijk: wat wordt er bedoeld met algemene opmerkingen (27) bijvoorbeeld. Je go-show-verleden lijkt het aantal malen dat je daadwerkelijk op komt dagen bij de gate.

Het plan om deze data op te slaan en onderling te delen, wordt dit jaar door het Europees Parlement behandeld. Ondanks fel verzet van privacyvoorvechters lijkt er een meerderheid in het parlement te zijn voor deze massale dataopslag.

Index

Bron:

Tubrosa-virus laat je pc stiekem YouTube-video's bekijken

Beveiligingsfirma Symantec waarschuwt voor malware die je pc massaal YouTube-video's laat bekijken, zonder dat je het doorhebt. Cybercriminelen verdienen aan je omdat ze advertentie-inkomsten krijgen van Googles videodienst.

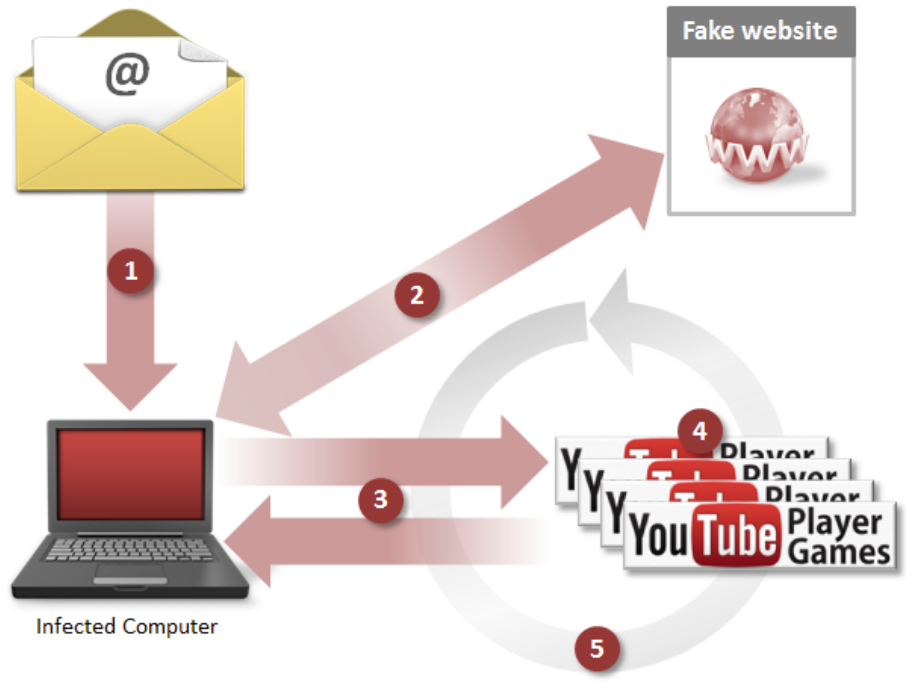
Om de scam mogelijk te maken, hebben de cybercrminelen eerst video's van andere YouTube-gebruikers gestolen en ze op hun eigen kanalen geplaatst. De Tubrosa-trojan is zo geschreven dat het bij Google lijkt alsof de video's telkens door een andere connectie worden bekeken. Daardoor heeft het systeem van YouTube niet door dat er eigenlijk wordt gefraudeerd.

Om te maskeren dat er YouTube-video's op de geïnfecteerde pc worden afgespeeld, dempt de malware ook softwarematig je speakers. Dit gaat net zolang door totdat je computer niet meer te gebruiken is, omdat het zoveel rekenkracht vraagt.

Phishing

De video's die door de criminelen op YouTube zijn gezet en waar je computer dus naar doorverwijst zijn op die manier al meer dan twee miljoen keer 'bekeken.' Symantec verwachtdat er zo al duizenden dollars aan advertentie-inkomsten zijn buitgemaakt.

Het virus wordt verspreid via phishing mails en heeft vooral huisgehouden in Zuid-Korea, India en Mexico. Europese landen lijken er nog geen doelwit van te zijn geweest. Google is er inmiddels van op de hoogte gebracht.



Steps in Attack

1. Spear-phishing email sent to victim and infects computer
2. The Trojan contacts fake website
3. Creates YouTube session with referrer and useragent
4. Silently opens a YouTube page
5. Process loops back to step 3

Index

Bron:

Hackers via een marktplaats in te huren

De term 'hacker' is verre van positief en wordt vaak geassocieerd met criminele activiteiten. Hacken is ook niet legaal, want het indringen van een computernetwerk zonder toestemming is tegen de wet.

Maar wat nu als de hacker toestemming heeft? Voor mensen die een hacker nodig hebben is er nu een marktplaats.

Op Hackerslist.com bieden hackers zichzelf aan om met toestemming van de gebruiker iets te hacken. Nu klinkt dit erg spectaculair, maar vaak draait het om simpele dingen zoals het opnieuw instellen van een wachtwoord of het heractiveren van een mailaccount.

Toch zitten er ook een aantal verzoeken bij die niet helemaal binnen de wet vallen. Zo vraagt iemand of het emailadres van zijn ex even gehackt kan worden, is er een andere persoon diezijn geldbalans bij een kredietbureau wil veranderen en staan er tientallen hackverzoeken voor iPhones. Onder deze verzoeken kunnen hackers reageren met hun geraamde prijs en aangeven waarom ze er de beste persoon voor zijn.

Verboden, maar lastig tegen te houden

Deze site is logischerwijs niet legaal. Uit een artikel van de New York Times blijkt dan ook dat de makers ondergedoken zijn en hun locatie niet bekendmaken. Zelf vinden ze het een juridisch grijs gebied en hebben ze helemaal niets illegaals voor ogen, zo blijkt uit veel gestelde vragen op de site. Daar geeft Hackerslist aan dat site is bedoeld voor het plaatsen van legale en ethisch verantwoorde hackverzoeken.

Dat hacken ‘hot’ is op het moment blijkt wel uit de recente gebeurtenissen omtrent hackersgroep Lizard Squad en het wereldwijde hackschandaal van Sony. Veelal verhalen die ver van je bed zijn, maar met deze marktplaats komt het potentieel wel erg dichtbij.

Index

Bron:

Logo belangrijk bij phishing

Een succesvolle phishingaanval blijkt over verschillende kenmerken te beschikken die de "cognitieve processen" van slachtoffers veranderen.

Met name "informatierijke" phishingmails met logo's en afbeeldingen, aangevuld met persoonlijke tekst die angst oproept, blijken zeer succesvol te zijn. Door het gebruik van de logo's en tekst op deze manier zouden de berichten veel persoonlijker aanvoelen. "We ontdekten in deze gevallen dat als het bericht om persoonlijke informatie vraagt, mensen eerder geneigd zijn dit snel te geven", aldus de onderzoekers.

Bij het onderzoek (pdf) dat de onderzoekers onder 125 studenten uitvoerden werd er met deze informatierijke phishingmails een slachtofferpercentage van 68% gehaald. De studenten kregen een e-mail die zogenaamd van de universiteit afkomstig leek en die gevoelens van spoed en angst moest oproepen. Volgens het bericht stonden de instellingen van het e-mailaccount niet goed en moesten ze dit corrigeren, anders zouden ze de toegang eroe verliezen.

49 studenten reageerden meteen en 36 nadat ze een reminder hadden ontvangen. "Nu e-mailtechnologie de standaard communicatiemethode wereldwijd wordt, zal phishing waarschijnlijk toenemen als technologie geavanceerder wordt en phishers nieuwe manieren vinden om slachtoffers aan te spreken", zegt professor en onderzoeker Arun Vishwanath. "Hoewel deze criminelen misschien niet snel worden gestopt, is weten wat ons kwetsbaar voor deze aanvallen maakt essentieel om internetgebruikers te kunnen beschermen."

Index

Bron:

Overheden bedreigen voortbestaan van het internet

Het internet staat op breken en dat komt vooral door overheden en meer specifiek door geheime diensten en hun allesvretende cyberspionage.

Het is niet bepaald rozegeur en maneschijn inhet nieuwste rapport van ENISA, de beveiligingsadviseur van de Europese Unie. Het internet dreigt zijn samenhang te verliezen, het vertrouwen in de digitale infrastructuur is tanende, mensen raken apatisch en laks, de traditionele beveiligingsoplossingen hebbben hun tijd gehad en cybercriminelen worden een flink handje geholpen door de geheime diensten als NSA en GCHQ.

Schuld van de overheden

ENISA spaart niemand in het rapport Threat Landscape 2014, en dat is terecht. "Het Internet" heeft nog nooit in zo'n kritieke fase verkeerd als nu, en dat lijkt vooralsnog voornamelijk de schuld van overheden waar ook ter wereld. De constateringen die ENISA doet laten daar weinig misverstand over bestaan. Europa boekt tot nu toe alleen vooruitgang in het vergaren en delen van informatie over bedreigingen; in het bevechten van die bedreigingen worden weinig slagen gewonnen.

ENISA legt dus de bal meerdere malen bij de overheid in het hok als het gaat om de toenemende onveiligheid op het internet in het algemeen en de bedreiging voor de stabiliteit van diverse infrastructuur in het bijzonder. "Het is zonder enige twijfel een feit dat geavanceerde aanvalsmethoden die tegenwoordig gebruikt worden binnen cyberspionage de beste voeding zijn voor de steile leercurve van cybercriminelen", concludeert ENISA onomwonden.

Methoden die vandaag gebruikt worden door spelers met veel (financiële) armslag en kennis worden morgen overgenomen door cybercriminelen, voegt ENISA eraan toe. En dat geeft weer "uitdagingen" in de ontwikkeling van een goede verdediging.

De nasleep van Snowden's onthullingen

En dan is er nog Snowden. Of liever gezegd, zijn onthullingen over de praktijken van inlichtingendiensten als de NSA en het Britse GCHQ. ENISA ziet de reacties op die onthullingen met lede ogen aan. De kans op fragmentatie van het internet zou erdoor toenemen, de zogeheten Balkanisering van het internet. "Als dat zich werkelijk zou voordoen zou dat de huidige staat van het internet en de cyber-security jaren terugwerpen in de tijd", griezelt ENISA.

Daarom moeten overheden hun verantwoordelijkheid nemen, en meer transparant zijn over hetgeen hun veiligheidsdiensten (mogen) doen. De eindgebruiker, zoals ENISA de internettende Europeaan noemt, is immers wantrouwend afgehaakt, wat op zich een groot risico is vanwege nalatigheid en desinteresse in simpele beveiligingsmaatregelen. En terecht overigens, nu zelfs versleutelde communicatie niet meer veilig is en traditionele beveiligingssoftware (antivirus etc) volstrekt ontoereikend is geworden.

ENISA zegt niet dat overheden moeten stoppen met (massa)surveillance, maar dat ze daar meer open over moeten zijn naar de samenleving toe. Overheden moeten een betere balans weten te vinden tussen hetgeen technisch mogelijk is en wat juridisch transparant kan zijn, poneert ENISA cryptisch. Betere regels zouden kunnen helpen.

Index

Bron:

Grote privacyproblemen in slimme energiemeters

De slimme energiemeter blijkt erg gevoelig voor fraude. Daarvoor waarschuwen brancheorganisaties Netbeheer Nederland en Energiebeheer Nederland. Het blijkt bij sommige meters kinderlijk eenvoudig om informatie van internet te plukken.

Het blijkt erg simpel om de gegevens van anderen te ontfutselen via de portal van sommige energieaanbieders. Welke dat zijn, wil Netbeheer niet bekend maken vanwege de veiligheid. Ineen verklaring waarschuwt de organisatie ervoor dat met alleen een naam, adres en telefoonnummer alle informatie zo te vinden is.

NAW-gegevens

Klanten met een slimme meter kunnen hun gegevens bekijken via websites en apps. Die moeten verifiëren of de klant ook echt op een adres wonen. Dat is vaak al mogelijk met alleen een combinatie van de naam en een telefoonnummer, en soms eventueel een geboortedatum. Die gegevens zijn van veel mensen makkelijk te achterhalen.

De brancheorganisaties pleiten voor een betere beveiliging in de apps en websites.

Handig

De slimme meters worden sinds vorig jaar steeds vaker verplicht in nieuwbouwhuizen. Met een slimme meter kan alle informatie over stroom- en gasverbruik direct worden doorgespeeld naar de energieleverancier, en kunnen gebruikers hun eigen energieverbruik zelf in de gaten houden. Dat kan jaarlijks veel geld besparen. Ook wordt misbruik (zoals het opzetten van wietplantages) makkelijker ontdekt.

Schaduwzijde

Maar de 'handige' slimme meter heeft een schaduwzijde, want critici waarschuwen voor potentiële fraude en diefstal. Gedetailleerde gegevens over stroomverbruik zijn namelijk erg waardevol voor identiteitsfraudeurs en andere criminelen. Die kunnen de informatie bijvoorbeeld gebruiken om precies te weten wanneer iemand op vakantie of op zijn werk is.

Index

Bron:

Politie: digitale vrijstaat door verdwijnen bewaarplicht

Als de bewaarplicht in Nederland wordt afgeschaft kan er een digitale vrijstaat ontstaan, zo waarschuwden politie en het Openbaar Ministerie.

Volgens beide partijen is het van essentieel belang dat telecom- en internetproviders bepaalde communicatiegegevens gedurende een bepaalde periode bewaren, ondanks kritiek van de Raad van State en het Europese Hof van Justitie dat de bewaarplicht in strijd met de fundamentele grondrechten is...

...Ook verschillende experts van Bits of Freedom, het Instituut voor Informatierecht (IVIR) en het College bescherming persoonsgegevens (CBP) waren bij de hoorzitting aanwezig. "Dat is snel. Het woord "kinderporno" viel binnen een paar minuten in de hoorzitting", aldus Bits of Freedom. Hoogleraar Egbert Dommering liet zich kritisch uit over de argumenten van politie en justitie dat de bewaarplicht juridisch noodzakelijk zou zijn. Alleen de opslag van communicatiegedrag is volgens de hoogleraar al een grote inbreuk op de privacy van burgers. Het CBP voegde toe dat als politie de doelmatigheid van de bewaarplicht niet kan aantonen er een fundamenteel probleem is.

Achtergrond >

Data Retention Directive) is op 3 mei 2006 in werking getreden en voorziet in een verplichting voor aanbieders van openbare elektronische communicatienetwerken en aanbieders van openbare elektronische communicatiediensten tot het bewaren van een bepaalde lijst van telecommunicatiegegevens gedurende een bepaalde periode.

Dit is een Europese richtlijn van de Europese Commissie om internet- en telefoniegegevens voor een bepaalde tijd op te slaan, en ter beschikking te houden van politie- en veiligheidsdiensten. De bewaarplicht is gebaseerd op een plan van de G8 uit mei 2001 wat erop is gericht op misdrijven op internet effectiever te bestrijden. Sinds de aanslagen van 11 september 2001 wordt ook terrorisme als een reden gegeven voor de maatregel. De meeste landen (ook België bij monde van minister Patrick Dewael van binnenlandse zaken en Nederland - minister Piet Hein Donner van justitie) zijn voorstander hiervan, al moet er voldoende afweging zijn ten opzichte van de privacy.

Op 14 december 2005 heeft het Europees Parlement (met 378 stemmen voor, 197 tegen en 30 onthoudingen) het compromis gesteund dat de fractievoorzitters van de twee grootste partijen in het EP, de christendemocraten en de sociaaldemocraten, enige dagen voorafgaand aan de plenaire vergadering hadden bereikt met de Raad. Dit akkoord wijkt af van het voorstel dat de LIBE commissie en haar rapporteur Alvaro aan het parlement had voorgelegd. Deze heeft gevraagd zijn naam als rapporteur te schrappen aangezien hij zich niet kon vinden in het compromis.

In Duitsland heeft de rechter op 27 februari 2009 bepaald dat de bewaarplicht niet in overeenstemming is met het Europees Verdrag voor de Rechten van de Mens (EVRM): "Het Gerechtshof ziet in de Bewaarplicht een schending van het grondrecht op privacy. Zij is in een democratie onnodig. Het individu geeft geen aanleiding voor die inbreuk, maar kan bij normaal gedrag wel geïntimideerd worden vanwege het risico op misbruik en het gevoel gecontroleerd te worden (..) Het op grond van artikel 8 van het EVRM opgelegde evenredigheidsbeginsel wordt door de richtlijn niet nageleefd, en is daarom ongeldig".[1][2]

In het Verenigd Koninkrijk is de zogenaamde "Data Retention (EC Directive) Regulations 2009" op 6 april 2009 van kracht geworden. Sindsdien moeten internet providers in het Verenigd Koninkrijk details van internet toegang (met name IP-adres), e-mailberichten en internettelefonie opslaan. De inhoud van de communicatie wordt niet opgeslagen, net zo min als het bezoek van websites.
[3] Telefoongegevens van het vaste net en mobiele net werden al opgeslagen door de telefoonbedrijven, inclusief de geografische locatie van de gebruikers.[4]

Sinds het najaar van 2005 speelt er een discussie over deze dataretentie in het Europees Parlement. Verschillende groeperingen (waaronder vertegenwoordigers van de muziek- en filmindustrie) willen dataretentie verplicht stellen in de Europese Unie, waardoor onder meer internetaanbieders gegevens over het internetgebruik van hun klanten voor een bepaalde tijd zouden moeten bewaren.

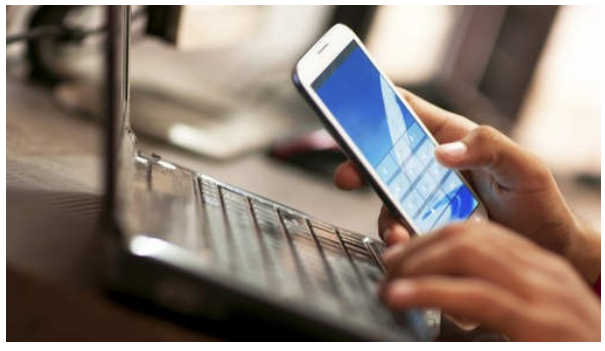
Op 15 december 2005 nam het Europees Parlement een voorstel aan dat het opslaan van communicatiegegevens verplicht stelt, maar niet de communicatie zelf. Men zal dus kunnen nagaan wie met wie wanneer contact heeft gehad via de telefoon, sms, of e-mail, maar de inhoud van de communicatie hoeft men niet te bewaren. De meeste Nederlandse Europarlementariërs stemden tegen de bewaarplicht.

Index

Bron:

Surf- en belgedrag burgers niet meer bewaard

Telecombedrijven en internetproviders hoeven geen gegevens over internet- en telefoniegebruik meer te bewaren. De wet die het massaal verzamelen en opslaan van gegevens over internet- en telefoongebruik van burgers in Nederland verplicht, is buiten werking gesteld.



De wet was ingesteld om politie en justitie te ondersteunen bij de opsporing. Belgegevens moesten een jaar worden opgeslagen, maar mochten alleen worden geraadpleegd bij een onderzoek naar een misdrijf waar een straf van acht jaar of meer op staat. Als het ging om criminaliteit die met minder dan acht jaar wordt bestraft, werd de toegang tot de gegevens gehalveerd naar een half jaar. Voor opgeslagen internetgegevens was de bewaartermijn zes maanden.

De rechter zegt in het vonnis zich ervan bewust te zijn dat het buiten werk stellen van deze wet 'ingrijpende gevolgen kan hebben voor de opsporing en vervolging van strafbare feiten'. In de omstreden wet is geen onafhankelijke toetsing geregeld voor de toegang tot de bewaarde privégegevens. Het Openbaar Ministerie dat dit zou moeten doen, is niet onafhankelijk, concludeert de rechter.

Onder meer de Nederlandse Vereniging van Journalisten, de Nederlandse Vereniging van Strafrechtadvocaten en privacyvoorvechter Privacy First eisten in een kort geding dat de wet buiten werking zou worden gesteld. Het Europese Hof van Justitie bepaalde vorig jaar dat het opslaan van communicatiegegevens van iedereen - zonder concrete verdenking - een zware aantasting van de privacy is en niet is toegestaan.

'Overwinning'

,,De rechter heeft een einde gemaakt aan het verplicht bewaren van communicatiegegevens van iedereen, inclusief niet-verdachte burgers'', reageert een van hun advocaten Fulco Blokhuis. ,,Het belang van privacy weegt terecht zwaarder. Het oordeel van de rechter is in lijn met adviezen van het College Bescherming Persoonsgegevens en de Raad van State.''

Collega Otto Volgenant is het met hem eens. ,,Deze uitspraak is geen verrassing. De Nederlandse wet was in strijd met het Europese recht. Dit is een overwinning voor journalisten en advocaten die moeten kunnen rekenen op de vertrouwelijkheid van hun communicatie. En dit is vooral een overwinning voor de privacy van alle burgers'', aldus de advocaat.

Index

Bron: AD

BMW dicht lek waarmee hackers auto's konden ontgrendelen

Met een software-update verhelpt BMW een serieus veiligheidsprobleem. Hackers konden de deuren van de wagens openen met een smartphone.

De Duitse autoconstructeur BMW heeft een lek in zijn Connected Drive-software verholpen met een veiligheidspatch. Door de fout konden dieven de deuren van de wagens openen met een willekeurige smartphone.

Enkele jaren geleden wuifde de fabrikant nog een probleem weg waarbij dieven misbruik maakten van het keyless entry-systeem van zijn wagens. BMW zei toen dat diefstal een probleem was van alle constructeurs. In dat geval zouden hackers apparaatjes aan het ODB-systeem (On Board Diagnostics) gekoppeld hebben om zo een nieuwe sleutel te programmeren.

Connected Drive

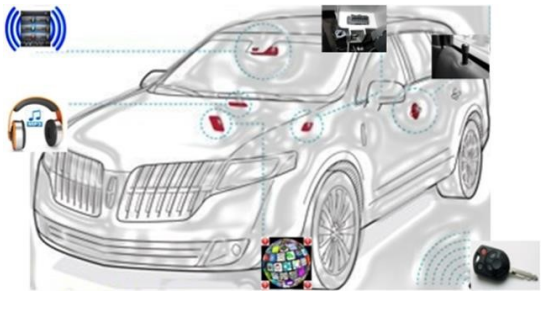
Een nieuwe fout met ongeveer dezelfde gevolgen wordt nu blijkbaar serieuzer genomen. BMW rolt naar 2,2 miljoen wagens (BMW's, Rolls-Royces en Mini's) een software-update voor het Connected Drive-systeem uit. Dit platform werkt met een ingebouwde simkaart voor navigatiedoeleinden en apps, en kan ook gebruikt worden voor noodoproepen en om een wifi-hotspot in de wagen te installeren.

Volgens de Duitse automobilistenvereniging ADAC, die de fout aan BMW meldde, konden hackers op enkele minuten tijd via het systeem de deuren van de wagens openen, zonder enig spoor achter te laten.

Waar het lek precies zit, meldt BMW niet, maar het bedrijfbevestigt dat ADAC inderdaad "een potentieel veiligheidsgevaar" heeft gevonden wanneer er "data wordt verstuurd" en dat het de veiligheid van Connected Drive heeft opgeschroefd. Dat gebeurt door alle gegevensverkeer van het systeem langs een versleutelde HTTPS-verbinding te sturen. HTTPS is vooral bekend van de bankenwebsites. Het zorgt er voor dat klanten in een beveiligde omgeving transacties en overschrijvingen kunnen afhandelen via pc-banking. De laatste jaren is het aantal toepassingen echter fors toegenomen.

olgens BMW zouden er nog geen gevallen gemeld zijn waarbij auto's werden gestolen via de hack.

Nu steeds meer auto's een online verbinding krijgen, lopen wagens steeds meer in het vizier van hackers. Bluetooth is daarbij een geliefkoosde methode omdat het relatief eenvoudig te kraken is. Met de ingebouwde gsm-verbinding is het in theorie dan weer mogelijk om een wagen op honderden kilometers afstand te hacken.



Index

Bron:

Schud je online achtervolgers af

Smartphone-apps gebruiken steeds vaker je huidige locatie om een dienst aan te bieden - maar die data komt helaas ook bij adverteerders terecht.

Weet jij welke apps op je smartphone weten waar jij bent?

De meeste mensen geven applicaties als Yelp, Google Maps of een weer-app zonder nadenken toegang tot de gps-data van hun telefoon. Daar krijgen ze ook een dienst voor terug: restaurants in de buurt in een onbekende stad, of de snelste manier om thuis te raken zonder files tegen te komen bijvoorbeeld.

Het probleem daarbij, zoals wel vaker het geval is, is dat de diensten in kwestie die gps-data ook deelt met adverteerders en andere derde partijen, vaak zonder dat de gebruiker zich daarvan bewust is.

Zelfs het anoniem vrijgeven van deze data beschermt de privacy van mensen niet per se. Een voorbeeld: de stad New York gaf anonieme data vrij aan het publiek over taxiritten in de stad. Binnen de kortste keren had een groep aan de hand daarvan achterhaald welke celebrities regelmatig tripjes maakten naar stripclubs.

Het mag dus niemand verbazen dat computerwetenschappers volop aan het werken zijn aan beschermingsmethoden.

Aan Duke University in Durham ontwikkelden onderzoekers een systeem dat ze CacheCloak doopten. Dat geeft je exacte coördinaten niet door aan een dienst als Google Maps; in plaats daarvan stippelt het een imaginair pad uit dat jij zou kunnen volgen, en zorgt ervoor dat de paden van verschillende gebruikers zo veel mogelijk door elkaar lopen. De consument krijgt nog steeds een vrij accuraat resultaat, maar het bedrijf dat gps-data verzamelt krijgt alleen maar een groot aantal mogelijk af te leggen paden te zien krijgt.

Een andere optie is het meesturen van neplocaties met de echte gps-data van een gebruiker, een systeem waar Microsoft mee experimenteerde. Als de opeenvolging van neplocaties steek houdt, kan een dienst niet onderscheiden wat de echte locatie is, en zal de app informatie voor beide punten weergeven. De gebruiker kan de verkeerde punten dan gewoon negeren.

Natuurlijk heeft die strategie een aantal nadelen, zo stelt Michaël Herrmann, een computerwetenschapper aan de KU Leuven, in Science. De bibliotheek van nep-routes die gebruikt wordt kan maar beter geen genante plaatsen bevatten; veel mensen willen waarschijnlijk liever dat Google weet dat ze naar de supermarkt gingen dat dat die trip gemaskeerd werd door een neproute naar een HIV-kliniek, om maar iets te noemen.

Een derde optie is om gewoon de juistheid van de locatiemeting naar beneden te halen. Als diensten enkel maar weten in welk blokje van een vierkante kilometer je je bevindt, kunnen ze niet veel aanvangen met die data. Jammer genoeg zorgt dat ervoor dat de kwaliteit van de dienstverlening van die app erop achteruit gaat.

Index

Bron:

Een USB-stick beveiligen

SecurStick maakt een haast onkraakbare Safe Zone aan op je USB-stick, waar je al je gevoelige informatie versleuteld kwijt kan.

Je downloadt SecurStick . Pak het bestand uit en kopieer SecurStick.exe naar de stick die je wil beveiligen. Met een dubbelklik op het exe-bestand wordt je browser opengegooid en kom je op een pagina terecht die je wat meer info geeft over de tool.

Heb je nog geen zogenaamde Safe Zone aangemaakt op deze stick, dan moet je hier een wachtwoord kiezen. De instructies zijn behoorlijk streng, om zeker te zijn dat je een sterk wachtwoord kiest: het moet minstens vijf tekens lang zijn, hoofd- en kleine letters bevatten, er moet minstens een cijfer en minstens een speciaal teken inzitten. Het vinkje bij 'Encrypt file names' laat je best staan, voor extra veiligheid. Met een druk op 'Create' wordt er een Safe Zone aangemaakt.

De webpagina vertelt je dat je ingelogd bent, en Windows Verkenner opent automatisch de veilige zone op je stick.

De veilige zone verschijnt ook als aparte schijf in Windows Verkenner. Alles wat je hiernaartoe kopieert wordt voortaan beschermd door SecurStick. Ben je klaar, vergeet dan niet uit te loggen door op 'Logoff' te klikken. De Safe Zone is nu niet meer zichtbaar in Windows Verkenner, om weer aan je bestanden te kunnen dubbelklik je op SecurStick.exe en log je in. Let wel: als je je wachtwoord vergeet, ben je je bestanden voorgoed kwijt.

Je kan wel verschillende veilige zones aanmaken, door een kopie vanSecurStick.exe in een submap te steken en van daaruit hetzelfde proces te doorlopen.

Index

Bron:

Vijf antivirusscanners voor je Mac

Mac-gebruikers denken nog vaak dat ze geen bescherming nodig hebben, maar het platform wordt steeds populairder bij hackers.

Ben je van mening dat je op je Mac geen antivirussoftware nodig hebt? Je bent zeker niet de enige die dat denkt, maar zijn Macs altijd virusvrij? Het korte antwoord is neen. Hoewel de kans dat je op een Mac last krijgt van malware kleiner is dan op een Windows-pc, is er nog steeds een risico. De toegenomen populariteit van het platform zorgt ervoor dat ook steeds meer hackers hun pijlen op het ecosysteem richten.

Het beschermen van je Mac zijn de kosten niet. Vier van de vijf virusscanners die wij hier op een rij hebben gezet zijn gratis te gebruiken.

Sophos Antivirus voor Mac Home Edition

Een uitgebreide scanner die niet alleen uitkijkt naar OS X-malware, maar ook het verspreiden van Windows-virussen stopt die je eventueel hebt opgepikt. Eenmaal geïnstalleerd werkt de software stilletjes op de achtergrond. Je kan scannen bij het openen van een document, wanneer je het handmatig aanzet of volgens een schema.

Sophos Antivirus werkt op Macs die werken met OS X 10.6 Snow Leopard tot het laatste OS X 10.10 Yosemite.

Vindt en verwijdert virussen, trojans en wormen.

Stopt alle dreigingen, zelfs als ze nieuw zijn.

Eenvoudig te installeren en draait rustig.

AVG Antivirus voor Mac

Eenvoudig in gebruik maar erg krachtige antivirusscanner die altijd alert is. De software draait op de achtergrond en beschermt je tegen oude en nieuwe gevaren.

Beschermt tegen malware van OS X, Windows en Android.

Drag-and-drop-interface stelt je in staat makkelijk verdachte bestanden te scannen.

Automatische updates.

Avast Free Mac Security

Een lichtgewicht maar toch krachtige antivirusscanner. Hij houdt niet alleen je systeembestanden in de gaten, maar zorgt ook voor een veilige mail- en webervaring.

Avast wordt wereldwijd door 220 miljoen klanten gebruikt.

Constante updates.

Veilige VPN voor je iOS- of Androidapparaat om publieke wifi te beschermen.

ClamXav

Een gratis en openbron antivirusscanner voor je Mac. De software beschermt je tegen zowel OS X- als Windows-malware.

Makkelijk in gebruik.

Markeert besmette bestanden op een duidelijk manier.

Veelzijdig en eenvoudig in te stellen.

Krachtige openbron scanner.

Intego Mac Internet Security X8

Het enige betaalde product in de lijst (beginnende vanaf 40 euro). Toch is het de moeite van het vermelden waard, want het biedt premiumopties die de gratis programma's niet kennen, zoals een firewall en ouderlijke controle.

Bescherming tegen malware en virussen voor Mac en Windows.

Netwerkbescherming die zich bewust is van de locatie.

Simpele configuratie, ook voor niet-technische gebruikers.

Index

Bron:

Vier redenen waarom we weinig geven om onze privacy

Facebook registreert je locatie. Banken verkopen je data. Televisies sturen je kijkgedrag door. En toch malen wij er niet om. Hoe komt dat?

De laatste maanden kwamen enkele gevallen aan het licht. Facebook registreert je locatie. Banken sluiten een mogelijke verkoop van klantengegevens aan adverteerders en externe bedrijven niet uit. En onlangs bleken bepaalde smart-tv's van LG informatie te verzamelen en door te sturen aan servers van het Koreaanse bedrijf.

We zijn vaak verbolgen over praktijken en gaan vaak te keer op sociale media. Maar we zullen niet snel Facebook, Google of onze bank vaarwel zeggen. "Snowden verandert nog weinig aan ons gedrag", schrijven auteurs Sander Klous en Nart Wielaard in het boek 'Wij zijn big data'.

"We zijn vaak heel boos, maar kunnen die boosheid ook weer met het grootste gemak opbergen in ons geheugen", schrijven ze. In 'Wij zijn big data' sommen de auteurs vier redenen op voor ons tegenstrijdig gedrag:

1. We zijn dol op gratis

There's no such thing as a free lunch. Menig product of dienst lijkt gratis, maar is dan nooit echt. En met de komst van internet is de gratis-economie, en met name het advertentiemodel, heel dominant geworden.

Voor de consument is dat goed nieuws: we hoeven onze portemonnee niet open te trekken om te mailen, met vrienden in contact te blijven, onze route te bepalen of foto's te stockeren. We betalen met onze persoonlijke data. "Maar als iets gratis is, zijn we waarschijnlijk zelf het product."

2. We zijn kuddedieren

In het boek 'The power of habbit' van Charles Duhigg wordt beschreven hoe een vrouw haar leven compleet omgooit. Ze stopt met roken, verandert van baan en gaat marathons lopen. Op hersenscans is te zien dat de patronen in haar hersenen ook fundamenteel veranderd zijn. De mens zit vastgeroest in routines die nauwelijks of moeilijk te veranderen zijn.

We zijn niet alleen gewoontedieren, maar ook kuddedieren. Dat is de oorzaak van veel fraude en normoverschreidend gedrag, en van de hele bankencrisis.

3. We zijn geen haar beter dan de NSA

Het scenario in 1984 van Georges Orwell ging uit van een algehele surveillancestaat. De realiteit is dat we daar zelf volop aan meewerken. "We leggen onze dagelijkse realiteit - en die van onze vrienden - doorlopend vast met onze telefoon. Die beelden komen dan op Facebook, Flickr, Instagram, Vine of Youtube."

Dankzij dashboardcamera's kunnen we meegenieten van ongevallen van onze medeweggebruikers. Met name in Rusland blijkt die activiteit erg populair.

4. We zijn verslaafd aan maatwerk

Persoonlijk maatwerk is de norm geworden in dienstverlening. "We willen dat onze typfouten in zoekopdrachten worden gecorrigeerd. We willen onze favoriete en persoonlijke Spotify-playlist op elk apparaat. We willen dat ons e-mailprogramma onze mail helpt te sorteren."

Gemak dienst de mens. Maar al deze wensen zijn alleen in te vullen als we bereid zijn om bedrijven toegang te geven tot onze data.

Index

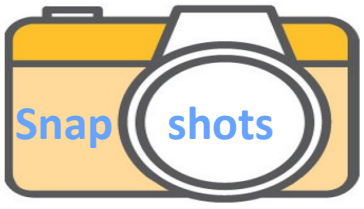
Bron:

Software schatkist

De kist is gevuld met nieuwe software. Nieuwsgierig?

Open de kist middels de sleutel en ontdek…….

Index



Al bij een op de drie echtscheidingen speelt wat we allemaal delen op facebook, een rol. Een advocatenkantoor in Leeds, Engelandanalyseerde tweehonderd scheidingen en in 66 daarvan werden uitlatingen, foto's, gedrag en zelfs likes op facebook als bewijs aangevoerd. 'Dingen die we posten, foto's, berichten waarin we getagd worden – het geeft een schat aan informatie die in de rechtbank kan gebruikt worden', aldus advocaat Lyn Ayrton. Ze geeft als voorbeeld de ex die blijmoedig verhaalt over ontvangen bonus, verre vakantie of nieuwe job – het kan er op wijzen dat er gelogen is over de financiën. Of die persoon die zegt geen nieuwe relatie te hebben terwijl er op facebook foto's staan en uitnodigingen voor een housewarming party. 'Post niets op facebook als je niet eerlijk bent'.

==========

Wat nou high tech crime? In Engeland had een 7-jarig meisje, Betsy Davies, niet meer dan 10:54 minuut nodig om een wifi-aanval uit te voeren. Het meisje liet, als onderdeel van een bewustwordingscampagne van een provider, daarmee zien hoe simpel het is om ergens in te breken. Ze keek eerst naar een instructievideootje op YouTube en zette vervolgens een 'roque acccespoint' op waarmee ze het verkeer van de gebruikers kon onderscheppen. Het experiment werd bijgewoond door een onafhankelijke internetbeveiligingsexpert, Marcus Dempsey, die verklaarde niet verrast te zijn. 'Hacking is letterlijk kinderspel'.

==========

Als gevolg van de aanslagen in Parijs en de politieacties in België gaan radicale moslims massaal offline, schrijft juridisch redacteur Robert Bas van de NOS. Twitteraccounts worden verwijderd, Facebook en YouTube niet meer geüpdatet – allemaal om maar uit het zicht van opsporings-, inlichtingen- en veiligheidsdiensten te blijven. Want dát die diensten tegenwoordig sociale media afschuimen op zoek naar informatie, is geen nieuws meer. Volgens Bas gingen er onder jonge moslims al snel na 'Parijs' geruchten dat er een reeks arrestaties aanstaande was en hebben veel van hen daarom het hazepad gekozen. Sommigen zouden zelfs al het land uit zijn, denkt Bas.

==========

Het aantal Nederlanders dat toegeeft wel eens illegaal te downloaden, wordt steeds kleiner. Nog maar een kwart doet dat,blijkt uit cijfers van onderzoeksbureau GfK. Een half jaar terug ging het nog om 37%. In dezelfde periode steeg het aantal Nederlanders dat gebruikt maakt van streamingdiensten als Spotify en Deezer van 63 naar 75%. Nederland blijkt een belangrijke markt voor zulke diensten: 4,6 miljoen Nederlanders streamen muziek. Spotify heeft wereldwijd overigens 60 miljoen gebruikers, Deezer 16 miljoen. Ook video-streaming wordt populairder. Al 4,7 miljoen Nederlanders gebruiken diensten als Netflix.

==========

The Guardian bericht over een forse database met gegevens over westerse jihadstrijders en -sympathisanten, volledig gebouwd via openbronnen als twitter en facebook. De database, met al zevenhonderd profielen, is gebouwd door een team sociale media-experts van het International Centre for the Study of Radicalisation and Political Violence (ICSR) aan King's College in London en wordt dagelijks bijgewerkt – gesneuvelde strijders worden dezelfde dag nog 'verwijderd'. Vaak op basis van tweets of postings, die dan aangevuld worden met informatie uit andere (open) bronnen. Van elke persoon in de database worden 72 data points bijgehouden, van geboorteplaats tot voormalige werkgevers. Van de negentig Britten die in het systeem zaten, zijn er nog vijftig over – de meeste afvallers zijn gedood bij luchtaanvallen op IS-posities. Het ICSR werkt momenteel aan een nieuwe database waarin de gegevens van circa zeventig vrouwen worden bijgehouden – ook weer vooral op basis van hun 'social media footprint'.

==========

Het meldpunt MIND kreeg in 2014 meer dan driehonderd meldingen van internetdiscriminatie, een stijging van 22% ten opzichte van 2013. De meeste meldingen betreffen discrimatie op basis van ras (159), antisemitisme (31) en leeftijd (29). Opvallend is dat bijna de helft van alle meldingen is ingegeven door uitingen op sociale media. Volgens directeur Titus Visser van MIND is in de meldingen 'de verontwaardiging van burgers over online discriminatie' terug te zien, bijvoorbeeld in het gedoe rond zwarte piet en de selfie van voetballer Leroy Fer.

==========

Tja. Dan ben je 16, schiet je een klasgenoot in z'n gezicht en dan maak je een selfie met het lijk. In Jeannette,
Pennsylvania is de 16-jarige Maxwell Morton opgepakt en aangeklaagd voor de moord op klasgenoot Ryan Mangan. Morton maakte het de politie wel erg gemakkelijk: hij maakte een foto van zichzelf en zijn slachtoffer en zette die op Snapchat. Voorzien van de tekst dat Ryan 'not the last one' was. 'Told you I cleaned up the shells'. De meeste foto's blijven maar een paar seconden zichtbaar op Snapchat maar natuurlijk niet als iemand er direct een schermafdrukje van maakt. Dat deed een vriendje van Morton, waardoor de foto binnen no time bij de politie lag. Volgens de politie toont de foto in ieder geval aan dat Morton op de crime scene aanwezig was. Officier van justitie John Peck liet weten in de dertig jaar dat hij bij het OM werkt, nog nooit zoiets te hebben meegemaakt. Morton heeft inmiddels bekend, het wapen en enkele kogelhulzen zijn gevonden.

==========

In Italië staat agent Dino Maglio (35, uit Padua) van de Carabinieri terecht omdat hij vrouwen misbruikte die hij via een website had ontmoet. De man was als 'Leonardo' actief op Couchsurfing, een site waar mensen hun woning aanbieden aan toeristen. De agent heeft bekend dat hij een 16-meisje uit Australië, die met haar moeder en zus Italië bezocht. Hij drogeerde – een slaappil in een glas Baileys – en verkrachtte het meisje. Volgens de aanklacht heeft hij 'veel meer' vrouwen misbruikt, mogelijk zestien. Volgens de agent was de seks vrijwillig maar bij huiszoeking werden veertig slaappillen gevonden. De site Couchsurfing kwam al in 2009 met een vergelijkbaar incident in het nieuws, toen een meisje uit Hong Kong in Leeds, Engeland werd verkracht.

==========

Index

Het ministerie van Binnenlandse Zaken heeft afsprakengemaakt met twaalf verkoopsites, waaronder Marktplaats, waar veel postadressen worden aangeboden. Met die adressen, onder meer gebruikt om illegaal in vakantiehuisjes te wonen of om je ergens in een gemeente in te schrijven, wordt nog wel eens gefraudeerd. Het Agentschap Basisadministratie Persoonsgegevens en Reisdocumenten waarschuwde vorig jaar honderd particuliere aanbieders. Nederland telt circa vijftigduizend briefadressen. Zien de verkoopsites advertenties daarvoor, dan wordt dat aan BZ doorgegeven. Die waarschuwt dan weer de desbetreffende gemeente die het adres zal controleren.

==========

In de rechtbank, onder toeziend oog van de rechter heeft een student (20, uit Oudenbosch) alle naaktfoto's van zijn 17-jarige vriendin van zijn laptop moeten verwijderen. Hetzelfde deed hij met zijn smartphone. De student was in kort geding gedaagd door het meisje nadat hij dreigde haar foto's op internet te zetten. Het stel had elkaar op Instagram leren kennen, ze wisselden (naakt)foto's uit maar toen de jongen seks met haar wilde, haakte ze af. Om haar te dwingen, dreigde de jongen haar, haar vrienden en haar familie de foto's te publiceren. Hij eiste ook haar wachtwoorden voor twitter en facebook, om te zien of ze nog andere vriendjes had. Toen een bemiddelingsgesprek niks opleverde, deed het meisje aangifte. De advocaat van de jongen wees het meisje als schuldige aan. Hoe dan ook, tijdens de zitting werd een 'vredesakkoord' getekend. Foto's verwijderen, aangifte intrekken en zand erover, aldus de rechter.

==========

In een poging de zaak van Les Strijder, in 2002 dood aangetroffen op een parkeerplaats langs de A27 bij Hilversum, op te lossen, heeft het cold case team ook een facebookpagina geopend. Strijder werd gevonden op een plek die destijds als 'mannenontmoetingsplek' bekend stond. Het doel van de pagina? 'De Coldcasezaak Bosberg met elkaar oplossen!' De zaak was ook bij diverse opsporingsprogramma's op tv. Na enkele tips van burgers is een man (36) aangehouden.

==========

Europol-directeur Rob Wainwright heeft gepleit voor nauwere samenwerking tussen veiligheidsdiensten en technologiebedrijven als Facebook en Twitter. Behalve als recruteringsmiddel worden sociale media ook voor propaganda gebruikt. Wainwright wil nieuwe wetten waarmee veiligheidsdiensten terreurverdachten beter kunnen controleren. Volgens Europol zijn er in de EU zo'n vijfduizend burgers 'potentieel terrorist'. De helft daarvan staat op een lijst.

==========

In 2014 is voor bijna 8 miljoen euro aan internetfraude bij de politie gemeld. Het ging om bijna 44 duizend aangiftes, waarvan er overigens bijna zevenduizend weer werden ingetrokken. In Oost-Nederland werden de meeste aangiftes gedaan (8182), in Limburg de minste (2751). Gemiddeld gingen de slachtoffers voor 182 euro het schip in, blijkt uit cijfers van het Meldpunt Internetoplichting. Omdat naar schatting van de politie slechts de helft tot tweederde van de slachtoffers aangifte doet, is de schade in werkelijkheid veel hoger. Volgens Jesse van der Putte, coördinerend officier van justitie van het LMIO, is aangifte doen daarom essentieel. Hij ziet een verschuiving nasar professionale criminaliteit: groepen oplichters met een centrale aansturing, een stel katvangers, mensen die katvangers werven en mensen die de betalingen organiseren. Opsporing van deze bendes wordt steeds ingewikkelder, zegt Van der Putte, die benadrukt dat internetklant ook zelf veel kan doen. Als iets te mooi is om waar te zijn, dan is het dat ook. Een andere tip is te googlen op de verkoper. 'Het lijken open deuren maar als je naar de cijfers kijkt, zijn nog veel online kopers zich er niet van bewust'.

==========

Je DigiD gekaapt? Zou best eens door een oude politiesite kunnen komen. Uit onderzoek van Reporter Radio blijkt dat op meerdere verlopen internetdomeinen van de Nederlandse politie, mogelijk was om DigiD-logins te stelen en malware bij gebruikers te installeren. De domeinnamen kwamen 'vrij' bij de overstap van alle voormalige korps- en politiewebsites naar het concern-domein Politie.nl. Omdat veel wijkagenten én media bleven verwijzen naar die oude adressen, kwamen mensen onbedoeld toch op een (inmiddels door criminelen overgenomen) nepsite terecht. Beveiligingsonderzoeker Wouter Slotboom wist, samen met Reporter, vijftien verlopen domeinnamen in bezit te krijgen. Hij plaatste daarop nepinfo en wist zo onder meer DigiD-gegevens van gebruikers te verkrijgen. Volgens Slotboom moet juist een vertrouwde organisatie als de politie scherper zijn op identiteitsdiefstal – aan waarschuwingen hiertegen spendeert de Nederlandse overheid miljoenen euro's. Slotboom heeft de bewuste domeinen inmiddels overgedragen aan de politie. De domeinen waren 'aan de aandacht ontsnapt' .

Index

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

opgelet op internet.nl

Voor vragen over veilig internetbankieren bij uw eigen bank, kunt u op een van de onderstaande websites terecht.

Websites banken	
ABN AMRO	LeasePlan Bank
Argenta	Rabobank
Credit Europe Bank	SNS Bank
DeltaLloyd Bank	Staal Bankiers
DHB Bank	Triodos Bank
Friesland Bank	Van Lanschot Bank
ING Bank	ASN Bank

MARKTPLAATS: "Wat moet ik doen als ik denk dat ik ben opgelicht?"

Antwoord

1. Wanneer u vooraf betaalt, maar de verkoper het product vervolgens niet levert, adviseren wij het volgende:

Neem eerst nogmaals contact op met de verkoper. Mogelijk is er sprake van een misverstand of wordt het product alsnog geleverd. Breng in geval van oplichting altijd de Politie op de hoogte (dit kunnen wij niet voor u doen). Zij hebben immers de kennis, expertise en opsporingsbevoegdheden om onderzoek te doen naar strafbare feiten. Wij adviseren u om aangifte te doen bij het Meldpunt Internetoplichting van de Politie via www.mijnpolitie.nl (formulier Melding Internetoplichting).
Wij adviseren u om het formulier zo accuraat en volledig mogelijk in te vullen.
Zorg dat u, wanneer u aangifte gaat doen, alle relevante gegevens bij de hand heeft zoals:

- Uw eigen (contact)gegevens, inclusief uw Burgerservicenummer (BSN).
- De (contact)gegevens van de partij met wie u heeft gehandeld (zoals naam en bankrekeningnummer).
- De gegevens van de transactie, zoals het advertentienummer en de onderlinge communicatie.

Meld oplichting ook altijd aan Marktplaats. Wij nemen dergelijke meldingen zeer serieus en nemen waar mogelijk gerichte maatregelen. Indien u aangifte doet via het formulier Melding Internetoplichting op www.mijnpolitie.nl wordt direct

Index

Cybercrime wetsartikelen

Wetsartikelen voor computercriminaliteit in enge zin

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

Voor cybercrime in enge zin zijn de volgende wetsartikelen beschikbaar:

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

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

. Artikel 161 septies WvSr: stoornis in de gang of in de werking in een geautomatiseerd werk of werk voor telecommunicatie door schuld.

. Artikel 350a WvSr: het opzettelijk onbruikbaar maken en veranderen van gegevens.

. Artikel 350b WvSr: het onbruikbaar maken en veranderen van gegevens door schuld,

. Artikel 139c WvSr: het aftappen en/of opnemen van gegevens en

Artikel 139d WvSr: het plaatsen van opname-, aftap- c.q. afluisterapparatuur.

Er zijn geen specifieke wetsartikelen om cybercrime in ruime zin aan te duiden. Voor de hoofddaad worden dezelfde wetsartikelen gebruikt als wanneer de criminele daad niet metICT zou worden gepleegd.

———————————————————

Haatzaaien.

'Het zaaien van haat of het (opzettelijk) beledigen of discrimineren van een groep mensenwegens hun ras, hun godsdienst of levensovertuiging, hun hetero- of homoseksuelegerichtheid of hun lichamelijke, psychische of verstandelijke handicap, zonder een bijdrage te leveren aan het publieke debat, waarbij ICT essentieel is voor de uitvoering' .

Haatzaaien staat niet als zodanig in het wetboek.

Aan de hand van de geformuleerde definitie kunnen echter de volgende wetsartikelen worden onderscheiden die delicten omschrijven welke vallen onder deze noemer:

- Artikel 147 WvSr: godslastering
- Artikel 90quater WvSr: discriminatie.
- Artikel 137d WvSr: aanzetting tot discriminatie van een bevolkingsgroep.
- . Artikel 137e WvSr: openbaarmaking discriminerende uitlatingen.
- . Artikel 137f WvSr: deelname of steunen van discriminatie.
- . Artikel 137g WvSr: discriminatie in ambt, beroep of bedrijf.
- . Artikel 131 WvSr: opruiing.

———————————————————

Cyberstalking.

'Cyberstalking' is de verzamelnaam voor het stelselmatig lastigvallen van een persoon doorprovocerende uitspraken te doen en/of berichten te plaatsen via online forums, bulletin boards en chatrooms, of de ander als het ware via spyware te bespioneren dan wel voortdurend ongevraagd e-mail en spam te sturen. Er is sprake van een verregaande inbreuk op de privacy van het slachtoffer' .

Relevante wetsartikelen zijn:

Artikel 285b WvSr: belaging.

Artikel 138a WvSr: computervredebreuk.

Artikel 266 WvSr: belediging.

———————————————————

Grooming.

Grooming wordt door het particuliere Meldpunt Kinderpornografie op Internet (MKI) opgevat als het zich op internet anders voordoen (door een volwassene) met het doel om seksueel getinte contacten te leggen met kinderen. Deze contacten kunnen zowel virtueel (seksuele handelingen voor de webcam) als fysiek (een ontmoeting waarbij het kind daadwerkelijk seksueel misbruikt wordt) zijn . Op dit moment is grooming niet strafbaar.

Grooming is echter wel opgenomen in het door Nederland ondertekende, maar nog niet door Nederland geratificeerde EU-verdrag van Lanzarote van 25 oktober 2007, artikel 23 ('Solicitation of children for sexual purposes'), waarin landen zich verplichten om grooming strafbaar te stellen. Grooming is dan het door een volwassene via ICT leggen van contacten-met een jongere met de intentie deze te ontmoeten voor het verrichten van seksuele handelingen, gevolgd door het feitelijk geven van uitvoering aan het tot stand brengen van die ontmoeting. Dat is een aanzienlijk engere uitleg dan het MKI geeft, vooral omdat volgens het verdrag begonnen moet zijn met het realiseren van de ontmoeting ('material acts leading to such a meeting').

———————————————————

Handel in mensen of foute goederen.

Verschijningsvormen:

drugs, geneesmiddelen, vuurwapens en explosieven, mensenhandel- en smokkel, heling.

Kenmerkend bij deze vormen van cybercrime is dat de handel plaatsvindt op of middels ICT

(bijvoorbeeld marktplaats) en dat de betrokken partijen weten dat het gaat om illegale handel.

Relevante artikelen zijn:

Artikel 273a WvSr mensenhandel.

Artikel 416 WvSr opzetheling.

Artikel 417 WvSr opzetheling (gewoonte).

Artikel 274 WvSr slavenhandel.

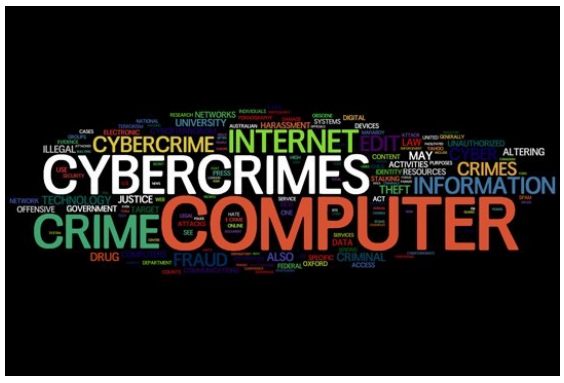
Artikel 2 Wwm: wet wapens en munitie

Artikel 31 Wwm: overdragen van wapens of munitie

Artikel 2 Ow: opiumwet

Artikel 3 Ow: opiumwet

Artikel 3b Ow: opiumwet



Index

Cybercrime wetsartikelen (2)

Bij piraterij gaat het feitelijk om illegale handel van allerhande 'cd's, dvd's, films, software en andere producten waarvoor auteursrechten gelden' . De nadruk ligt volgens het KLPD veelal bij eindgebruikers, internetpiraten en vervalsers, en in mindere mate bij gebruikers van licenties (bijvoorbeeld bedrijven) en computerverkopers. In alle gevallen is piraterij echter strafbaar en valt het onder meer onder het Wetboek van Strafrecht, de Auteurswet en de Merkenwet.

Relevante artikelen uit het wetboek van strafrecht zijn:

- Artikel 337 WvSr: handel goederen vervalste merken.
- Artikel 328 WvSr: oneerlijke mededinging.
- Artikel 441a WvSr: heling.
- Artikel 1 AW: auteurswet
- Artikel 31 AW: opzettelijk inbreuk op auteursrecht
- Artikel 31a AW: voorwerp met daarop een inbreuk op auteursrecht
- Artikel 31b AW: beroep maken van inbreuk op auteursrecht

———————————————————————————-

Kinderpornografie.

Kinderpornografie is in Nederland strafbaar gesteld in artikel 240b Wetboek van Strafrecht.

Kinderpornografie is volgens dit artikel iedere afbeelding - of gegevensdrager die een afbeelding bevat - van een seksuele gedraging waarbij iemand, die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar betrokken is'. Zowel het verspreiden, tentoonstellen, vervaardigen, invoeren, doorvoeren, uitvoeren als in bezit hebben ervan is in Nederland strafbaar. In Nederland is het enkel kijken naar kinderpornografie niet strafbaar.

———————————————————————————-

Illegale kansspelen.

'Volgens de Wet op de kansspelen (Wok) is er in Nederland een verbod op het aanbieden,

propageren en gebruikmaken van kansspelen waarvoor geen vergunning is verleend. Illegale

kansspelen en gokken op het internet (bijvoorbeeld het online casino) is één van de groeiindustrieën

op internet' .

Relevante wetsartikelen zijn:

Artikel 1 Wks: wet op de kansspelen

Artikel 1a Wks: piramidespelen

———————————————————————————--

E-fraude.

'De essentie van fraude is steeds dezelfde: mensen eigenen zich middels bedrog geld of vermogensbestanddelen toe waarop ze geen recht hebben en tasten daardoor de rechten van anderen aan. Er zijn verschillende begrippen in omloop om de cybervorm van fraude te beschrijven, zoals fraude in e-commerce en internetfraude . 'Bij deze vorm van fraude wordt het internet gebruikt om op oneigenlijke wijze gelden, goederen en diensten te verkrijgen zonder daarvoor te betalen of tegenprestaties te leveren' .

Bij internetfraude wordt er al snel gedacht aan oplichtingen via verkoopsites op internet zoals marktplaats en e-bay. Wij gebruiken de term 'e-fraude' als overkoepelende term. E-fraude is bedrog met als oogmerk het behalen van financieel gewin waarbij ICT essentieel is voor de uitvoering. Fraude staat niet als zodanig in de wet genoemd. Relevante wetsartikelen uit het wetboek van strafrecht zijn:

Artikel 326 WvSr: oplichting.

Artikel 225 WvSr: valsheid in geschrifte.

Artikel 231b WvSr: identiteitsfraude

Artikel 310 WvSr: diefstal.

Artikel 321 WvSr: verduistering.

Artikel 416 WvSr: heling.

———————————————————————————

Index