Jaargang 2 Juli 2018

Veilig Digitaal Magazine



Helft Nederlanders maakt gebruik van onveilig WIFI network

Windows 10 beschermt bestanden tegen ransomware

Online seksueel misbruik groeiend probleem

Half miljoen routers besmet met gevaarlijke malware

Hoe Telegram de gedoodverfde opvolger van het dark web werd

Politie meldt grote toename van ongebruikelijke transacties met cryptomunten

Privacywetgeving in de public cloud: hoe zit dat?

www.veiligdigitaal.com

INDEX

PGP-encryptie e-mails kwetsbaar door beveiligingslek

Slachtofferschap in een gedigitaliseerde samenlenving

Politie meldt grote toename van ongebruikelijke transacties met cryptomunten

Online seksueel misbruik groeiend probleem

Hoe Telegram de gedoodverfde opvolger van het dark web werd

Half miljoen routers besmet met gevaarlijke malware

Agentschap Telecom waarschuwt voor hackbare apparaten

Privacywetgeving in de public cloud: hoe zit dat?

Windows 10 beschermt bestanden tegen ransomware

Helft Nederlanders maakt gebruik van onveilig WIFI netwerk

Cybercrime is een probleem dat we met z'n allen moeten aanpakken

Politie accepteert beledigen op internet niet meer

Juridische commissie EU stemt voor 'uploadfilter'

Snelle weergave macOS lekt versleutelde gegevens

Ook als je Facebook niet gebruikt, kun je je data opvragen

Regering hoeft van rechter huidige 'aftapwet' niet te schrappen

Veilig Digitaal Magazine is een uitgave van veiligdigitaal.com

Ga naar de Facebookpagina

Ga naar de website

Rubrieken:

- Cops in Cyberspace
- Rechtspraak
- Verschijningsvorm cybercrime
- Wetsartikel
- Video

PGP-encryptie e-mails kwetsbaar door beveiligingslek

De PGP-encryptie die vaak wordt gebruikt om e-mails beveiligd te versturen, zou kwetsbaar zijn door een breed beveiligingslek. Dat concluderen beveiligingsonderzoekers.

Op dinsdag 15 mei werd een verslag gepubliceerd waarin de kwetsbaarheid wordt omschreven, maar belangenorganisatie Electronic Frontier Foundation (EFF) had het lek al ingezien en waarschuwde gebruikers om zo spoedig mogelijk te stoppen met het gebruik van PGP.
PGP staat voor Pretty Good Privacy. Bij de encryptiemethode wisselen de ontvanger en verzender van mails unieke digitale sleutels uit. Alleen de bezitters van deze sleutels kunnen dan de inhoud van een mail lezen.

Volgens de EFF is het riskant om e-mails met PGP te lezen en te versturen. Ze raden gebruikers aan om tijdelijk een andere versleutelde vorm van communicatie te gebruiken, zoals de chatdienst Signal.

Ennetcom
Het Nederlandse OM kraakte afgelopen jaar 3,6 miljoen versleutelde berichten van het Nederlandse bedrijf Ennetcom, waarbij ook PGP werd gebruikt ter versleuteling. De politie had op een niet nader genoemde wijze de encryptiesleutels bemachtigd. De berichten waren afkomstig van een bedrijf dat BlackBerry-telefoons met PGP-encryptie aan criminelen verkocht.

Slachtofferschap in een gedigitaliseerde samenlenving

In opdracht van het WODC is het NSCR een onderzoek gestart naar slachtoffers van online criminaliteit. Het onderzoek kijkt naar de financiële en psychologische impact van deze snelgroeiende vorm van criminaliteit en naar de behoeftes van slachtoffers.

Online criminaliteit is een nieuwe en diffuse vorm van criminaliteit. Reden voor het Ministerie van Justitie en Veiligheid om te laten onderzoeken of het slachtofferbeleid hierop moet worden aangepast. Want wat is de impact van online criminaliteit op slachtoffers? Wat zijn hun behoeftes ten aanzien van politie en justitie? En hoe kijken medewerkers van politie en justitie aan tegen slachtoffers van online criminaliteit?

Online criminaliteit ongrijpbaar

NSCR-onderzoekers Rutger Leukfeldt, Marijke Malsch en Raoul Notté voeren het onderzoek uit. Rutger, die eerder al een Veni-beurs ontving voor het onderzoeksproject De offline kant van cybercriminaliteit: 'Online criminaliteit kán anders van aard zijn. Dader en slachtoffer hoeven elkaar bijvoorbeeld niet te zien en de schaal waarop het gebeurt kan veel groter zijn. Dat maakt online criminaliteit voor slachtoffers ongrijpbaar.'

Gedigitaliseerde traditionele criminaliteit

Het onderzoek richt zich op 'nieuwe' delicten zoals hacken en ransomware, en op gedigitaliseerde 'traditionele' criminaliteit zoals fraude, interpersoonlijke delicten en zedendelicten. Rutger: 'Online delicten zijn inmiddels een veelvoorkomend probleem. In Nederland zijn er jaarlijks al meer slachtoffers van hacken dan van fietsendiefstal. Ook zie je dat online oplichting, bedreiging en stalking steeds vaker voorkomen. De vraag is of politie en justitie die online varianten van traditionele delicten wel serieus genoeg nemen. Op het eerste gezicht lijkt een online delict soms niet zo erg, maar we weten uit onderzoek dat de impact op iemands leven enorm kan zijn.'

Mogelijk aanpassing slachtofferbeleid

Om een goed overzicht te krijgen, gaat het onderzoeksteam ook praten met politie en justitie. Rutger: 'Als zo'n zaak binnenkomt, wat gebeurt er dan en waarom? We zien nu dat de aangiftebereidheid bij slachtoffers laag is. Hoe komt dat en wat kunnen we daaraan doen? Op basis van de resultaten van het onderzoek zullen wij een aantal scenario's schetsen. Deze geven het WODC inzicht in de vraag of het bestaande slachtofferbeleid moet worden aangepast als het gaat om online criminaliteit.'

Het onderzoek Slachtofferschap in een gedigitaliseerde samenleving. Op weg naar een herijking van het slachtofferbeleid? wordt november 2018 afgerond. Raoul Notté is naast zijn werk bij het NSCR ook onderzoeker bij de Haagse Hogeschool, waar vorig jaar het Lectoraat Cybercrime in het MKB is gestart. Onder leiding van Rutger Leukfeldt richt het lectoraat zich op drie onderzoekslijnen: de digitale weerbaarheid van MKB-ers, inzicht in cybercriminaliteit en de aanpak van cybercriminaliteit gericht op MKB'ers. Doel van het lectoraat is wetenschap en onderzoek direct te koppelen aan de praktijk.

Politie meldt grote toename van ongebruikelijke transacties met cryptomunten

In 2017 verklaarde de Financial Intelligence Unit Nederland (de FIU-Nederland) aan de hand van analyse en onderzoek 40.546 transacties met een totale waarde van bijna 6.7 miljard euro verdacht, het hoogste bedrag sinds de oprichting.

Witwassen door het gebruik van cryptocurrencies

De FIU-Nederland zag in 2017 het gebruik van cryptocurrencies toenemen. Het aantal meldingen van ongebruikelijke transacties gerelateerd aan cryptocurrencies steeg over de laatste vijf jaar van 300 in 2013 naar circa 5000 in 2017.

De wereldwijde toenemende mate van aandacht voor dit onderwerp kan er aan hebben bijgedragen dat er in 2017 meer onderzoek op dit onderwerp werd verricht. Mede doordat meldende instellingen zoals payment service providers en banken steeds meer grip krijgen op het herkennen van ongebruikelijke cryptocurrency-gerelateerde transacties neemt het aantal meldingen van ongebruikelijke transacties op dit gebied de laatste jaren toe.
De FIU-Nederland waarschuwt daarbij dat de toename van het aantal meldingen niet per definitie hoeft te duiden op een algehele criminalisering ten aanzien van cryptocurrencies.

Terrorismefinanciering
In 2017 werden 3.139 transacties door de FIU-Nederland verdacht verklaard op basis van een mogelijk verband met het financieren van terrorisme, onderzoeken naar contraterrorisme of een verbinding met een uitreis naar gebieden waar Islamitische Staat actief was.
Ook zag de FIU-Nederland dat bij het analyseren van aan terrorisme geassocieerde transacties, dat er in sommige gevallen sprake was van geldstromen die ook te maken hadden met andere criminele activiteiten.

Online seksueel misbruik groeiend probleem

Het aantal gevallen van online seksueel misbruik stijgt en daders zijn moeilijk op te sporen. In het eerste kwartaal van 2018 zijn al 477 meldingen gedaan van misbruik via internet, zo blijkt uit onderzoek van Reporter Radio. Er komen nieuwe wetten aan op wraakporno, maar gaat ook de pakkans van daders omhoog?

Sexting

Met een populair woord heet het versturen van naaktfoto's en -video's sexting. Uit onderzoek van Rutgers blijkt dat één op de acht jongeren onder de 25 jaar dat weleens heeft gedaan. Ondertussen ziet hulporganisatie Helpwanted dat het aantal gevallen van online seksueel misbruik al jaren stijgt. In 2010 werden er 327 meldingen gedaan, de cijfers uit het eerste kwartaal van 2018 beloven een totaalaantal van maar liefst 1.900 meldingen.

Online seksueel misbruik kent verschillende vormen. De meest bekende vorm is het verspreiden van naaktbeelden zonder toestemming (ook wel wraakporno). Dat overkwam ook Chantal uit Werkendam. Een video van haar kwam via een nepaccount op Facebook terecht, waarna het massaal werd gedeeld.

Daders ongrijpbaar

De zaak van Chantal (2015) laat zien hoe moeilijk het is om daders van online seksueel misbruik op te sporen. Om erachter te komen wie de plaatser van haar filmpje was, vroeg Chantal aan Facebook informatie. Die wilde Facebook niet geven. Chantal spande een zaak aan tegen Facebook, en won. Maar een dader vond ze nooit.

Via nepaccounts op sociale media is het bijvoorbeeld vrij gemakkelijk om als dader geen sporen achter te laten. Als er al een dader wordt gepakt, is de veroordeling bovendien mild. Daders van wraakporno worden, mits het slachtoffer volwassen is, berecht op smaad en laster. "Die wetten komen uit de prehistorie", kaart gespecialiseerd advocaat Thomas van Vugt aan. Van Vugt stond Chantal bij in haar zaak tegen Facebook.

Nieuwe wetten

Naar aanleiding van Chantals' en soortgelijke zaken werden strengere wetten aangekondigd tegen wraakporno. De strafbaarstelling van wraakporno werd zelfs opgenomen in het jongste regeerakkoord en op 16 mei kondigde minister Ferd Grapperhaus van Justitie en Veiligheid aan dat er zwaardere straffenmogelijk worden - tot twee jaar celstraf. Daarmee wordt wraakporno expliciet strafbaar. Het plan van Grapperhaus sluit aan op de wet computercriminaliteit III, waarin vast wordt gelegd dat de politie meer middelen krijgt om daders op te sporen. Die wet ligt op dit moment in de Eerste Kamer.

De nieuwe wetten passen bij de groeiende (politieke) aandacht voor online seksueel misbruik. Zestien jaar na de eerste zaak van wraakporno in Nederland, die van Francien Regelink, lijkt er verandering te komen in de opsporing en berechting van daders.

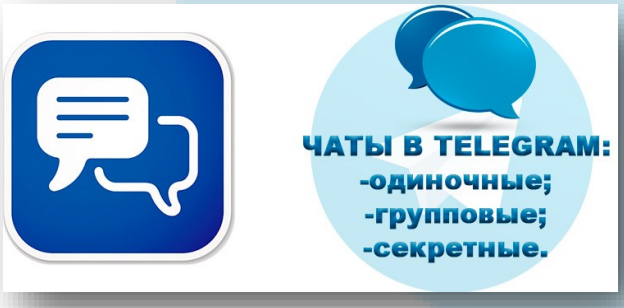
Hoe Telegram de gedoodverfde opvolger van het dark web werd

Het dark web is een broedplaats voor illegale activiteiten. Van wapenverkoop tot Ransomware-as-a-Service: kopers en verkopers gebruiken de duistere kant van het internet om zowel kennis als producten uit te wisselen.

Het dark web is echter niet meer de veilige haven die het vroeger was. Vorig jaar haalden succesvolle acties van Europese en Amerikaanse politiediensten tegen de populaire marktplaatsen Hansa Market en Alpha Bay de internationale krantenkoppen.
De overwinning van de veiligheidsdiensten is niets meer dan de recentste zet in een voortdurend kat- en muisspel. Ons onderzoeksteam ontdekte dat cybercriminelen zich in de nasleep van de actie verplaatst hebben naar nieuwe kanalen in een poging internationale overheden opnieuw een stapje voor te zijn. Ze lijken vooral de mobiele berichtenapplicatie Telegram te omarmen.

De overstap naar Telegram
Op het dark web zijn vooral hacking forums populaire platformen waarop criminelen vacatures posten, hun producten aanbieden en zelfs overleggen met elkaar.
De afgelopen jaren gaan veiligheidsdiensten steeds beter om met de uitdagingen van het dark web, waardoor ze meer greep kregen op de forums en sommige grote namen zelfs offline werden gehaald. De migratie van criminele activiteiten naar geheimere maar ook eenvoudiger toegankelijke platformen is daar een direct resultaat van.
De versleutelde chat-applicatie Telegram werd in 2013 gelanceerd. Na een servercrash bij concurrent WhatsApp zag Telegram zijn aantal gebruikers met vijf miljoen in de hoogte schieten in amper 24 uur tijd.
Net als bij WhatsApp kunnen Telegramgebruikers zowel individueel chatten als in groepsgesprekken met elkaar praten. Telegram draagt beveiliging erg hoog in het vaandel, waardoor sommige groepsgesprekken handige alternatieven zijn geworden voor de geheime fora op het dark web.

Communiceren via kanalen
Een bepaald type groepschat gaat door het leven onder de noemer ‘channel’. Administrators van zo’n kanaal kunnen dat gebruiken om berichten te verzenden naar een ongelimiteerde hoeveelheid abonnees. Alle verzonden berichten zijn zichtbaar, maar de eventuele antwoorden gestuurd door de ontvangers zijn wel privé. De discretie inherent aan dergelijke kanalen maakt hen ideaal om illegale intenties te verbergen.



De kanalen zijn een functie die je niet bij WhatsApp terugvindt. Groepsgesprekken of 'broadcasts' bevatten daar maximaal 250 deelnemers, die enkel op uitnodiging kunnen toetreden. Dat nuanceverschil maakt dat Telegram, erg populair in Rusland, momenteel kop van jut is. De Russische regering heeft de app zelfs helemaal verboden, en toonde zich al bereid delen van het internet ontoegankelijk te maken om het verbod op de applicatie te handhaven.

Iemand met criminele ambities kan een aanbod lanceren via een kanaal en vervolgens een privéconversatie starten met end-to-end encryptie. Dat is veiliger dan de voor iedereen zichtbare forumgesprekken op het dark web. In het verleden moest je verschillende stappen ondernemen om anoniem te zijn op het dark web, via onder andere het TOR-platform. Vandaag kan iedere Telegramgebruiker zich met één druk op de knop abonneren op een kanaal via zijn smartphone, terwijl zijn of haar identiteit helemaal verborgen blijft.

Rekruteren en vervalsen

Ons team ontdekte verschillende clandestiene kanalen waaronder 'Dark Jobs', 'Dark Work', en 'Black Markets', al zijn er veel meer. Kanalen zoals Dark Jobs bevatten doorgaans vacatures voor crimineel werk, maar worden ook gebruikt om bijvoorbeeld gestolen documenten of hacking-tools aan te prijzen aan potentiële kopers. De aanpak werkt de groei van cybercriminaliteit in de hand, aangezien de vacatures en tools ook worden aangeboden aan onervaren gebruikers, wat op het dark web veel minder het geval was. De interessantste berichten zijn misschien wel diegene waarin criminelen op zoek gaan naar werknemers van bepaalde bedrijven of banken. Ze kunnen toegang tot de werknemers misbruiken om vertrouwelijke informatie te bemachtigen, die vervolgens verkocht kan worden. Dergelijke gegevens zijn ook nuttig om een cyberaanval van binnenuit op te zetten. Wat geldt in de echte wereld, is ook waar voor cybercriminelen: niet wat je kent is het belangrijkst, wel wie je kent.

Documentvervalsing is een andere populaire dienst die via Telegramkanalen wordt aangeboden. Vervalsing van onder andere identiteitskaarten, paspoorten en bankdocumenten behoort tot de mogelijkheden. De auteur van één van de posts claimde zelfs connecties te hebben bij de Russische verkeerspolitie, en zou in staat zijn rijbewijzen in categorieën naar keuze af te leveren.

Het gemak van Telegramkanalen laat cybercriminelen toe om veiliger en eenvoudiger dan ooit met elkaar te praten. Hoewel berichtenapps een integraal onderdeel van het moderne samenleven zijn, wordt de beveiliging die bedoeld is om de privacy van legitieme gebruikers te garanderen, misbruikt door misdadigers. Hierdoor is de toegang tot malware en andere malafide producten eenvoudiger dan ooit. Het hoeft dan ook niet te verwonderen dat het aantal cyberaanvallen op zowel organisaties als mensen blijft groeien.

Consumentenbond verliest weer inzake update-beleid Samsung

Voor de tweede keer heeft een rechtbank de eis Consumentenbond afgewezen, die stelt dat Samsung te weinig doet om zijn toestellen veilig te houden.

De consumentenorganisatie verwijt het bedrijf al jaren gebruikers onvoldoende ondersteuning te bieden op het gebied van updates voor besturingssysteem Android, met volgens de bond onveilige toestellen als gevolg.

De organisatie vindt dat de toestellen tot ten minste twee jaar na verkoop aan een klant en tot vier jaar na introductie op de Nederlandse markt softwarematig moeten worden ondersteund. Samsung beperkt zich tot ten minste twee jaar na introductie. De updates stoppen niet per se na die twee jaar, maar het bedrijf garandeert het niet meer.

Niet concreet en overtuigend

Volgens de rechter heeft de Consumentenbond onvoldoende duidelijk gemaakt waar er daadwerkelijk sprake is van een veiligheidsrisico. Ook heeft de bond niet goed aangetoond waarom Samsung sneller zou moeten updaten en dat het bedrijf ten onrechte updates achterwege laat bij bepaalde toestellen. "De door de Consumentenbond overlegde stukken zijn weinig specifiek en bieden, gegeven de technische toelichting door Samsung, geen van alle concrete en overtuigende aanknopingspunten voor een andersluidend oordeel", schrijft de rechtbank.

De eis van de bond om tot vier jaar na introductie telefoons softwarematig te ondersteunen, is door de rechtbank ook weerlegd. De rechter zegt in de uitspraak dat het deels gaat om zaken die zich in de toekomst afspelen, namelijk updates van nog niet bedachte of aangekondigde producten, en daar kan geen uitsprak over worden gedaan.

Risico's

Daarnaast verweet de Consumentenbond Samsung klanten onvoldoende te informeren over de risico's van onveilige telefoons. Ook op dat vlak geeft de rechtbank Samsung gelijk: het bedrijf biedt op zijn site voldoende informatie aan, luidt het oordeel. Daarnaast vindt de rechtbank dat van consumenten mag worden verwacht dat die verschafte informatie op waarde kan schatten en zo nodig extra informatie kan opvragen.

"Wij zijn verheugd over deze uitspraak", zegt Gert Jan ter Haar, hoofd technisch productmanagement van Samsung Nederland in een persverklaring. "Het vonnis onderstreept dat onze aanpak werkt om smartphones veilig te houden."

De Consumentenbond is teleurgesteld in de uitspraak: "Samsung krijgt de ruimte om zich te verschuilen achter een veelheid aan modellen en technische en economische afwegingen", zegt directeur Bart Combée. "Maar Samsung kiest er zelf voor zoveel modellen op de markt te brengen, er is niemand die ze daartoe dwingt."

Kort geding

In maart 2016 verloor de Consumentenbond in een kort geding over dit onderwerp ook van Samsung. De Amsterdamse rechter zei toen dat de zaak geen spoedeisend belang had en de dat de financiële gevolgen voor Samsung, als het telefoons veel langer van updates moet voorzien, 'enorm' zijn. De Consumentenbond startte vervolgens de bodemprocedure, met deze uitspraak tot gevolg.

Half miljoen routers besmet met gevaarlijke malware

Toestellen van onder andere Linksys, Netgear en TP-Link zijn getroffen met de VPNfilter-malware. Het is een complex virus dat niet eenvoudig te verwijderen is.

Securityfirma Talos onthulde gisteren het bestaan van de malware VPNFilter, een malware-variant dat ondertussen zo'n 500.000 routers en NAS'en wereldwijd zou besmet hebben. Tot nu toe heeft Talos, dat een onderdeel vormt van het netwerkbedrijf Cisco, infecties bij verschillende consumentenproducten van Linksys, Netgear, MikroTik, en TP-Link vastgesteld; alsook bij de Network-Attached Storage-apparaten van QNAP. De malware kan communicatiedata verzamelen, exploits uitvoeren en heeft ook de mogelijkheid om routerhardware te beschadigen en te vernietigen.

Russische connectie

VPNFilter is een erg geavanceerd programma. Talos wijst erop dat de malware een reboot van een toestel kan overleven, een capaciteit die erg zeldzaam is bij virussen geschreven om Internet-of-Things-toestellen te infecteren. Daarnaast overlapt de gebruikte code deels met een andere beruchte malware, BlackEnergy. BlackEnergy was het programma dat in december 2016 een deel van het energienetwerk van Oekraïne platlegde, een grootschalige cyberaanval die wordt toegeschreven aan de Russische overheid.

Talos gaat niet zo ver dat het Rusland aanwijst als schuldige, maar het merkt wel op dat de malware "Oekraïense toestellen actief besmet aan een alarmerend tempo". Na het afwegen van de risico's op een nieuwe cyberaanval koos het securitybedrijf ervoor om de informatie die het nu heeft al openbaar te maken, ook al is zijn onderzoek naar VPNFilter nog niet helemaal afgerond. "We beoordelen met een hoge mate van zekerheid dat deze malware gebruikt wordt om een uitgebreide en moeilijk te identificeren infrastructuur te creëren die voor verschillende doeleinden kan ingezet worden door de groep die er achter zit," aldus Talos.

Herstarten

Omdat VPNFilter zichzelf kan maskeren is het moeilijk om een infectie vast te stellen. Daarnaast zijn routers slecht uitgerust om zich te beschermen tegen geavanceerde malware. Ze hebben vaak geen ingebouwde antivirussoftware, ze zijn moeilijk te patchen en zijn vaak rechtstreeks met het internet verbonden zonder veiligheidsmechanismes.

Talos raadt dan ook aan om alle potentieel getroffen routers en NAS'en opnieuw op te starten. Dat verwijdert de malware niet definitief, maar schakelt wel de schadelijke componenten van de software uit. Verder is het wachten op eventuele patches die routerbedrijven uitbrengen.

Talos somt de specifieke toestellen die kwetsbaar zijn voor VPNFilter op in zijn verslag, dat je hier vindt.

Agentschap Telecom waarschuwt voor hackbare apparaten

Het wordt hoog tijd dat onveilige apparaten van het internet worden geweerd, vindt het Agentschap Telecom. Het kabinet heeft ook plannen voor een keurmerk, zodat consumenten kunnen zien of zij een apparaat kopen dat veilig online kan. Maar het agentschap vindt dat dit veel te lang duurt, omdat het IoT allang een feit is.

Het Agentschap Telecom ziet het liefst een soort CE-keurmerk komen voor apparaten die via internet te bedienen zijn. Het CE-keurmerk beschermt consumenten onder meer tegen elektrische apparaten die niet voldoen aan eisen op het gebied van veiligheid. Volgens de overheidsorganisatie vormen onveilige Internet of Things-apparaten, zoals webcams en slimme thermostaten, een steeds groter probleem. Voor consumenten is het volstrekt onzichtbaar of een apparaat veilig gebruikt kan worden of niet. Er zijn apparaten die hackers heel eenvoudig toegang geven. Niet alleen tot het apparaat zelf, maar ook tot het netwerk waarop dit is aangesloten. Dit geldt ook voor sommige beveiligingscamera's.

Bedrijven aan zet

Zolang de overheid niet met een keurmerk komt, adviseert het Agentschap Telecom bedrijven om gezamenlijk een keurmerk uit te brengen. Ook adviseert de organisatie telecom- en internetproviders om op zoek te gaan naar onveilige apparaten op hun netwerken en de gebruiker daarvoor te waarschuwen. Enkele jaren geleden werden wereldwijd duizenden IP-beveiligingscamera's gehackt om er DDoS-aanvallen mee uit te voeren op grote websites. Ook worden de beelden ervan onderschept en op vage websites online gezet.

Privacywetgeving in de public cloud: hoe zit dat?

Facebook heeft in het verleden naar de seksuele geaardheid van gebruikers gevraagd en op basis van deze informatie gerichte advertenties getoond. Volgens de spelregels van de Nederlandse privacywetgeving is dit niet toegestaan. Maar wat als het Europese hoofdkantoor en datacenters in Ierland staan? Geldt de Nederlandse wetgeving dan nog wel?

De Nederlandse privacywetgeving lijkt in de meeste gevallen duidelijk: iedere in Nederland gevestigde organisatie moet zich aan de spelregels houden. Bij publieke clouddiensten met servers over de grens ontstaat echter een ingewikkelde situatie. Welke privacyspelregels gelden in de public cloud?

Bijzondere persoonsgegevens
Facebook mag volgens de Autoriteit Persoonsgegevens (AP) niet zomaar data vragen over de seksuele voorkeur van gebruikers.
Het gaat hierbij namelijk om bijzondere persoonsgegevens. Deze mogen alleen onder zeer strikte voorwaarden worden verwerkt. Het tonen van gerichte advertenties is daar in ieder geval niet een van.
Facebook verweerde zich: het Europese hoofdkantoor en de datacenters staan in Ierland, buiten het bereik van de Nederlandse wetgeving. De AP zou dus helemaal geen recht van spreken hebben.
Volgens de AP speelde de Nederlandse vestiging van het bedrijf echter een rol in het geheel, door Nederlandse bedrijven te adviseren over de advertentiemogelijkheden op het sociale netwerk. De kwestie heeft volgens de AP dus wel degelijk een Nederlands tintje.

Belangrijkste spelregels
Het laatste woord over de kwestie is nog niet gezegd. Wel is duidelijk dat privacywetgeving in de cloud niet altijd vanzelfsprekend is en jurisdictie absoluut een rol speelt. Daar dient u serieus rekening mee te houden als een cloudprovider namens u persoonsgegevens van uw klanten bewerkt.
Gelukkig zijn er ook een aantal ‘harde’ afspraken waar cloudproviders aan moeten voldoen. De public cloud is erg privacyvriendelijk, zolang providers zich houden aan een aantal spelregels van de Nederlandse privacywet. We zetten de belangrijkste op een rij:

- Bewerkersovereenkomst

Veel public clouddiensten verwerken persoonsgegevens. Niet alleen van hun klanten, maar in veel gevallen ook van de klanten van hun klanten. Denk aan een administratiekantoor dat gebruikmaakt van een SaaS-oplossing voor onlineboekhouden, of een uitgever die een abonnementenbestand bijhoudt in Office 365.
In zo’n geval is een bewerkersovereenkomst altijd verplicht. Dat is een officieel document waarin de organisatie afspraken maakt met de cloudprovider over de gegevensbewerking. De cloudprovider belooft in zo’n overeenkomst eenvoudig gezegd dat het zijn best doet de privacy van de klanten van de organisatie waarmee het de overeenkomst sluit zo goed mogelijk te beschermen. Ook maakt u in zo’n overeenkomst afspraken over verantwoordelijkheden bij een datalek.

- Serieuze beveiligingsmaatregelen

Een cloudprovider die persoonsgegevens verwerkt, is verplicht serieuze beveiligingsmaatregelen te nemen. Het gaat daarbij zowel om technische securitymaatregelen als organisatorische afspraken en procedures. Denk dus aan zaken als securitysoftware, een deugdelijke firewall, IDS/IPS, maar ook aan een duidelijk gedocumenteerd privacybeleid.

- Meldplicht richting verantwoordelijke

Een cloudleverancier moet zijn klanten direct op de hoogte brengen bij een datalek. Dus niet rechtstreeks melden bij de AP, die verantwoordelijkheid ligt bij de klant. Die is immers weer eindverantwoordelijk over de persoonsgegevens van zijn klanten, ook wanneer de cloudleverancier bewust of onbewust zijn mond houdt over het lek. Dat is direct een sterk argument om alleen met cloudleveranciers in zee te gaan met een goede staat van dienst.

- Doorgifte naar buitenland

Het kan voorkomen dat de cloudprovider data verhuist naar een land buiten de EU. Als klant moet je dat scherp in de gaten houden en harde afspraken over maken.
De privacywetgeving verbiedt namelijk het verplaatsen van persoonsgegevens naar niet-EU-landen, tenzij het land over een minstens zo hoog beschermingsniveau beschikt.
Een providerwissel kan in zo'n geval noodzakelijk zijn om aan de Nederlandse privacywetgeving te blijven voldoen. Bijvoorbeeld wanneer de data verhuizen naar een land dat weinig tot geen privacyregels kent.
Die waakzaamheid geldt overigens ook wanneer de cloudprovider toegang tot persoonsgegevens op afstand verleent aan een niet-EU-land, zoals een helpdesk in India. Ook dan kan sprake zijn van verwerking van persoonsgegevens door niet-bevoegde personen en dus een overtreding van de privacywet.

De VS: een apart geval

De Verenigde Staten zijn wat betreft de cloud een vreemde eend in de bijt. Komen data van Europese burgers terecht op Amerikaanse servers, dan vallen deze onder het Privacy Shield. Het Amerikaanse cloudbedrijf moet wel zijn aangemeld op het Privacy Shield-programma. Is dat het geval, dan mogen persoonsgegevens door hen worden verwerkt.
Het moet echter nog maar blijken hoe duurzaam deze afspraak is. De afspraak kan ieder jaar worden bijgewerkt.

De private cloud is met de enige oplettendheid absoluut geen privacyonvriendelijke plek. Goed voorwerk en duidelijke afspraken met de cloudprovider verminderen de kans op datalekken en andere ellende.

Windows 10 beschermt bestanden tegen ransomware

Slachtoffer worden van ransomware, dat wil je natuurlijk tot elke prijs voorkomen. Vanaf het komend najaar krijgen gebruikers van Windows 10 hierin steun van Microsoft. In Windows 10 komt de mogelijkheid om gebruikers te laten kiezen welke programma's wel of juist niet toegang krijgen tot bepaalde mappen. Hierdoor wordt het risico op versleutelen van cruciale bestanden door ransomware in ieder geval een stuk verminderd.

Nieuwe optie Windows Defender

In de Windows Fall Creaters Update, die waarschijnlijk in september van dit jaar wordt uitgebracht, krijgt Windows Defender, het antivirusprogramma dat standaard met Windows wordt meegeleverd, de mogelijkheid een 'controlled folder access' aan te zetten. Met deze functie wordt geregeld dat alleen bepaalde programma's toegang krijgen tot bepaalde mappen, zoals de mappen bureaublad, documenten, en dergelijke.

Eerst toestemming vragen

De nieuwe optie gaat werken met een standaardlijst, waarin de programma's staan die voldoende rechten hebben. Zodra een programma toegang probeert te krijgen tot een bepaalde map wordt gekeken of het programma in die goedgekeurde lijst staat. Als dat niet het geval is, dan krijgt de gebruiker een melding. Standaardlijsten kunnen niet worden gewijzigd, maar je kunt wel zelf applicaties toevoegen aan de lijst. Ook kun je dan extra mappen aan de lijst mappen met een beschermde status toevoegen.

Helft Nederlanders maakt gebruik van onveilig WIFI netwerk

Uit onderzoek van het CBS blijkt dat de helft van de Nederlandse bevolking toegeeft wel eens gebruik te maken van een onveilig WIFI netwerk. Vooral onder de jongeren ligt het percentage onveilige internetgebruikers hoog. Zij houden het minst risico met eventuele gevolgen op het gebied van bijvoorbeeld privacyschending.

Mogelijkheid tot gegevens bekijken

Maar liefst zeven op de tien jongeren tussen 18 en 25 jaar maken weleens gebruik van netwerken die niet beveiligd zijn. Zij houden er vaak geen rekening mee dat wanneer je je niet hoeft in te loggen met een gebruikersnaam en wachtwoord je gegevens zomaar door anderen kunnen worden bekeken. Slecht een op de tien 75-plussers neemt dit risico.

Bewust van risico

Toch is een aardig deel van de gebruikers zich wel bewust van dergelijke risico's: 34% hiervan laat weten dat het wel degelijk invloed heeft op hoe zij internet gebruiken wanneer ze op een openbaar netwerk zitten. Zij zorgen er bijvoorbeeld bewust voor dat ze geen persoonlijke gegevens openen of delen wanneer ze op een openbaar netwerk zitten om zo te voorkomen dat anderen hun gegevens kunnen bekijken.

Beveilig jouw WIFI met een VPN verbinding

Een VPN verbinding zorgt ervoor dat jij jouw informatie versleuteld verstuurt over WIFI verbindingen. Dit is bijzonder handig, maar vooral belangrijk, als je persoonlijke of belangrijke gegevens verstuurt terwijl je gebruik maakt van een publiek draadloos netwerk zoals WIFI verbindingen. Iets waar iedereen tegenwoordig geregeld gebruik van maakt op bijvoorbeeld stations, cafe's, hotels, flexwerkplekken, bibliotheken enzovoort.

Bron: CBS

Cybercrime is een probleem dat we met z'n allen moeten aanpakken

Hij zei het onlangs ook in een mooi artikel in Tijdschrift voor de Politie en nu ook in de Volkskrant: of het nu gaat om kinderpornonetwerken en identiteitsfraude of om virussen die je computer kapen, digitaal is de politie 'nog steeds niet bij de tijd'.

Volgens professor Wouter Stol, lector Cybersafety en bijzonder hoogleraar Politiestudies aan de OU, zijn er op zestigduizend politiemensen maar een paar honderd digitaal specialisten.

De rest heeft volgens hem nauwelijks een idee van wat er allemaal speelt op digitaal gebied. 'Die kunnen dus ook niet optreden wanneer er in de eigen omgeving digitale criminaliteit plaatsvindt'.

Zorgwekkend, vindt Stol, die een teamchef onlangs hoorde zeggen dat het darkweb 'veel te gevaarlijk was' voor een wijkagent. Terwijl die wijkagent natuurlijk móet weten wat er in zijn (digitale) wijk gebeurt. 'Laatst kwam mijn vrouw thuis met een verhaal over een buurjongen die zonder enig probleem een stapel valse biljetten van 20 euro had gekocht. Hoe kunnen politiemensen daar adequaat op reageren, als ze geen idee hebben hoe het werkt?' Volgens Stol moet de politie dáár zijn waar het gevaarlijk is, dus ook op het darkweb.

Hij bepleit daarom een bredere aanpak van cybercrime, niet alleen omdat politie en justitie er te weinig kennis van hebben maar ook omdat het probleem ook sociologische en psychologische invalshoeken heeft. 'Cybercrime is een probleem dat we met z'n allen moeten aanpakken', misschien wel op de manier waarop Nederland de afgelopen decennia het aantal verkeersdoden heeft weten te verkleinen. Dan wordt 'digitaal' een normaal en integraal onderdeel van de politieorganisatie.

'De politie moet zich sneller aanpassen aan de digitalisering van de samenleving en ze kan dus niet volstaan met het draaien van meer cybercrimezaken. Zij moet verlangen dat alle medewerkers digitale mogelijkheden benutten bij al hun zaken en andere taken'.



Politie accepteert beledigen op internet niet meer

De politie in de Achterhoek gaat harder optreden tegen mensen die agenten online uitschelden.

Die scheldpartijen variëren van ‘vrij onschuldig vloeken’ tot het toewensen van ‘de meest vreselijke ziektes en racisme’, zegt operationeel specialist Harry van Olst.

‘Soms zeggen dat ze het grappig bedoeld hebben, maar wij kunnen er niet om lachen’.
Afgelopen week nog werd een jongen (18, uit Doetinchem) door de politie thuis opgehaald voor een goed gesprek omdat hij de politie grof beledigd had op facebook. ‘Dat ging over de seksuele geaardheid van politiemedewerkers. En het was echt gericht op agenten’, aldus een woordvoerder. T

oen de jongen, uitgenodigd om op bureau te verschijnen, schreef dat hij daar geen tijd voor had, is hij, na toestemming van de officier van justitie, thuis opgehaald.

Volgens Van Olst maakt de politie door zo streng op te treden duidelijk dat zulke beledigingen via sociale media niet worden geaccepteerd.

Juridische commissie EU stemt voor 'uploadfilter'

De juridische commissie van het Europees Parlement heeft woensdagochtend voor een zogenoemd 'uploadfilter' gestemd. Internetplatformen zoals Facebook en YouTube moeten volgens de nieuwe regels controleren of materiaal dat door hun gebruikers wordt geüpload, overeenkomt met auteursrechtelijk beschermd werk. Is dat het geval, dan moeten zij de upload van het materiaal tegenhouden.

De maatregel valt onder een breder pakket aan copyrightregels die voor de Europese Unie moet gaan gelden. Met de nieuwe regels wil Brussel makers van auteursrechtelijk beschermd materiaal beter beschermen voor het illegaal delen van hun werk op het internet.

De nieuwe regels verplichten internetplatformen die 'grote hoeveelheden werk bewaren en beschikbaar stellen' om 'passende maatregelen' te nemen tegen auteursrechtelijk beschermd materiaal dat illegaal wordt geüpload.

Tegenstanders van de maatregel spreken van een 'uploadfilter'. Zij vrezen dat de algoritmes die auteursrechtelijk beschermd materiaal moeten herkennen, in de praktijk ook rechtmatig geüpload werk gaan tegenhouden.

Voordat de copyrightregels van kracht worden, moeten het voltallige Europees Parlement en de Europese lidstaten er nog akkoord mee gaan. Het Europees Parlement stemt begin juli over het voorstel.

Snelle weergave macOS lekt versleutelde gegevens

De Snelle weergave-functie op de Mac kan via de cache versleutelde gegevens openbaar maken. Iemand met toegang tot je systeem kan daardoor versleutelde informatie bekijken. De techniek zou al langer gebruikt worden door forensische instanties.

De Snelle weergave, in het Engels Quick Look, is een handige functie op je Mac waarmee je bestanden al kunt bekijken voordat ze geopend worden. Het enige wat je hoeft te doen is een bestand selecteren en vervolgens op de spatiebalk drukken. In macOS Mojave breidt Apple de Snelle weergave verder uit. Je kunt dan meer bewerkingen uitvoeren, zoals afbeeldingen bewerken of tekst uitvoeren, ook zonder het bijbehorende programma te openen. Nu hebben twee beveiligingsonderzoekers een lek ontdekt, waardoor versleutelde gegevens zichtbaar zijn.

Beveiligingsonderzoekers Patrick Wardle en Wojciech Reguła hebben dit probleem ontdekt. In een blogpostleggen zij uit hoe dat komt. Het komt erop neer dat de Snelle weergave een thumbnail van het bestand opslaat, zelfs als het bestand versleuteld is. De thumbnails worden in de cache opgeslagen en zijn via daar te benaderen, ook als het origineel verwijderd is. In de blogpost laat Wardle zien hoe een foto van Luke Skywalker te achterhalen is. Deze techniek werkt zelfs bij bestanden in de APFS-container waar een extra wachtwoord op zit.

Op deze manier kunnen versleutelde foto's dus zichtbaar gemaakt worden, al zijn ze wel kleiner dan de originele afbeeldingen. Behalve voor foto's werkt dit ook met tekstbestanden, zo laat Wardle zien. Volgens de onderzoekers is het niet zo eenvoudig om de gegevens te zien als de Mac uitgeschakeld is, omdat de schijf van een Mac zelf versleuteld is. Maar als iemand toegang heeft tot een ingeschakeld systeem, is het een ander verhaal. Denk bijvoorbeeld aan instanties die je computer in handen krijgen.

Of Apple ook op de hoogte gebracht is, blijkt niet uit de blogpost. Ben je bang dat versleutelde gegevens via deze manier te achterhalen zijn, dan kun je het beste handmatig de cache van de Snelle weergave legen.

Ook als je Facebook niet gebruikt, kun je je data opvragen

Ook mensen die geen account hebben op Facebook, kunnen bij het sociale medium aankloppen om gegevens op te vragen die het bedrijf over hen verzamelt.

Dat meldt Facebook in de eerste reeks van antwoorden op vragen die dinsdag in het Europees Parlement onbeantwoord bleven.
"Als je Facebook niet gebruikt, kun je informatie die we over jou verzamelen opvragen via een formulier in het helpcentrum van Facebook", schrijft het sociale medium. Het bedrijf benadrukt dat mensen moeten specificeren naar welke gegevens zij op zoek zijn.
Schaduwprofielen

Met de antwoorden reageert Facebook op vragen over zogenaamde 'schaduwprofielen': het verzamelen en verwerken van gegevens door internetgebruikers die geen Facebook-account hebben of niet met hun account zijn ingelogd.
"Elke website of app die je bezoekt moet bepaalde informatie verzamelen om ervoor te zorgen dat de dienst goed werkt. Facebook is daarop geen uitzondering", schrijft het bedrijf.
"Bovendien versturen websites die onze diensten gebruiken - zoals het plaatsen van een like-knop of de mogelijkheid om met Facebook in te loggen - informatie naar Facebook wanneer je die sites bezoekt."

Facebook zegt dat het bedrijf informatie van niet-ingelogde gebruikers niet gebruikt om 'schaduwprofielen' op te stellen. Het bedrijf schrijft in de antwoorden op vragen dat niet-ingelogde internetgebruikers op websites van derden geen gepersonaliseerde advertenties of andere gepersonaliseerde content te zien krijgen.

Cookie
Dit komt niet overeen met wat Facebook in zijn helpcentrum over gegevens van niet-ingelogde gebruikers schrijft. Daarin staat dat Facebook een zogenaamde cookie verstuurt naar gebruikers met een Facebook-account, maar ook naar internetgebruikers die de website van Facebook hebben bezocht.

Zodra de gebruiker vervolgens een website met bijvoorbeeld een like-knop bezoekt, ontvangt Facebook informatie over die cookie. Volgens het helpcentrum gebruikt het bedrijf die informatie onder meer om "je een gepersonaliseerde ervaring op zowel die site als op Facebook te bieden". De gegevens die Facebook via die cookie verzamelt, worden volgens het sociale medium binnen negentig dagen verwijderd of geanonimiseerd.

Steeds meer 'hidden tunnels' in gebruik

Cybercriminelen bouwen in toenemende mate aan een netwerk van 'verborgen tunnels' om geavanceerde command and control (C&C) aanvallen uit te voeren tegen banken en andere financiële instellingen. Doel is om persoonsgegevens te stelen, aldus een nieuw industrieonderzoek.

Hoewel dit soort aanvallen niet nieuw zijn, zijn zij zeer populair geworden sinds de Equifax-breach van 2017. Bij deze aanval werden meer dan 146 miljoen persoonlijke gegevens buit gemaakt. Daarmee was de breach een van de grootste datalekken in de geschiedenis waarbij persoonlijke data is gestolen.

Onontdekt

Wat de situatie zo mogelijk nog ernstiger maakt, is het feit dat de meeste van deze aanvallen pas na vele maanden ontdekt worden, aldus het rapport 'Spotlight Report on Financial Services"' dat de security-bedrijf Vectra op 20 juni publiceerde. Met behulp van haar eigen software voor het opsporen en bestrijden van bedreigingen verzamelde Vectra tussen augustus 2017 en januari van dit jaar metadata en netwerkverkeer van 4,5 miljoen apparaten bij banken, financiële instellingen en andere ondernemingen.

In een toelichting zegt Will LaSala, Director Security Solutions en security evangelist bij OneSpan (het voormalige Vasco): "Hidden tunnels dienen te allen tijde te worden beschermd. Veel app-ontwikkelaars zetten poorten in firewalls open om services makkelijker toegankelijk te maken vanaf hun apps. Maar diezelfde poorten kunnen hierdoor ook door cybercriminelen worden uitgebuit."

Automatisch

Met behulp van de juiste ontwikkelingstools kunnen app-ontwikkelaars de gegevens die door deze gaten echter versleutelen, stelt LaSala. "Soms hebben ontwikkelaars haast om een nieuwe functie te implementeren. Bijvoorbeeld om klanten te behouden of om de business te laten groeien. Dan kan dit leiden tot situaties waar een verborgen tunnel wordt gemaakt en niet beveiligd. Door gebruik te maken van ontwikkeltools die een automatisch een beveiligde tunnel toepast, kunnen developers beginnen met een solide fundament voor hun app creëren."

Secure Communications API's maken het voor een developer mogelijk om hun gegevens te versleutelen binnen hun applicatie voordat de netwerklaag wordt toegepast, die vaak apps beschermt tegen de injectie van een kwaadaardige backdoors. "Door het toepassen van Application Shielding-technieken kan de applicatie vaak nog verder worden 'gehard' tegen aanvallen.

Een gelaagde beveiliging van applicaties kan niet alleen huidige aanvallen tegenhouden, zoals de kwaadaardige 'malicious hidden tunnels', maar kan ook vaak voorkomen dat nieuwe aanvallen worden geprobeerd tegen een beschermde app", aldus LaSala.

Regering hoeft van rechter huidige 'aftapwet' niet te schrappen

Dat heeft de rechter bepaald na een kort geding. Een groep privacyinstanties en bedrijven stapte recent naar de rechter om het kort geding aan te spannen. Zij vinden dat de Wet op de inlichtingen- en veiligheidsdiensten (Wiv), ook wel de aftapwet of sleepwet genoemd, niet in zijn huidige vorm ingevoerd mocht worden.

De wet die op 1 mei in werking trad, bevat nog niet de beloofde wijzigingen. Daar wordt alleen in extra documentatie naar verwezen. Volgens de regering is dat voldoende, maar de aanklagers vinden het reden om de wet te schrappen tot de aanpassingen wel in de wetstekst zijn.

"Dat de regering wel aankondigt de wet te willen wijzigen, maar het woord nog niet bij daad voegt en de wet al wel invoert, doet geen recht aan de uitslag van het referendum", aldus Hans de Zwart, directeur van belangenorganisatie Bits of Freedom. "De wet had eerst gewijzigd moeten worden. Dat is belangrijk, omdat de Tweede en de Eerste Kamer recht kunnen doen aan de zorgen van de burger"

Het samenwerkingsverbond van aanklagers gaat op korte termijn bespreken of ze juridische vervolgstappen willen nemen.

Tijdens een referendum over de Wiv zei een meerderheid van de Nederlanders tegen de wet te zijn. De regering beloofde daarom een aantal aanpassingen te maken.

De sleepwetfunctie binnen de wet wordt bijvoorbeeld ingeperkt. Daarnaast is de bewaartermijn van drie jaar gewijzigd naar één jaar met twee verlengmogelijkheden van ieder een jaar.

Cyberspace

De politie heeft de MacBook Pro van een verdachte die met een wachtwoord was beveiligd weten te ontgrendelen door middel van een wachtwoord dat op de iPhone van de verdachte werd aangetroffen. Dat blijkt uit het vonnis van de rechtbank Midden-Nederland. De 29-jarige verdachte uit Geldrop werd vandaag voor het maken en bezitten van kinderporno veroordeeld tot een gevangenisstraf van 4 jaar, waarvan 1 jaar voorwaardelijk.

———————————————

Het aantal door de politie uitgevoerde telefoon- en internettaps is vorig jaar nagenoeg gelijk gebleven ten opzichte van 2016 en 2015, zo blijkt uit het Jaarverslag van het ministerie van Veiligheid en Justitie. Vorig jaar werd er voor bijna 25.000 nummers een bevel tot aftappen gegeven.

———————————————

Bij het OM moeten 'grote stappen' gezet worden om de digitale misdaad adequaat te kunnen bestrijden, schrijft het parket in het jaaroverzicht 2017. Doelgerichte computercriminaliteit kan op dit moment niet effectief worden aangepakt. Daarvoor is 'meer capaciteit, kennis en expertise nodig', aldus OM-woordvoerder Bart Vis. In 2017 kreeg het OM 231 zaken rond computercriminaliteit. Slechts 71 zaken kwamen voor de rechter, waarvan in 60 zaken een veroordeling volgde. Jaarlijks is 26 miljoen euro beschikbaar voor de aanpak van digitale misdaad. Het OM vindt dat te weinig.

———————————————

De politie heeft twee mannen (18 en 32, uit Groningen) opgepakt die een vrouw zouden hebben afgeperst. Bij een inbraak zouden ze de computer van de vrouw hebben gestolen. Daarop gevonden naaktfoto's dreigden ze openbaar te maken, als de vrouw (29, uit Amsterdam) niet betaalde. De vrouw werd via facebook benaderd door een van de verdachten. 'Ik weet wie je pc heeft'. Ze zou die terug krijgen als ze betaalde voor de (acht jaar oude) foto's. De vrouw stapte naar de politie en maakte een afspraak met de dieven. Die werden onderweg aangehouden. De vrouw heeft inmiddels aangifte tegen de twee gedaan.

———————————————

Toen medewerkers van de 'intelafdeling van de recherche' in Rotterdam een online advertentie vonden waarin vuurwapens werden aangeboden, werd een groot onderzoek gestart. Dat leidde naar een verdachte (35) in Waddinxveen. Bij een inval in diens woning werden zes vuurwapens, twee luchtdrukwapens en een imitatiewapen gevonden. De man is aangehouden, alle wapens zijn in beslag genomen. In het pand werden ook een vervalst id-bewijs van de politie, een zwaar vest, een politiekoppel en munitie gevonden.

———————————————

De politie Assen heeft een vechtpartij tussen twee meisjes weten te voorkomen. Op twitter meldt de politie dat die ruzie tot gevolg had dat een groep van 50 à 60 jongeren onderweg was om het uit te vechten. Met behulp van politiehond en wapenstok werd het weer rustig. Een van de tienermeiden (14, uit Assen) is aangehouden wegens bedreiging, een jongen (16, uit Assen) voor belediging van agenten.

———————————————

De politie heeft nieuwe instructies opgesteld voor het gebruik van beelden op sociale media, schrijft De Monitor – waar al maandenlang extra goed gelet wordt op wat de politie op sociale media doet. Volgens de instructies, die kennelijk zijn geopenbaard, moeten agenten 'de herleidbaarheid van personen minimaliseren'. De instructies zijn mede ingegeven door het speurwerk van De Monitor, dat eerder aantoonde dat (vooral) in politievlogs, op facebook en twitter, soms te veel persoonsgegevens te zien waren. Ook woningen, locaties en auto's waren vaak te goed zichtbaar. De nieuwe instructie stelt dat gezichten, en ook tatoeages, sieraden, opvallende kleding/haardracht en postuur, onherkenbaar moeten zijn in foto's of video's.

———————————————

Steeds meer agenten zijn actief op Instagram. Ze plaatsen er veel berichten en zijn in sommige regio's 'razend populair' onder jongeren, schrijft het AD. Volgens de instacops is het 'een geweldige manier om met hen in contact te komen'. Een wijkagent die klaagt over een in de fik gestoken fiets, krijgt spontaan hulp van jongeren die de pd schoon willen maken. Een andere wijkagent die 'nog aan het klooien is', heeft al 600 volgers. 'Het is een bij uitstek het medium om ook te laten zien hoe mooi mijn werk is'. De instacops zijn 'gewoon begonnen', zonder cursus, en werken zonder regels. 'Het is gewoon je gezond verstand gebruiken'. Een politiewoordvoerder zegt dat zulke opleidingen wel beschikbaar zijn. Verbinding is volgens haar het toverwoord. 'We kunnen het publiek zo een uniek inkijkje geven in ons werk'.

Rechtspraak

Een 35-jarige man is veroordeeld tot een gevangenisstraf van 1 jaar, waarvan 6 maanden voorwaardelijk, voor het hacken van online accounts van meerdere bekende Nederlanders. Ook moet hij zich verplicht laten behandelen voor een persoonlijkheidsstoornis.

———————————————

Drie mannen die via facebook de anti-Zwarte Piet-activist Quinsy Gario bedreigden, hebben boetes gekregen. De mannen schreven onder meer dat Gario 'afgeschoten' moest worden. Ze kregen ieder 200 euro boete nadat ze spijt betuigden. Met overbekende excuses. De een zei dat hij in een impuls had gehandeld, de andere twee hielden vol dat hun accounts gehackt waren. Gario kreeg alleen al via facebook achthonderd bedreigingen en beledigingen. Negentien daarvan werden door het OM nader onderzocht. Uiteindelijk werden vijf personen als verdachte aangemerkt. Eén zaak werd geseponeerd, de vijfde verdachte moet nog voor de rechter verschijnen.

———————————————

Een ex-basisschooldirecteur is veroordeeld tot acht maanden cel voor seks met een minderjarig meisje dat hij via Seksjobs.nl had leren kennen. De verdachte Khalid T. was directeur van een islamitische basisschool in Alphen aan den Rijn en tevens PvdA-raadslid in Gouda. Hij reageerde op een advertentie op de sekssite en dacht dat het meisje 21 was. In werkelijkheid was ze 13. Via Whatsapp bood de man haar 900 euro voor drie keer seks per maand en spraken ze af voor een seksdate, augustus 2017, in het Campanilehotel in Gouda. De verdachte ontkende alles. Volgens hem had het meisje ruzie thuis en had hij 'uit goedheid' een kamer voor haar geboekt. De rechter geloofde dat niet en vindt dat de man, volwassen én directeur van een school, beter had moeten weten. De zaak ging spelen toen de moeder van het meisje de politie vertelde dat dochterlief seks had gehad met een volwassen man. Het meisje deed geen aangifte, het OM besloot de man ambtshalve te vervolgen. De verdachte moet verder 1500 euro schadevergoeding betalen aan het meisje, dat, gezien haar leeftijd, een 'heel grote mate van bescherming' verdient, aldus het vonnis. Die bescherming is zo groot, 'dat er ook sprake is van ontucht als zij zichzelf via een website aanbiedt'.

———————————————-

Een man (54, uit Brussel) is veroordeeld voor het bezit van 3500 kinderpornografische foto's en filmpjes tot 2,5 jaar (waarvan een jaar voorwaardelijk). De man liep tegen de lamp toen hij chatte met Britse undercoveragenten en naar Engeland vloog om seks te hebben met een kind. Eenmaal gearresteerd, vroeg hij collega's in België om zijn computers te wissen. Die collega's stapten echter naar de politie waarna in een loods meerdere harde schijven en dozen met uitgeprinte foto's werden gevonden. Het OM had tien jaar geëist, vooral omdat de man in 2005 al eens veroordeeld was voor dezelfde feiten, maar rechtbank was mild. Wel mag de man tien jaar lang geen 'professionele of vrijetijdsactiviteit beoefenen' die hem in contact kunnen brengen met minderjarigen.

———————————————

De rechtbank in Leeuwarden heeft een man (37, uit Leeuwarden) veroordeeld tot vier jaar celstraf (een jaar voorwaardelijk) voor grootschalige internetoplichting. De man, ict-expert, bouwde webshops voor bedrijven maar dan zo dat hij inloggegevens van klanten kon achterhalen. Ruim vijfhonderd bedrijven en particulieren deden aangifte tegen de verdachte die met de gegevens ook probeerde familie en vrienden van zijn slachtoffers te bestelen. De 'facebookhacker' werd gepakt toen hij te zien was op camerabeelden van winkels waar hij zijn aankopen kwam afhalen.

Verschijningsvorm cybercrime	138ab *lid 1*	138ab *lid 2*	138ab *lid 3*	138b	139c *lid 1*	139d	139e	161 *sexies*	161 *septies*	350a *lid 1*	350a *lid 2*	350a *lid 3*	350b *lid1*	350b *lid2*
● Malware														
Malware maken en/of verspreiden	X					X		X	X	X	X	X	X	X
Malware (Trojaanse paarden) gebruiken	X	X			X			X	X	X	X	X	X	
● Computerinbraak														
Computerinbraak (hacking)	X		X								X			
Computerinbraak vervolg-handelingen		X	X		X	X	X	X	X	X	X	X		
Portscan						X								
Spoofing/cache poisoning	X	X		X	X	X	X	X		X	X			
Sniffing					X	X	X			X				
Draadloze netwerken hacken/ misbruiken	X	X	X	X	X		X	X		X	X			
Password guessing	X			X		X								
● Website aanvallen														
Veroorzaken open relay									X				X	
Wederrechtelijk open relay gebruiken	X							X		X				
Defacing/vernielen website	X							X	X	X			X	
Defacing/doorleiden internet-verkeer	X							X	X	X				
Cross-site scripting	X	X			X	X	X	X		X			X	
SQL-injecties	X	X						X		X				
● Botnets														
Botnet bouwen en beheren	X	X	X		X					X		X		
● Denial of Service														
DDoS-aanval				X				X		X			X	
● Social Engineering														
Phishing		X			X		X							
Vishing/Smishing		X			X									
● E-mail gerelateerd														
Wederrechtelijk open mail relay gebruiken	X							X	X	X				
Spamming (met DoS tot gevolg)				X				X	X				X	

Wetsartikel

Art. 138ab, lid 1 Sr Hacken: opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk

Art. 138ab, lid 2 Sr Hacken: overnemen, aftappen of opnemen van gegevens uit een geautomatiseerd werk na binnendringen daarvan

Art. 138ab, lid 3 Sr Hacken door tussenkomst van een openbaar telecommunicatienetwerk

Art. 138b Sr Het belemmeren van toegang tot of gebruik van een geautomatiseerd werk

Art. 139c Sr Het aftappen of opnemen van gegevens (afluisteren)

Art. 139d, lid 1 Sr Plaatsen van opname-, aftap- of afluisterapparatuur; voorbereidingshandelingen

Art. 139d, lid 2 Sr Het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen of toegangscodes bedoeld om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen

Art. 139d, lid 3 Sr Zoals in art. 139d, lid 2 Sr, maar met oogmerk gericht op art. 138ab, lid 2 en 3 Sr

Art. 139e Sr Het bezit en verspreiden van gegevens of een voorwerp waarop gegevens staan die door wederrechtelijk aftappen of opnemen zijn verkregen

Art. 161sexies Sr Opzettelijk vernielen etc. van een geautomatiseerd werk of werk voor telecommunicatie; voorbereidingshandelingen

Art. 161septies Sr Vernieling etc. van een geautomatiseerd werk of werk voor telecommunicatie door schuld

Art. 231b Sr Identiteitsfraude

Art. 232 Sr Opzettelijk valselijk opmaken, vervalsen, gebruiken, etc. van betaalpas, waardekaart e.d.

Art. 240b Sr Kinderpornografie

Art. 248e Sr Grooming

Art. 273, lid 2 Sr Bekendmaking bedrijfsgeheimen; heling computergegevens ondernemingen

Art. 273d Sr Schending telecommunicatiegeheim

Art. 317, lid 2 Sr Afpersing door de bedreiging dat gegevens opgeslagen door een geautomatiseerd werk onbruikbaar, ontoegankelijk of gewist worden

Art. 326c Sr Het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen

Art. 350a, lid 1 Sr Opzettelijke vernieling van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350a, lid 2 Sr Het feit gepleegd in lid 1 met tussenkomst van een openbaar telecommunicatienetwerk

Art. 350a, lid 3 Sr Opzettelijk gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Art. 350b, lid 1 Sr Vernieling door schuld van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350b, lid 2 Sr Door schuld gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Video

Tek Tok Late Night:

1. Privacy
2. Internetvrijheid
3. Digitale veilig heid
4. High Tech Crime
5. Data in onderwijs
6. Cybersurveillance
7. Techtrends in onderwijs
8. Veilig internetten
9. MKB cyber secure
10. Cyberellende bij Tek Tok
11. Standaarden en keurmerken
12. Operation Hijg Tech Crime
13. Kraak van de Maand

You Tube:

- Doe jij het veilig online
- Malware
- WiFi ontvangst verbeteren
- Internetfraude via de telefoon
- Documentaire: Veiligheid en privacy
- Herken een nep-hotspot
- Gebruik wachtzinnen
- Drive-by-downloads voorkomen
- Hoe herken je een phishing mail
- Beveiligd internetbankieren
- Privacy—ik heb toch niets te verbergen
- Mousejack

Help wanted:

- Grooming
- Sexting
- Webcammisbruik
- Bedreigd/ gechanteerd
- Kinderporno
- Nepprofiel