



Secure Computing Magazine

[Trends in 2017: cybersecurity](#)

[Waarom iedereen kan worden opgelicht](#)

[Onderzoek witwassen en cybercrime](#)

[Onderzoek gegevensdragers](#)

[Nanotechnologie in dienst van veiligheid en justitie](#)

[Toepassing Social Media Data-Analytics](#)

[OM let in aanloop naar verkiezingen op discriminatie via sociale media](#)

[Europol en EURid werken samen in strijd tegen cybercriminaliteit](#)

[Why the hack?](#)

[Digitalisering en de beginselen van de strafrechtspleging](#)

[Big data, big consequences](#)

[WebVoyager](#)

[Drugshandel via internet](#)

[Toegangsblokkade gratis WiFi-hotspots opheffen](#)

[Ransomware bepaalt losgeldbedrag per slachtoffer](#)

[Silverlight-update in document blijkt keylogger](#)

[Update voor Windows-beveiligingstool EMET](#)

[Malware voor geldautomaten ondersteunt nu Windows 10](#)

[Politie verwacht bewijs via Internet of Things](#)

[Tubrosa virus laat je pc ongewenst Youtube video's bekijken](#)

[Politie pakt jihad via sociale media harder aan](#)

[Chrome-gebruikers doelwit van zogenaamde font-update](#)

[Zeven misverstanden over algemene voorwaarden](#)

AKTUEEL

Politie gaat cyberteams oprichten in strijd tegen cybercrime

Om cybercrime effectiever te kunnen bestrijden gaat de politie tien nieuwe cyberteams oprichten. Dat heeft korpschef Erik Akerboom in een interview tegenover Nu.nl laten weten. Alle regionale eenheden zullen straks een cyberteam krijgen dat zich met de bestrijding van cybercrime in brede zin zal bezighouden.

Naast het opsporen van cybercriminelen gaat het ook om preventie en het signaleren van dreigingen. Bij een aantal politie-eenheden zijn al cyberteams actief. "Mijn ambitie is om reguliere en veel voorkomende cybercrime aan te laten pakken door regionale eenheden. De cyberteams worden de aanjagers van de aanpak van cybercrime in de eenheden", laat Akerboom weten. De teams zullen uit minimaal tien rechercheurs gaan bestaan en krijgen ondersteuning van specialisten die over specifieke ict-kennis beschikken. De politie wil dit en volgend jaar honderd van dergelijke specialisten werven.

Akerboom herhaalt wat hij ook vorig jaar al liet weten, namelijk dat de politie een informatiefabriek aan het worden is. Forensisch onderzoek en het tappen van criminelen zouden steeds minder opleveren. "Het accent verschuift naar data - de analyse daarvan. En daar zit nou net de ontwikkelingskracht in. Als we daar stappen in gaan maken, dan kunnen we veel beter doordringen tot de criminaliteit", laat de korpschef weten. Voor de plannen zijn wel flinke investeringen nodig, zowel in technologische middelen als personeel, aldus Akerboom.

Wetsvoorstel

In het interview gaat de korpschef ook in op het wetsvoorstel computercriminaliteit III, waardoor de politie de bevoegdheid krijgt om systemen van verdachten binnen te dringen. Volgens Akerboom gaat het om een bevoegdheid waarvoor de politie eerst toestemming moet vragen aan een officier van justitie en de rechter-commissaris. Mensen hoeven zich dan ook geen zorgen te maken dat de politie bij ieder vergrijp in computers zal grasduinen, zo merkt hij op.

Rubrieken:

- [Verder op de website](#)
- [Cops in Cyberspace](#)
- [Rechtspraak](#)
- [Verschijningsvorm cybercrime](#)
- [Wetsartikel](#)
- [Video](#)
- [Handig](#)

Trends in 2017: cybersecurity

Welke veiligheidsproblemen zullen dit jaar de kop opsteken?

Omdat we met z'n allen meer tijd en geld in digitale toepassingen steken, is het ook voor criminelen steeds aantrekkelijker om zich om te scholen en zich toe te leggen op de cyberwereld. Je moet alert blijven voor de gekende valkuilen van phishing en malware, maar zijn er ook nieuwe (on)aangename verrassingen te verwachten?

Intelligentie is leuk, maar 2017 dreigt ook het jaar te worden dat onze slimme apparaten zich tegen ons gaan keren. Dat de verkoop ervan in de lift zit, is een deel van het probleem. Die verbonden producten, vaak met de koepelterm "Internet of Things" (IoT) aangeduid, maskeren een grote schaduwzijde, die zich op 21 oktober voor het eerst wereldwijd liet gelden en een impact had op heel wat mensen en bedrijven. Toen zorgde een krachtige DDoS-aanval die het bedrijf Dyn uitschakelde ervoor dat grote delen van het internet voor een tijdje onbereikbaar waren.

Dyn is een populaire Domain Name System-provider, in essentie een adresboek van het internet, dat ervoor zorgt dat je bij het intikken van een webadres op de juiste webpagina komt. Het botnet dat servers van Dyn platgooide? Dat bestond uit huishoudtoestellen met een computerchip, gekaapt door hackers via malware met de naam Mirai.

Veiligheidsexperts luiden al langer de alarmbel over de povere beveiliging van slimme toestellen. Deze zijn in het overgrote deel van de gevallen maar met minimale middelen uitgerust om zich te beschermen tegen digitale indringers. Vaak is er ook geen optie om na aankoop nog software-updates uit te voeren om de beveiliging van een apparaat op te trekken. Die situatie, gekoppeld aan het feit dat steeds meer mensen IoT-toestellen zullen aanschaffen, maakt dat security-analisten de toekomst niet rooskleurig tegemoet zien.

Zij verwachten dat gelijkaardige grote DDoS-aanvallen meer zullen opdruken in het komende jaar. "De apparaten zijn gewoon te gemakkelijk te gebruiken en in grote capaciteit aanwezig om dit gevaar te negeren," stelt Rudolf De Schipper, senior projectmanager bij Unisys Belgium. Bovendien dient een oplossing voor het probleem zich niet meteen aan. Bij zowel fabrikanten als kopers is er momenteel weinig animo voor een betere beveiliging van hun toestellen.

Een recent initiatief om het probleem aan te pakken komt van de Broadband Internet Technical Advisory Group (BITAG), een organisatie waar ook Google, Intel en Microsoft zijn bij aangesloten. Via een lijst van veiligheidsstandaarden en het voorstel om met een kwaliteitslabel te werken, hoopt de instantie de situatie te verbeteren. Zolang die aanbevelingen echter niet in dwingend de richtlijnen worden omgezet, blijven bedrijven vrij om kwetsbare (en dus ook goedkopere) toestellen op de markt te brengen.

2016 zal bij securitybedrijven te boek komen te staan als het jaar van de ransomware. Dit type van malware is al langer gekend, maar vorig jaar groeide het aantal infecties exponentieel op wereldschaal. België en Nederland stonden bovendien beiden in de top van meest getroffen landen. Zet de ransomware-epidemie zich voort in het komende jaar? Op zich zijn er geen aanwijzingen dat hackers nog iets onaangenaam achter de hand hebben waardoor de ransomware zich nog sterker zal verspreiden, aan de andere kant is er ook niet meteen een grote verbetering te ontwaren bij de bescherming.

"Er is niet zoveel beweging bij antivirusbedrijven om dit meteen aan te pakken, al zijn dergelijke infecties ook voor een groot deel te wijten aan het feit dat beveiliging nog steeds geen integraal onderdeel uitmaakt van de meeste IT-systemen en ook de meeste gebruikers dit niet hoog op de agenda hebben staan. We zullen volgend jaar

Malware zal het komende jaar menselijk gedrag imiteren om de doeltreffendheid van aanvallen te vergroten.

waarschijnlijk het gebruikelijke slagveld mogen aanschouwen," aldus De Schipper. Securitybedrijf Kaspersky laat optekenen dat het verwacht dat de hackers achter de ransomware-aanvallen steeds onbetrouwbarder zullen worden vanwege het "toetreden van een lagere klasse van criminelen" die geld hebben geroken, en minder geneigd zullen zijn om bestanden aan slachtoffers terug te geven nadat ze losgeld hebben betaald.

Het gebruik van biologische gegevens in technologie heeft een grote vlucht genomen dankzij de populariteit van vingerafdruksensors op smartphones. Van een functionaliteit die enkel te vinden was op de duurste toestellen is die sensor geëvolueerd naar een standaard die je verwacht in het middensegment, en begint nu ook stilletjes aan binnen te druppelen bij de budgetmarkt via producten als de Wileyfox Swift 2. Het is dus niet meer zo raar om de huidlijntjes op je vinger te laten scannen en opslaan, en ook andere vormen van biometrische identificatie vinden langzaam aan ingang op gewone consumententoeestellen. Denk bijvoorbeeld aan de irisscanner op de spijtig genoeg explosief ter ziele gegane Samsung Galaxy Note 7.

Biometrie werd in het verleden al weleens onthaald als hét instrument waarmee we eindelijk die onhandige wachtwoorden zouden kunnen afschaffen. Het registreren van je vingerafdruk of handpalm zal echter nooit het wachtwoord volledig vervangen. "Biometrie wordt steeds meer mainstream," bevestigt Rudolf de Schipper, "maar tegelijkertijd zien we ook de negatieve kantjes steeds duidelijker. Misbruik is nog altijd mogelijk. Om veiligheidsredenen zou een biometrische scan nooit zowel de functie van gebruikersnaam als je wachtwoord mogen opnemen. Je biologische gegevens zijn eigenlijk enkel als gebruikersnaam in te zetten, voor de rol van wachtwoord zijn ze ongeschikt omdat je ze niet kan veranderen. Binnen een goed identificatiesysteem zal er dus altijd een tweede element in het spel nodig zijn naast je biometrische gegevens."

Om het allemaal nog moeilijker te maken is deze zomer nog een andere zorgwekkende trend aan het oppervlakte gekomen: de opkomst van gepersonaliseerde malware. Die dreiging werd vastgesteld bij de ontdekking van ProjectSauron, geavanceerde spionagesoftware "waarbij alle functies werden aangepast aan elk slachtoffer," aldus Kaspersky. Die kameleon-eigenschap steekt stokken in de wielen van securitybedrijven, omdat infecties geen vast patroon meer hebben. Dergelijke complexe programma's zal je als gewone burger gelukkig niet snel op je pc binnenhalen, ze zijn op dit moment nog beperkt tot het domein van de staatsspionage.

Waarom iedereen kan worden opgelicht

Opbeurend nieuws. Wie weleens het tv-programma Opgelicht?! ziet, valt van de ene verbazing in de andere: wie geeft nou zomaar zijn bankpas aan een vreemde? Wie maakt nou geld over naar een onbekende in het buitenland? Mij overkomt dat niet, denk je dan.

Maar dat is een misvatting: iedereen kan slachtoffer worden van oplichting. Dat heeft niets te maken met arm of rijk, slim of dom.

Koffertjes met nepgeld, geheime middeljes om het zichtbaar te maken, loterijen met 'administratiekosten', de prins op het witte paard voor wie je tienduizenden euro's 'paspoortleges' betaalt, een zwaar hoverboard dat iemand wel even opstuurt ... tja, de meeste trucs zijn meer dan bekend.

Maar veel oplichters maken zo slim gebruik van de psychologie dat het bijna onmogelijk is om er niet in te trappen. Zo zijn we nu eenmaal. En dus kan iedereen slachtoffer worden. Onderzoek toonde al aan dat in twee jaar tijd maar liefst 1,1 miljoen Nederlanders werden opgelicht, de totale schade bedroeg maar liefst 5,3 miljard euro. Zeventig procent raakte minder dan vijfhonderd euro kwijt maar 7% verloor meer dan tien mille! Velen van hen dachten/denken dat ze de trucs wel kunnen doorzien of hebben 'de illusie van controle'.

Maar die controle is er niet, zegt gedragspsycholoog Liza Luesink. 'Opgelicht worden, denken we, dat overkomt ons gewoon niet.' De werkelijkheid is anders, zou je ook moeten weten. Luesink spreekt van de just-world fallacy: 'we geloven in een eerlijke wereld waarin slechte mensen gestraft worden en goede mensen niet. Als goed volk wanen we ons veilig'. En dus plakken we de webcam niet af, doen we online bankzaken via de wifi van de McDonalds en geven we netjes onze wachtwoorden als Microsoft belt.

"We geloven in een eerlijke wereld waarin slechte mensen gestraft worden en goede mensen niet. Als goed volk wanen we ons veilig."

Omdat oplichters ook steeds slimmer worden, en gericht te werk gaan, hebben ze altijd succes. Voor elke vorm van oplichting is wel een speciale doelgroep te vinden. Volgens de Fraud Victim Study van de Amerikaanse psychologen Karla Pak en Doug Shadel zijn alleenstaande, wat armere laagopgeleiden gemiddeld genomen gevoeliger voor het kopen van valse loten en vallen ouderen sneller voor oplichting door kennissen of familieleden. Goedopgeleide mannen met een hoog inkomen blijken weer vaker slachtoffer van investeringsfraude. Een verklaring daarvoor is dat we, naarmate we ergens meer van weten, de kans steeds kleiner inschatten dat we worden misleid. Psycholoog Maria Konnikova schreef daar over: wie zich veilig voelt, laat de waakzaamheid verslappen.

En die ezel dan, die van die steen? In Engeland circuleerde in 2014 onder oplichters een sukkellijst, waarop maar liefst 160 duizend mensen staan die meerdere keren opgelicht zijn. Autoriteiten die hen wilden voorlichten, stuitten op weerstand. Een deel zei zelfs nooit opgelicht te zijn ... Trouwens, van de vier bekendste oplichterstrucs spelen er drie rond internet: Microsoft aan de lijn, de gewonnen droomvakantie en de nepwebshop. Nieuwe trucs zijn te volgen via Fraudehelpdesk en (de app van) het tv-programma Opgelicht?!

Onderzoek witwassen en cybercrime

Over het witwassen bij cybercrime is, vergeleken met witwassen bij andere delicten, relatief weinig bekend. Bij veel delicten verdienen criminelen geld in contanten. Bij het witwassen van verdiensten uit cybercrime lijken echter in toenemende mate andere digitale betalingsmiddelen te worden gebruikt dan contant geld dat bijvoorbeeld uit drugshandel wordt verkregen.

Met de groei van cybercrime in de laatste jaren neemt de urgentie toe om zicht te krijgen op het witwasproces en de betrokken actoren in dit proces. Het onderzoek richt zich om die reden op het witwasproces, en het in kaart brengen van de betrokken actoren bij banking malware en ransomware.

Banking malware is, kort gezegd, kwaadaardige software die bedoeld is om slachtoffers geld afhandig te maken via betalingen met internetbankieren. Ransomware is kwaadaardige software waarmee iemands computersysteem (of bestanden die zich daarop bevinden) wordt 'gegijzeld' en losgeld wordt geëist om het systeem te ontsleutelen. Sinds een paar jaar is een variant van ransomware in opkomst, genaamd cryptoware, waarbij bestanden op een computer versleuteld worden en het losgeld in de virtuele valuta Bitcoin wordt geëist.

De centrale vraagstelling in het onderzoek is: op welke wijze en door welke actoren wordt geld verkregen uit banking malware en ransomware (al dan niet digitaal) witgewassen?

Het geld dat wordt verkregen uit banking malware en ransomware is doorgaans digitaal van aard. Bij banking malware wordt elektronisch geld buitgemaakt en bij ransomware wordt het losgeld veelal betaald met vouchers of in toenemende mate en vooral bij cryptoware) met bitcoins.

Het witwassen van deze opbrengsten bestaat uit het verbergen of verhullen van de criminele herkomst van het geld. De typologieën die zijn ontwikkeld om opzet bij opzetwitwassen te bewijzen, hebben vooral betrekking op contant geld bij (veelal) drugsdelicten. In de praktijk bestaat daardoor regelmatig onduidelijkheid over de vraag op welke moment bij transacties of bezit van grote sommen virtuele betalingsmiddelen kan worden gesproken van opzet bij witwassen. Veel typen digitale betalingsmiddelen kunnen worden gebruikt om de verdiensten uit cybercrime wit te wassen.

In het onderzoek wordt een onderscheid gemaakt tussen elektronisch geld en virtueel geld. Elektronisch geld is de digitale weergave van echt geld, terwijl virtueel geld niet door de overheid is gefiatteerd. Virtueel geld kan op zijn beurt centraal of decentraal beheerd zijn en wel of niet inwisselbaar zijn tegen echt geld.

Inwisselbaar, centraal beheerd virtueel geld betreft bijvoorbeeld tegoeden op websites, niet-inwisselbaar centraal beheerd virtueel geld betreft bijvoorbeeld speelgeld in online games en virtuele werelden. Inwisselbaar, decentraal beheerd virtueel geld betreft cryptocurrencies. Veruit de bekendste cryptocurrency is de Bitcoin, met 90% van de totale marktwaarde van virtuele valuta.

Lees of download [het hele onderzoek](#) via de Secure Computing website



Onderzoek gegevensdragers

“Wat is er bekend over de inbeslagneming van en het daaropvolgende onderzoek dat wordt gedaan aan elektronische gegevensdragers en in geautomatiseerde werken door opsporingsambtenaren?”

Uit deze algemene vraagstelling vloeit een aantal kwantitatieve en kwalitatieve onderzoeksvragen voort die bij het inzichtelijk maken van de inbeslagnemingspraktijk als algemene leidraad zijn genomen.

Het blijkt dat het Wetboek van Strafvordering nauwelijks specifieke regels kent ten aanzien van onderzoek aan in beslag genomen elektronische gegevensdragers of geautomatiseerde werken. Dit in tegenstelling tot het onderzoek aan gegevensdragers en geautomatiseerde werken tijdens een doorzoeking van een plaats ter vastlegging van gegevens, waarvoor de wet wel specifieke bepalingen bevat. Uit de besproken rechtspraak blijkt dat in lagere rechtspraak verschillend wordt geoordeeld over de vraag of de bepalingen inzake de inbeslagneming van voorwerpen, waaronder artikel 94 Sv, mede in het licht van het bepaalde in artikel 8 EVRM en tegen de achtergrond van technologische ontwikkelingen, nog een voldoende voorzienbare grondslag vormen voor het door een opsporingsambtenaar vergaren van gegevens die zijn vastgelegd op een in beslag genomen smartphone. De uitleg van die bepalingen voor zover die betrekking heeft op het in beslag nemen van voorwerpen teneinde nader onderzoek te verrichten om de daarop vastgelegde gegevens ter beschikking te krijgen met het oog op de waarheidsvinding, is niet eensluidend. Tot op heden is geen specifieke regelgeving op dit (deel) gebied voorhanden.

Ten aanzien van de kwantitatieve onderzoeksvragen komt naar voren dat op basis van de bestaande cijfers over de inbeslagneming van en het daaropvolgend onderzoek aan elektronische gegevensdragers en geautomatiseerde werken, aanzienlijke aantallen gegevensdragers door de opsporingsambtenaren in beslag worden genomen. Bij die cijfers wordt geen onderscheid gemaakt tussen de grond voor inbeslagneming en de betreffende autoriteit onder wiens verantwoordelijkheid of door wie de voorwerpen zijn in

beslag genomen. Hoewel de situatie wel voorkomt, zijn geen concrete cijfers bekend ten aanzien van het door een opsporingsambtenaar ter plaatse in een geautomatiseerd werk kijken om van de daarop opgeslagen gegevens kennis te nemen, zonder dat het voorwerp formeel in beslag wordt genomen. Met betrekking tot het wissen van bestanden van elektronische gegevensdragers of geautomatiseerde werken zijn ook geen cijfers bekend aangezien registratie daarvan achterwege blijft.

Ten aanzien van de kwalitatieve onderzoeksvragen wordt geconcludeerd dat in de meeste gevallen in de voorbereiding en voornamelijk ter plaatse een afweging wordt gemaakt omtrent de in beslag te nemen gegevensdragers. Deze afweging wordt in de meeste gevallen, gelet op het feit dat in de meeste gevallen de inbeslagneming plaatsvindt tijdens een doorzoeking van een plaats door de officier van justitie of de rechter-commissaris gemaakt. De uitkomst van die afweging is sterk afhankelijk van de verdenking van het strafbare feit en de omvang van het onderzoek, maar ook van de bij de inbeslagneming betrokken autoriteiten. Als uitgangspunt wordt ervan uitgegaan dat alle op de voorwerpen aanwezige gegevens mogen worden onderzocht, met uitzondering van de gegevens die onder het verschoningsrecht vallen. Gegevens worden geheel of deels gekopieerd voor verder onderzoek, tenzij de gegevens versleuteld zijn of de toegang tot die gegevens geblokkeerd is. De kopieën worden in bedrijfssystemen vastgelegd. Het beleid omtrent toegang tot die bedrijfssystemen verschilt regionaal. Er lijkt geen centrale regie te bestaan met betrekking tot de wijze waarop en het moment waarop gegevens vernietigd moeten worden dan wel ontoegankelijk moeten worden gemaakt. De Wpg stelt regels omtrent de bewaartermijnen en de vernietiging van die gegevens, maar de inhoud daarvan is niet breed bekend in de praktijk. Het Wetboek van Strafvordering bevat geen bepalingen daaromtrent.

In de praktijk worden problemen ondervonden op het gebied van de inbeslagneming van elektronische gegevensdragers en geautomatiseerde werken voor zover gegevens binnen de reikwijdte van het verschoningsrecht vallen. De bestaande

wet- en regelgeving lijkt daarover onvoldoende duidelijkheid te verschaffen aan de praktijk. Het filteren van gegevens waarover het professioneel verschoningsrecht zich uitstrekt, levert (nog) geen goed werkbaar resultaat voor het opsporingsonderzoek op.

Ten aanzien van het vergaren van gegevens die elders (in de cloud) zijn opgeslagen bevat de huidige wet geen specifieke bevoegdheid; ook beleidsregels ontbreken. Het vergaren van dergelijke gegevens vindt sporadisch plaats. Problemen hangen samen met vragen omtrent schendingen van de soevereiniteit van andere landen en de afwezigheid van een voldoende duidelijke wettelijke regeling op dit punt. Het uitgangspunt van beleid is, dat bij twijfel omtrent schendingen van soevereiniteit gegevens niet worden vastgelegd. Het is wenselijk de praktijk in dat kader duidelijkheid te verschaffen over de grenzen en mogelijkheden van grensoverschrijdend onderzoek. Het komt voor dat opsporingsambtenaren onderzoek verrichten aan, voornamelijk, geautomatiseerde werken die niet formeel in beslag genomen zijn. Bij de opsporingsambtenaren blijkt geen duidelijk beeld te bestaan over de wettelijke bevoegdheden en de gevallen waarin gegevensdragers mogen worden onderzocht.

In het geval ‘illegale content’ op de gegevensdrager wordt aangetroffen, wordt de gegevensdrager als uitgangspunt niet meer teruggegeven. Het beleid hierover blijkt regionaal verschillend te zijn. De mogelijkheid dat op een beveiligingscamera beelden van de doorzoeking zijn geregistreerd, waarbij de betrokken opsporingsambtenaren herkenbaar in beeld zijn gebracht, wordt regelmatig genoemd als te wissen ‘content’. Bij de opsporingsinstanties leeft de vraag in hoeverre die beelden verwijderd mogen worden en wie daartoe bevoegd is. Het ontbreken van een concrete regeling daaromtrent wordt in de opsporing als problematisch ervaren en zou ten grondslag kunnen liggen aan het niet registreren van het, al dan niet gedeeltelijk, wissen van bestanden van een elektronische gegevensdrager of geautomatiseerd werk.

Lees (of download) [het hele onderzoeksrapport](#) via de Secure Computing website.

Nanotechnologie in dienst van veiligheid en justitie

In de afgelopen 15 jaar is nanotechnologie steeds meer onder de aandacht gekomen en heeft de financiering van nanotechnologisch onderzoek een grote vlucht genomen. Een aantal producten op basis van nanotechnologie is reeds op de markt verschenen. Over het algemeen is nanotechnologie nog steeds een opkomende technologie en zijn toepassingen nog in ontwikkeling. In een WODC rapport wordt de betekenis van nanotechnologie voor civiele veiligheidstoepassingen besproken en de studie geeft een breed overzicht van opkomende nanotechnologieën en toepassingsdomeinen. De focus in dit rapport ligt op de kansen die nanotechnologie biedt voor veiligheidstoepassingen. Mogelijke risico's op het gebied van bijvoorbeeld gezondheid en milieu worden niet besproken.

Op basis van een meta-literatuurstudie zijn verschillende toepassingsdomeinen geïdentificeerd en besproken in dit rapport: (i) detectie, (ii) bescherming, (iii) veilige identificatie en communicatie en (iv) defensie. Hiernaast zijn mogelijk interessante nanotechnologieën voor de veiligheidstoepassingen in deze domeinen beschreven en toegelicht. Deze resultaten zijn aangevuld met uitkomsten uit interviews (in totaal 27) met onderzoekers en experts op het gebied van nanotechnologie; bedrijven die producten leveren voor veiligheidstoepassingen; en met verwachte eindgebruikers en veiligheidspartners van het Ministerie VenJ zoals politie, brandweer, Nederlands Forensisch Instituut, Dienst Justitiële Inrichtingen, Openbaar Ministerie, Koninklijke Marechaussee en het Ministerie van Defensie. De interviews geven inzicht in de behoeftes en wensen van veiligheidspartners ten aanzien van mogelijke nanotechnologietoepassingen en in de unieke eigenschappen van nanotechnologieën voor een toepassingsgebied. In de interviews zijn eveneens verwachte uitdagingen en toekomstige ontwikkelingen voor deze toepassingsgebieden besproken.

Voor de politie, de Koninklijke Marechaussee en andere onderdelen van het Ministerie van Defensie is de detectie van chemische, biologische, radioactieve en explosieve stoffen van groot belang. De detectie van explosieven speelt hier een bijzondere rol en zou bijvoorbeeld op vliegvelden het liefst op afstand, met zo weinig mo-

gelijk interventie en ongemak voor de passagiers moeten plaatsvinden. Voor de politie is op dit moment het detecteren van synthetische drugs en illegale drugslaboratoria een groot probleem waar nieuwe technologieën een alternatief kunnen bieden. Detectietechnologieën dienen efficiënt, effectief en betrouwbaar te zijn. Nanosensoren bieden een extra meerwaarde door op de lengteschaal van moleculen te meten, dus op enkele nanometers, waardoor zij een hoge sensitiviteit hebben en kleine concentraties tot enkele moleculen van een stof specifiek kunnen detecteren. Er wordt verwacht dat het gebruik van sensoren in de komende 5-10 jaar sterk zal toenemen, zeker voor gezondheidstoepassingen.

Voor forensisch onderzoek is de detectie van biologische sporen zoals DNA, bloed, sperma, haar en huid van groot belang voor de reconstructie van strafbare feiten. Nieuwe technieken zouden gebruikt kunnen worden om sporen beter te kunnen detecteren en meer informatie te verkrijgen. Bij de politie en het Nederlands Forensisch Instituut bestaat behoefte aan draagbare detectiemethoden die kunnen worden gebruikt op de plaats delict om verdachte sporen ter plekke te analyseren. Door onderdelen van sensoren steeds kleiner te maken en te integreren wordt het mogelijk om meer detectieapparatuur draagbaar te maken. Er wordt verwacht dat in de toekomst digitale data steeds relevanter zullen worden voor de politie en het forensisch onderzoek om een misdaad op te helderen.

Identificatie van personen en de verificatie van de echtheid van officiële documenten zoals (binnen- en buitenlandse) identiteitsbewijzen, visa en geld zijn van groot belang voor luchthavenbeveiliging, politie en het Openbaar Ministerie. De veiligheid van fraudegevoelige documenten zoals identiteitsbewijzen of toegangspassen voor gebouwen kan verbeterd worden met behulp van nanotechnologie. Door eigenschappen op de nanoschaal te benutten kunnen unieke identificatie en authenticatie kenmerken worden gemaakt die daardoor niet nagemaakt kunnen worden. Ook op de gebieden opsporen en volgen van personen, authenticatie en bescherming van data bieden nanotechnologieën toepassingen. Opsporen en volgen (track and trace) is een belangrijk punt voor veel veilig-

heidstoepassingen zoals het volgen van politie of brandweermensen tijdens een inzet of het volgen van reizigers op verkeersknooppunten. Het beveiligingsniveau voor gevangenen zal binnen de komende 10 jaar veranderen waarin nieuwe technologieën een interessante rol zouden kunnen spelen in het traceren van gedetineerden. Ten aanzien van authenticatie wordt verwacht dat de markt voor veilige authenticatie binnen de komende 5-10 jaar sterk zal groeien. De bescherming van sensitieve communicatie is belangrijk voor de politie, nationale veiligheidsinstellingen, organisaties binnen de overheid, banken, financiële instellingen en voor een groot aantal bedrijven. Ook het toenemend gebruik van sensoren vereist beveiligde communicatie.

Naast de beveiliging van dataverkeer is ook decryptie belangrijk, bijvoorbeeld voor het ophelderen van een misdaad en om communicatie van criminelen af te kunnen luisteren. Het decoderen van data is ook van belang voor de krijgsmacht om informatie over de vijand te krijgen. Encryptie en decryptie zullen dus een steeds grotere rol spelen in defensie en informatie zal steeds belangrijker worden vergeleken met conventionele wapens. Kwantumcommunicatie, dat een zeer hoge bescherming tegen afluisteren garandeert, is nu reeds commercieel beschikbaar.

De verscheidenheid van nanotechnologieën voor de hier gepresenteerde veiligheidstoepassingen is zeer breed. Het onderzoek biedt dus een overzicht van de technologieën die beschikbaar zijn dan wel in ontwikkeling zijn. Om de kansen die nanotechnologieën bieden goed te benutten is het van belang om de dialoog tussen eindgebruikers en wetenschappers te stimuleren en zo ervoor te zorgen dat technische ontwikkelingen nauw aansluiten bij huidige en toekomstige behoeftes in de operationele praktijksituaties van het Ministerie van VenJ en haar veiligheidspartners.

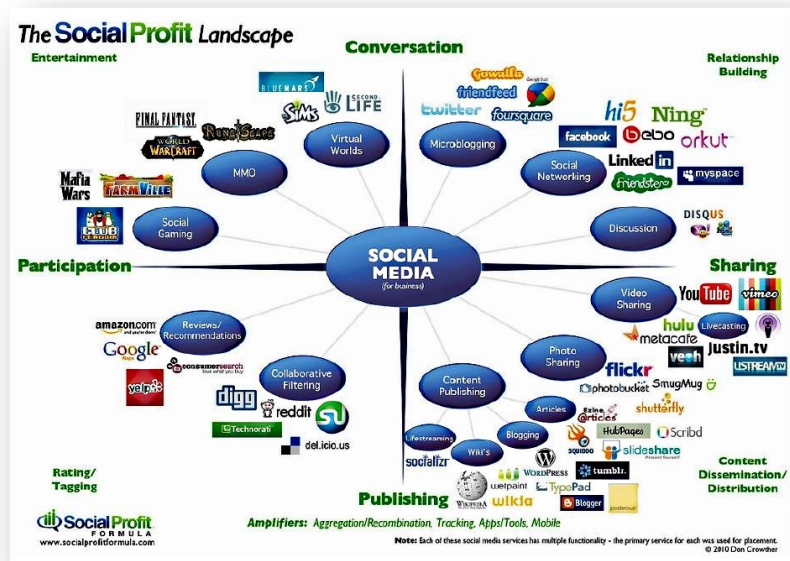
Lees (of download) [het hele rapport](#) via de Secure Computing website

Toepassing Social Media Data-Analytics

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het ministerie van Veiligheid en Justitie (VenJ) heeft [Coosto](#) een verkennende studie uitgevoerd naar mogelijke nieuwe social media toepassingen voor VenJ. Deze studie beoogt primair nieuwe toepassingen in kaart te brengen of bestaande toepassingen te herformuleren zodat ze bruikbaar zijn voor VenJ.

Het ministerie van Veiligheid en Justitie (VenJ) en haar diensten en partners gebruiken de tool Coosto sinds een aantal jaren voor verschillende toepassingen, denk bijvoorbeeld aan webcare. Binnen het veiligheidsdomein zijn bepaalde Coosto-toepassingen relevant die ook voor de commerciële markt gangbaar zijn en in de regel al zijn ontwikkeld. Er is echter ook een aantal andere toepassingen denkbaar die specifiek ontwikkeld kunnen worden voor VenJ. Om na te gaan welke toepassingen er specifiek voor het veiligheidsdomein voorhanden zijn of ontwikkeld kunnen worden, is aan Coosto gevraagd om dit (in samenwerking met het WODC) te onderzoeken.

Lees (of download) [het hele rapport](#) via de Secure Computing website.



OM let in aanloop naar verkiezingen extra op discriminatie via sociale media

Het OM gaat, in de aanloop naar de verkiezingen van maart 2017, extra letten op beledigen en discrimineren van politici op sociale media. Hoofdofficier van Justitie Theo Hofstee stelde dat het OM in die gevallen snel moet ingrijpen.

Hij verwees onder meer naar de uitlatingen tegen (inmiddels ex-) Denk'er Sylvana Simons. 'Zeker tien mensen' zullen in die zaak vervolgd worden, meldde het OM eerder. Hofstee vindt dat alle meningen geuit moeten kunnen worden, 'maar wel op een nette manier'.

In de aanloop naar de verkiezingen 'nemen de emoties toe en dus verwachten we meer van dit soort gevallen als we niet opletten'. Het speciale politieteam Bedreigde Politici kreeg in 2015 tweehonderd meldingen, waarvan het OM er 92 als strafbaar beoordeelde. In 24 zaken werd de verdachte gedagvaard.

Europol en EURid werken samen in strijd tegen cybercriminaliteit

Om een grip te krijgen op kwaadwillige webpagina's en informatie uit te wisselen over criminele trends, gingen Europol en EURid sinds kort een samenwerking aan.

Europol slaat de handen in elkaar met de Europese organisatie die toekijkt op de registratie van .eu-domeinen, EURid, om cybercriminaliteit tegen te gaan. Beiden tekenden in Den Haag een memorandum van overeenstemming.

Domeinwaakhond

EURid houdt zich als Europese waakhond van de .eu- en .euo-domeinen bezig met de controle van registrars en het ontwikkelen van veiligheidssystemen die valse domeinen moeten tegengaan. In 2016 schorste de organisatie al 5,877 domeinnamen, bijvoorbeeld omdat de websites malware bevatten of naar scams leiden.

Door met Europol samen te werken, staan beide organisaties sterker in de strijd tegen cybercriminaliteit en kunnen ze hun schouders zetten onder gezamenlijke projecten die online veiligheid kunnen stimuleren. Bovendien wordt gepland om statistische data uit te wisselen die kan helpen om meer informatie te verzamelen over criminele trends.

“Blijven evolueren”

“Het is cruciaal dat we doorgaan met het monitoren en identificeren van abusievelijke registraties en illegale activiteiten binnen de .eu- en .euo-ruimte, en op tijd actie ondernemen. Onze samenwerking met Europol zal helpen om dit te bereiken, maar we moeten blijven evolueren om degenen met kwaadaardige intenties voor te blijven,” bevestigt Giovanni Seppia, external relationsmanager bij EURid.



Why the hack?

Gehackte organisaties zijn geen zeldzaamheid meer en duidelijk is dat iedere organisatie doelwit kan zijn van hackers. Maar waar doen de hackers het eigenlijk voor?

Wanneer het gaat over de motivaties van hackers komen geregeld termen voorbij als geld, nieuwsgierigheid en spanning. Nog afgezien van het feit dat geld eigenlijk geen motivatie is – geld is een middel en de achterliggende motivatie kan een kwestie zijn van need of greed – ontbreekt het bij de bespreking van dergelijke motivaties vaak aan theoretische onderbouwing en empirisch onderzoek.

Het onderzoek dat hier besproken wordt, probeert daar verandering in te brengen. In dit onderzoek is een vragenlijst voorgelegd aan 65 hackers met een gemiddelde leeftijd van 27,5 jaar, waarbij de jongste 19 en de oudste 49 is. ‘Hacker’ is hier gedefinieerd als iemand die heeft geprobeerd computerbeveiligingssystemen zonder toestemming te omzeilen. Op de vraag hoe vaak zij beveiligingssystemen van organisatie-servers hadden omzeild, antwoordde 68 procent met “minimaal één keer”. Verder gaf 29 procent aan zich “minimaal één keer” te hebben ingelaten met ‘hacktivism’ (hacking activisme).

In de vragenlijst stonden ook vragen over frequent genoemde motivaties als nieuwsgierigheid, teamplay en gerechtigheid, en over motiverende waarden. Deze motiverende waarden vormen het hoofdonderzoek.

Lees [verder via](#) de Secure Computing website.



Digitalisering en de beginselen van de strafrechtspleging

De digitalisering heeft in de strafrechtspleging al behoorlijk grote veranderingen gebracht en dat zal in de toekomst eerder meer dan minder ingrijpend worden. In het strafrecht gelden echter fundamentele juridische waarden, veelal aangeduid met de term grondbeginselen, die bij het handelen en beslissen geëerbiedigd moeten worden. De vraag moet gesteld worden of en hoe dat gaat lukken: een digitalisering van de strafrechtspleging met respect voor de juridische grondbeginselen van de strafrechtspleging. Voor het uitvoeren van deze studie is de volgende vraag centraal gesteld:

Door welke informatietechnologische ontwikkelingen kan het handelen/beslissen van actoren in de Nederlandse strafrechtspleging veranderen? Welke positieve en negatieve aspecten brengen deze ontwikkelingen met zich mee ten aanzien van de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging?

De volgende deelvragen zijn onderscheiden.

- 1 Welke beginselen van strafrechtspleging zijn in verband te brengen met IT-ontwikkelingen?
- 2 Welke veranderingen in de Nederlandse strafrechtsketen zijn er in de afgelopen vijf jaar het gevolg van de ontwikkelingen in de IT?
- 3 Op welke punten ondersteunen de reeds zichtbare veranderingen de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging, dan wel leveren deze veranderingen spanning op met deze beginselen?
- 4 Welke voor de Nederlandse strafrechtsketen relevante IT-ontwikkelingen zijn in de komende tien jaren te verwachten?
- 5 Op welke punten zullen de te verwachten veranderingen steun geven aan de werking van verdragsrechtelijke en (grond)wettelijke beginselen binnen de strafrechtspleging, c.q. zullen de veranderingen spanning met deze beginselen betekenen?

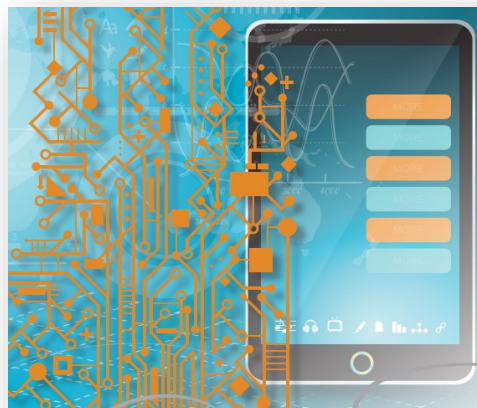
In de toekomstige gedigitaliseerde strafrechtspleging zal de relatie tussen de IT-specialisten en de juridische professionals niet als producent-consument bestempeld kunnen worden. Beide zullen zich op de andere discipline moeten richten en de genoemde rollen met elkaar moeten gaan combineren tot de 'conducenten' van de digitale afdoening van strafzaken. De veranderingen in het handelen en beslissen zullen vast en zeker tot nieuwe vormen van realisatie van de grondbeginselen

leiden, maar als beide disciplines vanuit hun principiële basis aan dit proces leiding geven, kan deze nieuwe toestand net zo verenigbaar zijn met het juridisch-normatieve kader als de huidige situatie en zijn er zelfs verbeteringen mogelijk.

De digitalisering van de strafrechtspleging is al lang aan de gang⁶ in die zin dat informatiesystemen en -toepassingen al vele jaren ingezet worden in organisaties in de strafrechtsketen. Iedereen gebruikt al jarenlang computers voor tekstverwerking en berichtenverkeer, gegevensopslag en registratie van handelingen en gebeurtenissen. Dat daarmee niets veranderd is in de werkwijzen, valt moeilijk vol te houden.

Toch is het al die tijd mogelijk gebleken om in het juridische kader aan de overgang naar informatiesystemen slechts zeer beperkt gevolg te geven, waardoor het vermoeden rijst dat de systemen en applicaties nog niet veel meer doen dan het ondersteunen van de reeds lang gebruikelijke, wettelijk verankerde werkwijzen. Als die aanname juist is, valt daaraan de veronderstelling te koppelen, dat ook de fundamentele kenmerken en beginselen van de strafrechtspleging tot nu toe fier overeind konden blijven staan.

Lees (of download) [het hele onderzoek](#) via de Secure Computing website



Big data, big consequences

Het lijkt de gouden graal van de informatiesamenleving: uit een grote berg ongestructureerde informatie allerhande niet voorziene verbanden en samenhang ontdekken. Aan de hoeveelheid informatie hoeft het niet te liggen, die is er in overvloed. De mogelijkheden van de technologie, zowel qua opslag als reken capaciteit, vormen ook steeds minder een belemmering. Niets lijkt aan een glorieuze toekomst van Big Data analysis in de weg te staan.

Ook binnen het domein van veiligheid en justitie zijn er mogelijkheden. De taak van juristen is om de randvoorwaarden aan te geven waarbinnen de mogelijkheden van de technologie kunnen worden benut. In een democratische samenleving is het van belang dat burgers de overheid vertrouwen. Door de recente onthullingen omtrent de activiteiten van veiligheidsdiensten lijkt er van een kentering sprake.

In deze verkenning is ingegaan op de privacy aspecten van Big Data analysis binnen het domein Veiligheid en Justitie. Besproken zijn toepassingen binnen de rechtspraak zoals voorspellen van uitspraken en gebruik in rechtszaken. Met betrekking tot opsporing is onder andere ingegaan op predictive policing en internetopsporing. Na een uiteenzetting van de privacy normen en toepassingsmogelijkheden, zijn de volgende zes uitgangspunten voor Big Data toepassingen voorgesteld:

1. Bepaal te analyseren probleem en definieer doel voor verwerking
2. Selecteer data en beperk verzamelen
3. Bewaar niet langer dan noodzakelijk
4. Wees transparant
5. Beveilig informatie
6. Evalueer de uitkomsten kritisch

Binnen justitie zijn er op dit moment al Big Data toepassingen, zoals [de Web Voyager](#), die grote hoeveelheden data van het internet analyseert op zoek naar verdachte patronen. Door berichtgeving over PRISM wordt de vraag waar de grenzen van verwerkingen van Big Data liggen nadrukkelijker gesteld dan voorheen. Deze grenzen zijn uit de aard van de te verrichten activiteiten bij veiligheidsdiensten minder scherp dan bij de opsporing en vervolging.

Lees (of download) [het hele onderzoek](#) via de website Secure Computing.



WebVoyager

WebVoyager is een instrument ontwikkeld door en voor de Nationale Politie waarmee illegale zaken op het open internet, dakweb en social media onderzocht kunnen worden. [WebVoyager](#) maakt het internet op een veilige en forensisch verantwoorde manier doorzoekbaar voor opsporingsdiensten.

In ons politiewerk zoeken we vaak naar allerlei soorten van informatie. We maken hiervoor vooral gebruik van politieregisters. Wat hierin staat, kan gevonden worden, maar is dat ook alles en hebben we daar genoeg aan? Veelal jeukt het ons om ook even te Googelen. Het is vaak verrassend wat je op het internet kunt vinden over zaken of personen.

Het internet heeft nog meer voordelen, namelijk dat er vaak gemakkelijk relaties tussen zaken, locaties en personen gevonden kunnen worden. Er zijn vaak veel potentieel identificeerbare gegevens rondom personen en zaken te vinden, zoals aliases, nicknames, social media accounts, maar ook wat complexere zaken zoals Bitcoins of Google Analytics accounts.

Het vinden en analyseren van deze informatie is handmatig eigenlijk niet te doen, al was het alleen maar om dat veel van deze informatie alleen 'onderwater' beschikbaar is. Google en andere zoekmachines vinden niet alles en laten ook nog eens niet alles zien. Je Google profiel bepaalt en beïnvloedt grotendeels je zoekresultaten. Ook laat je onbewust een herleidbaar spoor na van je zoektocht.

Er zijn de afgelopen jaren op diverse onderwerpen binnen de politie en andere opsporingsdiensten initiatieven gestart om het zoeken op internet vorm te geven.

Binnen WebVoyager zijn en worden de verschillende initiatieven bij elkaar gebracht zodat de kennis en kracht gebundeld kunnen worden.



Drugshandel via internet

Een analyse van de aard, de omvang en de rol van Nederland.

Het internet heeft over de afgelopen decennia een aanzienlijke impact gehad op een aantal sectoren in de economie. E-commerce heeft de efficiëntie van productieketens verbeterd, de toegang tot internationale markten vereenvoudigd en de transparantie voor consumenten verbeterd. Dat het internet ook een rol kan spelen bij het faciliteren van drugshandel werd voor het eerst echt duidelijk door het succes van Silk Road: de eerste grote online illegale marktplaats op het zogenaamde dark web. Silk Road werd door de FBI neergehaald in oktober 2013, maar andere, zeer vergelijkbare, markten vulden die ruimte alweer binnen enkele weken.

Vandaag de dag zijn er ongeveer 50 zogenoemde cryptomarkten en webshops die alleen toegankelijk zijn met behulp van encryptiesoftware. We gebruiken de term 'cryptomarkten', maar er wordt ook wel verwezen naar 'dark net markten' (DNMs). Cryptomarkten lijken qua uiterlijk veel op online marktplaatsen, zoals Marktplaats.nl of eBay, ook omdat het mogelijk is voor gebruikers om naar advertenties te zoeken en deze vergelijken en om verkopers te beoordelen met feedback. Cryptomarkten brengen verkopers en kopers samen, zodat ze onder pseudoniem illegale drugs, nieuwe psychoactieve stoffen (NPS), medicijnen en andere, vaak illegale goederen en diensten kunnen verhandelen. Het zijn echter niet alleen de donkere krochten van het internet waar drugs worden aangeboden. Er zijn talloze webwinkels op het open internet (het zogenoemde clear net) die gemakkelijk te vinden zijn met zoekmachines en die voornamelijk NPS, ook wel bekend als designer drugs, aanbieden die (nog) niet officieel zijn verboden.

Buiten het internet, heeft Nederland een centrale positie in Europese illegale drugsmarkten. Volgens het Europese Monitoring Centrum voor Drugs en Drugverslaving (EMCDDA) is Nederland de belangrijkste producent van xtc en cannabis en een belangrijke doorvoerhaven voor de distributie van hasj en cocaïne. Of die cruciale rol voor Nederland zich ook uitstrekt tot het handel via het internet is nog onduidelijk. Er is voldoende media-aandacht voor internet-gefaciliteerde drugshandel, maar harde cijfers over de omvang, aard en ontwikkeling zijn er nauwelijks.

Lees (of download) [het hele onderzoek](#) via de Secure Computing website.



Toegangsblokkade gratis WiFi-hotspots opheffen

Bij de meeste gratis WiFi-hotspots moet eerst via de hotspot-pagina akkoord worden gegaan met de algemene voorwaarden voordat gratis gebruik kan worden gemaakt van de WiFi. Is de startpagina van de browser echter ingesteld op een webpagina met een met HTTPS beveiligde verbinding (hetgeen steeds vaker het geval is), dan kan dat problemen opleveren bij het doorlinken naar de hotspot-pagina: er wordt een foutmelding getoond dat er geen verbinding met de server kan worden gemaakt.

De oplossing is gelukkig eenvoudig: bezoek een webpagina die gebruik maakt van een normale HTTP-verbinding (in plaats van HTTPS, bijvoorbeeld <http://www.nu.nl>), hierdoor zal de redirect naar de algemene voorwaarden van de gratis hotspot wèl goed werken.



Ransomware bepaalt losgeldbedrag per slachtoffer

De nieuwe soort ransomware Spora kan beoordelen of slachtoffers zakelijke gebruikers of consumenten zijn, en past daar de hoogte van het gevraagde losgeld op aan.

De gijzelsoftware richt zich voor zover bekend enkel op Russische gebruikers, meldt Bleeping Computer. Besmetting gebeurt net als bij de meeste ransomware wanneer gebruikers een malafide bestand downloaden en openen.

In tegenstelling tot bij de meeste afpers-malware heeft Spora daarna geen internetverbinding nodig. De ransomware gaat zonder aanwijzingen van een server aan de slag en versleutelt bestanden met extensies als .doc, .jpg, .pdf, .psd en .zip.

Eenmaal versleuteld geeft de ransomware het slachtoffer een infectie-ID en een logbestand. Dat bestand moeten mensen uploaden naar een beveiligde site via de anonieme Tor-browser, waar ze moeten inloggen het infectie-ID.

Betaling

Op basis van het logbestand bepaalt de site van de Spora-ontwikkelaars of het slachtoffer zijn computer zakelijk of particulier gebruikt. Op basis daarvan wordt het geëiste losgeld berekend. Gebruikers kunnen daarna al hun bestanden laten ontsleutelen en tegen extra betaling ook immuniteit voor verdere Spora-infecties kopen en alle Spora-bestanden van hun computer laten verwijderen.

Prijzen voor het ontsleutelen van bestanden lopen volgens Bleeping Computer uiteen van 79 dollar tot 280 dollar. Het losgeld moet met digitale valuta bitcoin worden betaald, gebruikelijk in het geval van ransomware.

De versleuteling die wordt toegepast is volgens beveiligingsbedrijf Emisoft geavanceerd. Bestanden worden per stuk versleuteld en kunnen alleen worden ontsleuteld wanneer de digitale sleutel van de ransomware-maker bekend is. Na betaling krijgen gebruikers een bestand waarmee zij hun eigen bestanden weer kunnen ontsleutelen.

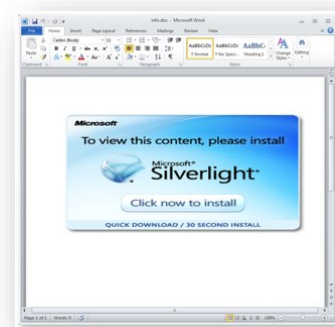


Silverlight-update in document blijkt keylogger

Onderzoekers waarschuwen voor een recent ontdekte campagne gericht tegen een financieel dienstverlener waarbij Word-documenten werden gebruikt die zogenaamd een Silverlight-update aanboden. In werkelijkheid ging het om een embedded Visual Basic-script dat een keylogger installeerde.

Dat laat beveiligingsbedrijf Proofpoint weten. Volgens het bedrijf is de aanval opvallend omdat die gericht was tegen een enkele organisatie. Daarnaast gebruikten de aanvallers geen macro's maar een embedded object dat een kwaadaardig script bleek te zijn. Dit script installeerde weer een keylogger die informatie van de computer naar twee Gmail-adressen doorstuurde.

Om de aanval te laten slagen moest het slachtoffer de zogenaamde Silverlight-update wel aanklikken en uitvoeren. "Hoewel het gebruik van embedded objecten in plaats van macro's niet nieuw is, blijven kwaadaardige macro's op dit moment de favoriete keuze van aanvallers.



Update voor Windows-beveiligingstool EMET

Microsoft heeft een nieuwe versie van de gratis [Windows-beveiligingstool EMET](#) uitgebracht die een aantal kleine verbeteringen bevat. EMET staat voor Enhanced Mitigation Experience Toolkit (EMET) en voegt een extra beveiligingslaag aan Windows en geïnstalleerde applicaties toe.

Deze extra beschermingslaag moet het lastiger voor aanvallers maken om zowel bekende als onbekende kwetsbaarheden in het besturingssysteem of geïnstalleerde programma's of plug-ins aan te vallen. Ook kan EMET systeembeheerders een waarschuwing geven als een applicatie door een mogelijke aanval is gecrasht. De beveiligingstool wordt dan ook door menig expert en organisatie aangeraden.

Microsoft is ondanks kritiek van beveiligingsexperts van plan om de ondersteuning van EMET op 31 juli 2018 stop te zetten. In de tussentijd zullen er echter nog steeds updates voor de beveiligingstool verschijnen, zoals de nu verschenen versie 5.52. In deze versie zijn verschillende bugs opgelost die voor vastlopers of andere problemen konden zorgen. Microsoft spreekt dan ook over een kleine update.



Malware voor geldautomaten ondersteunt nu Windows 10

Malware waarmee criminelen de geldcassettes van geldautomaten kunnen legen en die al jaren in gebruik is ondersteunt nu ook Windows 10. Het gaat om de Ploutus-malware die voor het eerst in 2013 in Mexico werd gezien. Er is nu een nieuwe variant van de malware ontdekt, zo meldt beveiligingsbedrijf FireEye.

Om de malware te installeren moeten criminelen fysieke toegang tot de automaat hebben. Eenmaal actief maakt ook de nieuwste variant het mogelijk voor katvangers om in een paar minuten grote bedragen uit de geldautomaat te stelen. Hiervoor zijn wel enkele stappen vereist. Zo moet de katvanger de geldautomaat fysiek zien te openen om vervolgens een extern toetsenbord aan te kunnen sluiten. Hierna moet een activatiecode worden opgegeven om de geldcassettes te legen.

De nieuwste versie van Ploutus bevat verschillende nieuwe eigenschappen. Zo ondersteunt de malware Windows 10 alsmede het Kalignite-platform voor geldautomatenplatform. Dit platform draait op de geldautomaten van 40 verschillende fabrikanten die in 80 landen worden gebruikt. De nu ontdekte variant is echter ingesteld om alleen Diebold-geldautomaten te infecteren. Daarnaast schakelt de malware ook aanwezige beveiligingsprocessen uit om detectie te voorkomen. Volgens FireEye is de malware al actief door criminelen gebruikt om geldautomaten te legen.



Politie verwacht bewijs via Internet of Things

Het 'Internet of Things' is de plaats delict van de toekomst, voorspelt Mark Stokes, chief digital forensics bij Scotland Yard. IoT-apparaten bevatten zo veel data dat de politie daar misdrijven mee kan oplossen.

Stokes wijst op slimme koelkasten en deurbellen die via draadloze camera's dan wel smartphone-apps data genereren. 'Al dat soort zaken laten een spoor achter'. Volgens Stokes worden (Britse) agenten en forensisch onderzoekers 'op dit moment' getraind om naar gadgets en ander witgoed te kijken die een digitale voetafdruk van het slachtoffer of de dader kunnen achterlaten.



Tubrosa virus laat je pc ongewenst Youtube video's bekijken

Symantec waarschuwt voor het zgh. Tubrosa virus. Dit virus zorgt ervoor dat jouw pc wordt gebruikt om video's op Youtube te bekijken zonder dat je het zelf door hebt. De virusschrijvers / cybercriminelen verdienen aan de advertentie-inkomsten die op de video's zitten.

De cybercriminelen copieren een populaire video op Youtube in hun eigen Youtube kanaal waarvan zij de advertentie-inkomsten krijgen. Voor Youtube lijkt het alsof de bezoekers steeds een andere verbinding gebruiken dus ze worden als unieke bezoekers geregistreerd. Ook al komt het verkeer van een en dezelfde computer.

Politie pakt jihad via sociale media harder aan

De politie gaat online oproepen tot geweld door moslimfundamentalisten steviger aanpakken. Een team van de Landelijke Eenheid krijgt als hoofdtaak om jihadpropaganda op openbare sociale media te bestrijden. Het team identificeert, duidt en meldt bepaalde content aan internetbedrijven met het oog op verwijdering.

Tot de werkwijze behoort ook het afstemmen van meldingen en het delen van content met relevante partijen binnen en buiten de politie. Het team heeft de naam Nederlandse Internet Referral Unit (NL IRU) en werkt nauw samen met een Europees IRU-team van Europol.

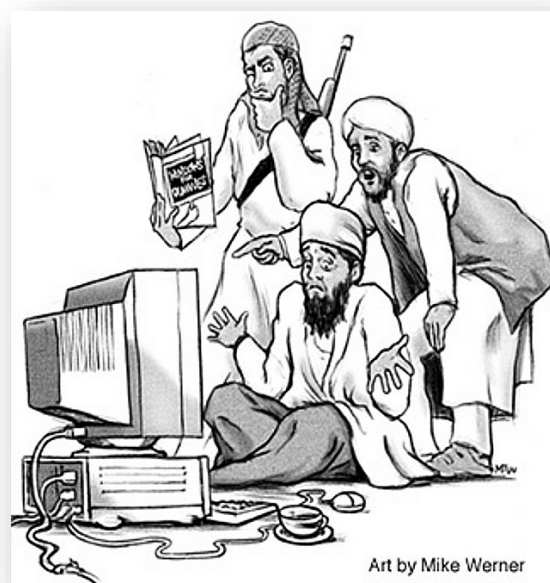
De eenheid is opgericht als onderdeel van het Actieprogramma Integrale Aanpak Jihadisme van de Nederlandse regering. In maart 2016 startte een team van vier politiemedewerkers. Na een proefperiode waarin werkwijzen, facilitaire voorzieningen en juridische kaders zijn afgestemd gaat de eenheid nu officieel van start en wordt het team uitgebreid met vijf operationeel specialisten.

De politie: 'De aanpak die de NL IRU hanteert, is gebaseerd op de methode Notice and Take Action (NTA): het identificeren, duiden en melden van bepaalde content aan internetbedrijven, met het oog op verwijdering. Tot de werkwijze behoort ook het afstemmen van meldingen en het delen van content met relevante partners binnen en buiten de politie, waaronder de EU IRU van Europol. Beide IRU's vullen elkaar aan, waarbij het Nederlandse team zich meer specifiek richt op content die het publiek in ons land beoogt te bereiken.'

Strafbare feiten

Samen met het Openbaar Ministerie is een kader vastgesteld, waarin de bescherming van de vrijheid van meningsuiting wordt afgewogen tegen de noodzaak van verwijdering. Volgens dat kader beperkt de politie de NTA-methode tot de strafbare feiten opruiing en werven voor de gewapende strijd.

Vrijdag 13 april 2016 maakte de politie ook bekend dat tien nieuwe cyberteams worden opricht. Korpchef Erik Akerboom meldde in een interview met Nu.nl dat de politie veel digitaal specialisten werft die beschikken over specifieke ict-kennis. De politie is nu bezig om honderd specialisten te werven die internetcriminaliteit aanpakken en gaat dat in 2018 herhalen.



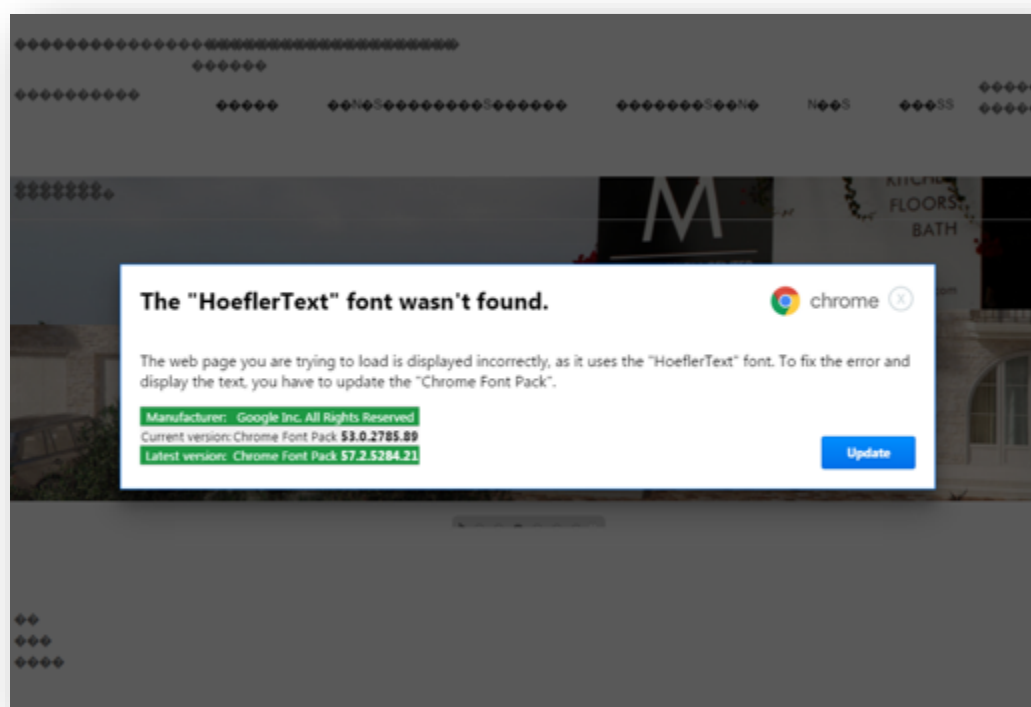
Chrome-gebruikers doelwit van zogenaamde font-update

Chrome-gebruikers zijn het doelwit van een nieuwe aanval waarbij cybercriminelen gehackte websites onleesbaar maken om de gebruiker zo een zogenaamde font-update te laten installeren. In werkelijkheid gaat het om malware. Aanvallers voorzien de gehackte websites van kwaadaardige code.

Deze code controleert of de gebruiker aan bepaalde eisen voldoet, zoals land, browser (Chrome op Windows) en juiste referer. Als aan deze eisen wordt voldaan maakt de kwaadaardige code de website onleesbaar. Vervolgens verschijnt er een pop-up die stelt dat het "HoeflerText" font niet is gevonden en het "Chrome Font Pack" moet worden bijgewerkt. De pop-up is volgens beveiligingsbedrijf Proofpoint niet via het kruisje te sluiten.

Wanneer de gebruiker voor de optie "Update" kiest wordt het bestand "Chrome_Font.exe" gedownload. Als de gebruiker dit bestand opent zal de Fleercivet-malware worden geïnstalleerd. Deze malware gebruikt de computer voor het plegen van advertentiefraude waarbij de computer onzichtbaar voor de gebruiker in de achtergrond allerlei websites en advertenties opent. De criminelen worden voor deze frauduleuze impressies en clicks betaald.

Volgens Proofpoint wordt het steeds lastiger voor cybercriminelen om internetgebruikers via exploitkits te infecteren, die misbruik van bekende beveiligingslekken maken die niet door de gebruiker zijn gepatcht. Daarom wordt er voor social engineering gekozen waarbij de gebruiker wordt verleid zelf zijn eigen systeem met malware te infecteren.



Zeven misverstanden over algemene voorwaarden

Algemene voorwaarden zijn verplicht.

Onzin. De wet eist nergens dat een ondernemer algemene voorwaarden voert. Het kan handig zijn, omdat je zo standaarddingen alvast geregeld hebt, maar dat is natuurlijk nog lang niet hetzelfde als ‘verplicht’. In de internetcontext zijn AV alomtegenwoordig, maar dat komt a) omdat de wet heel weinig regelt dus je kunt maar beter zelf aan de bak en b) omdat iedereen elkaar na-aapt als dat het zou moeten.

Algemene voorwaarden moeten worden gedeponeerd.

Onzin. De wet eist dat je je AV bijvoegt bij je offerte of dat je er in het online bestelproces naar verwijst. (Dienstverleners mogen soms volstaan met een bordje met aankondiging dat er AV zijn.) Deponeren is juridisch onzin, tenzij je de Albert Heijn of de NS bent – dan mag je ze deponeren in plaats van ter hand stellen.

Een webwinkel moet een vinkje laten zetten bij algemene voorwaarden.

Onzin. Volgens de wet moeten algemene voorwaarden van toepassing worden verklaard. Dat doe je door te zeggen “De algemene voorwaarden zijn van toepassing” in het bestelproces en door te verwijzen naar de vindplaats, maar een vinkje is niet nodig.

Alleen de inhoud van dat aparte document zijn algemene voorwaarden.

Onzin. Volgens de wet zijn algemene voorwaarden “voorwaarden die bestemd zijn om in meerdere overeenkomsten gebruikt te worden”, en het doet er dus niet toe of ze in een document staan dat “Algemene voorwaarden” of iets dergelijks heet. Ook bepalingen in een gewoon contract kunnen algemene voorwaarden zijn, en ook die bolletjes met “Betalingstermijn 30 dagen / Apparatuur alleen fabrieksgarantie” in de offerte zijn algemene voorwaarden als je ze naar meerdere klanten voert.

Algemene voorwaarden staan naast het contract.

Onzin. Algemene voorwaarden zijn voorwaarden die bedoeld zijn voor meerdere overeenkomsten, maar als ze correct van toepassing zijn verklaard, zijn ze gewoon deel van de overeenkomst. Ze hebben geen automatisch hogere of lagere status. Het enige is dat als een maatwerkafpraak in strijd is met een algemene voorwaarde, de maatwerkafpraak wint.

Algemene voorwaarden mogen eenzijdig worden gewijzigd.

Onzin. Natuurlijk mag je van tijd tot tijd nieuwe algemene voorwaarden publiceren, alleen die gelden dan niet voor bestaande overeenkomsten. De AV van een bestaand contract wijzigen mag alleen met toestemming van je wederpartij. Die kun je vooraf bedingen (in je oude algemene voorwaarden dus), maar het is en blijft een wijziging met toestemming.

Algemene voorwaarden mogen niet in strijd zijn met de wet.

Niets mag in strijd zijn met de wet. Het lastige is alleen dat in het contractenrecht een hoop wettelijke regels niet dwingend zijn, maar ‘regelend’ zoals juristen dat noemen. Het zijn defaults, in IT-taal. Als je bijvoorbeeld geen betalingstermijn afsprekt met je klant, dan zegt de wet (art. 6:119a BW) dat hij binnen 30 dagen moet betalen. Maar je mag 14 dagen, of 45 of zelfs 60 afspreken als je daar zin in hebt. (Meer dan 60 mag dan weer niet, tenzij als maatwerkafpraak en er hele goede redenen voor zijn.)



...verder op de website oa

Hoe wij te lui zijn om onszelf te beveiligen op het internet

Gratis tool vindt door ransomware versleutelde bestanden

Betere bescherming gebruikers van e-diensten

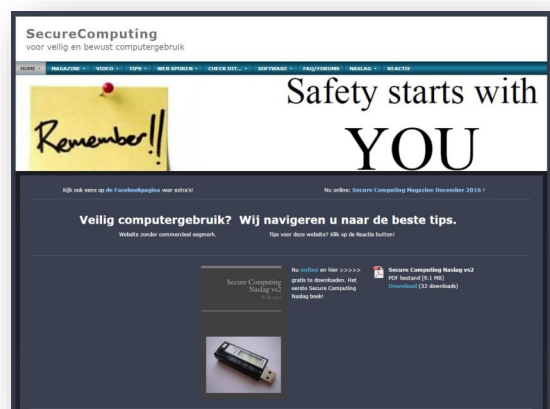
Netgear waarschuwt voor wachtwoordlek in routers

Politie waarschuwt voor niet afgeschermd Facebookprofielen

Onderzoekers: Mensen overmoedig bij phishingmails

.... en meer

(in het kader van actualiteit blijven de artikelen maximaal 2 weken na verschijnen van het Magazine beschikbaar op de website)



...verder op de Facebook pagina oa

Belastingdienst waarschuwt voor Whats Appjes

HP roept wereldwijd explosieve laptopbatterijen terug

Zo schakel je One Drive uit

Cyberdefensie ontleed (download het gratis dossier)

Satan is nieuwe ransomware-as-a-service

Pas op voor populaire foto-app Meitu

Verwijder onnodige rommel uit het rechtermuisklikmenu

Metadata van foto's bekijken en toevoegen

Internetgadgets die precies vertellen wat je kind online doet

.... en meer

Cops in cyberspace

Juridisch zeer interessant is een moordonderzoek in de Arkansas, VS.

Daar weigert webwinkel Amazon de politie van Bentonville gegevens te verstrekken waarop mogelijk moordverdachte Andrew Bates en zijn slachtoffer te horen zijn. Het gaat om Echo, de voice-app van Amazon, een apparaat dat altijd 'aan' staat en reageert op 'wекwoorden'. De politie hoopt dat de app (achtergrond)geluiden heeft opgenomen die de moord kunnen aantonen. Standaard worden alle Echo-conversaties door Amazon bewaard, zogenaamd om het systeem te laten leren en te verbeteren. Amazon heeft al metadata vrijgegeven, hoe laat activeerde Bates de app, hoe lang, wat kocht hij etcetera, maar nog niet de inhoud. Vanwege privacy uiteraard. Bates' advocaat is het daar mee eens. 'I have a big problem that law enforcement can use the technology that advances our quality of life against us'. De politie vindt zulke 'bronnen' uiteraard geweldig. Zo werd in de zaak al met de 'slimme' watermeter van Bates aangetoond dat hij in de nachtelijke uren na de moord ruim 530 liter water verbruikte – het slachtoffer werd dood gevonden in het Bates' hot tub – om sporen van de moord weg te spoelen, denkt de politie. Privacyorganisaties hebben al kritiek op het ongebreidelde gebruik van al deze big data. 'At a time when we have any number of devices tracking and automating our habits at home, should that information be used against us in criminal cases?'

De politie Noord-Nederland heeft twee jongeren (17 en 22, uit Hoogerveen) aangehouden die worden verdacht van meerdere winkeldiefstallen. De aanhoudingen volgden na tips uit een Whatsapp-groep voor winkeliers. Die leverden een duidelijk signalement zodat het duo kon worden aangehouden. Op heterdaad: ze waren nog in bezit van een tas met gestolen kleding.

De politie heeft bij een man uit Landgraaf 'een grote hoeveelheid' gegevensdragers in beslag genomen. De verdachte is mogelijk de man die zich in de facebookgroep Lesbische Vrouwen 25+ 'Cindy Klaassen' noemde en

onder die identiteit 25 lesbische vrouwen uit Nederland en België bedroog. Die vrouwen stuurden naaktfoto's en -filmpjes naar Cindy, waarop ze seksuele handelingen uitvoerden. Later werden ze met die beelden afgeperst. Een van de slachtoffers werd vier jaar lang aan het lijntje gehouden. 'Ze was altijd heel erg lief en zorgzaam, ik kreeg zelfs gevoelens voor haar'. Andere slachtoffers vonden haar 'opdringerig seksueel'. Afspraken met Cindy werden iedere keer op het laatste moment afgezegd. Eén slachtoffer (47, uit Cuijk) zette alles op alles om Cindy te ontmaskeren. Met succes wist ze bij Facebook Inc het ip-adres van de computer van de bedreiger te verkrijgen. Via een civiele procedure liet ze beslag leggen op al diens gegevensdragers. Dat waren er nogal wat: 850 cd-roms, 31 harde schijven, drie laptops en een telefoon. De politie onderzoekt deze apparatuur nu. Zeven andere vrouwen deden inmiddels aangifte tegen Cindy. Dat ging niet eenvoudig, schrijven kranten. Zo kreeg een vrouw te horen dat aangifte niet mogelijk was, en kon een ander slachtoffer dat pas na drie pogingen doen. De politie Limburg wil niet inhoudelijk reageren en zegt alleen dat het 'een complexe zaak' is.

De politie Rotterdam krijgt weer eens onderuit de Twitter-zak. Ging het voor de jaarwisseling nog over tweets waarin daklozen herkenbaar in beeld waren, deze week werd getwitterd over een inbeslaggenomen jas van een dakloze. De jas, met V-embleem, was van een beveiligingsbedrijf en de enigen die daarin mogen rondlopen zijn gecertificeerde beveiligers. De commotie was voor NRC aanleiding er een Stelling van de Week van te maken: de politie moet stoppen met 'het vernederen van daklozen' op twitter. Daarmee eens is GL-raadslid Arno Bonte die vindt dat het 'aan de schandpaal nagelen van de meest kwetsbaren in de samenleving' moet stoppen. 'Het afpakken van een jas is kinderachtig en menonwaardig bij vriestemperaturen'. Advocaat Richard Korver noemt het goed dat de politie alert is op gestolen kleding maar wijst ook op de Politiewet en de daarin vastgelegde hulp aan hen die dat behoeven. In een reactie zegt politiewoord-

voerster Miriam Slot dat 'een tweet van 140 tekens context mist'. Ze wijst op de spagaat: behalve voor zwervers 'die we richting zorg proberen te begeleiden', is de politie er ook voor bewoners en ondernemers 'die ons vragen iets te doen aan overlast'.

De Nederlandse internetprostitutiemarkt is booming, schrijft Revu. Het blad reed mee met het Prostitutie Controle Team van de politie Oost-Nederland dat 'een exclusief kijkje' bood 'in de schrijnende wereld achter de online seksadvertenties'. PCT-experts controleren niet alleen seksinstellingen maar monitoren ook het online aanbod van prostituees, zo'n vijftig tot zestig sekssites. Teamcoördinator Johan Stam ziet juist online 'relatief veel slachtoffers die seksueel worden uitgebuit'. Waar het aantal legale bordelen afneemt, stijgt het aanbod online. Waar 'het ene na het andere sekshuis' sluit, groeit het aanbod op sites als Sexjobs, Kinky en Citygirl vrijwel dagelijks. Zo zijn er in Oost-Nederland nog maar 68 vergunde seksinrichtingen (in 2013 nog 85) maar zijn er dagelijks wel tussen de 800 en 1200 niet-vergunde dames online. Voor heel Nederland zijn dat er 'op een doorde weekse dag' ongeveer zesduizend, ziet Stam. 'De markt heeft zich verplaatst naar het ondergrondse, illegale circuit, dat onmiskenbaar verband houdt met de stijging van het online aanbod'. Online vallen vooral prostitutees op die 24/7 beschikbaar zijn, 'een einde-loze reeks' aan seksuele handelingen aanbieden, inclusief onbeschermd seks en waarvan de profielteksten soms overduidelijk door een ander geschreven zijn, of vertaald door Google. 'Als er staat "mijn vriendje neemt op", is dat geen goed teken'. Stam vreest de effecten van de nieuwe Wet Regulering Prostitutie, waarbij thuiswerkers geen vergunning meer nodig hebben. Een rampsценario, vreest Stam. 'Door te stellen dat de zelfstandig werkende prostituee niet meer bedrijfsmatig opereert en geen vergunning nodig heeft, heb je dadelijk geen reden meer om te controleren'. Mensenhandel kan dan een ongewenst neveneffect zijn.

Rechtspraak

De politierechter in Alkmaar heeft een man (26, uit Hoorn) veroordeeld tot twee maanden celstraf voor witwassen. De verdachte had zijn bankrekening 'uitgeleend' aan ene Ismael, die er zijn zogenaamd met zwart werken verkregen inkomsten kon storten. In werkelijkheid bleek deze Ismael een oplichter die (natuurlijk niet bestaande) last minute-kaartjes voor concerten verkocht via Marktplaats en facebook. Op rekening van de verdachte werd enkele duizenden euro's gestort. Hij moet verder 1200 euro aan schadeclaims door gedupeerden vergoeden.

Het gerechtshof in Den Bosch heeft 23 verdachten in de 'Valkenburgse zedenzaak' een taakstaf opgelegd en vier verdachten vrijgesproken. De 23 veroordeelde mannen, verdacht van ontucht met de (toen) 16-jarige 'Kimberley' in een hotel in Valkenburg, hebben volgens het Hof 'onvoldoende gecontroleerd' of het meisje meerderjarig was. De mannen hadden gereageerd op een internet-advertentie waarin stond dat het meisje 18 was. 'De mannen hadden dit nauwkeurig moeten controleren en dat hebben zij niet gedaan' waardoor ze feitelijk bij een minderjarige terechtwamen. Onduidelijk blijft wát die mannen dan precies hadden moeten doen. In de zaak werden uiteindelijk tachtig klanten geïdentificeerd, twee pleegden zelfmoord, dertig werden vervolgd. De rechtbank had de meeste verdachten eerder tot één dag celstraf en een taakstraf veroordeeld. Het OM ging in beroep en eiste wederom langere celstraffen. Zonder succes: het Hof vindt onvoorwaardelijke gevangenisstraffen te zwaar. Sterker nog, de ene verdachte die van de rechtbank vijf maanden kreeg, hoeft van het Hof maar één dag te zitten. 'Het meest passend' is volgens het Hof een taakstraf, in combinatie met 'een zeer beperkte gevangenisstraf'. De opgelegde taakstraffen variëren van 90 uur taakstraf tot 240 uur en zijn gebaseerd op de verrichte seksuele gedragingen en de mate waarin de verdachte 'alert is geweest op de mogelijkheid dat hij met een minderjarige prostituee van doen had'. Ook woog mee of de verdachte zich uit eigen beweging bij de politie had

gemeld. Vier verdachten werden vrijgesproken. Uit het simpele feit dat hun namen in de telefoon van het meisje stonden, kan niet worden afgeleid dan wel bewezen dat ze ook seks met haar hadden. Het OM gaat mogelijk in cassatie tegen de uitspraak. Kimberley's pooier Armin A. kreeg overigens al eerder twee jaar cel.

Facebookterrorist' Ibrahim T. (28, uit Druten) moet 750 euro boete betalen voor het verspreiden en tonen van opruiende teksten. Hij kreeg verder, conform de eis van het OM, twee maanden voorwaardelijk. De verdachte zette vlak na de aanslagen op Zaventem (maart 2016) opruiende teksten op facebook. 'Nu mag heel Europa branden' schreef hij onder meer. T. was secretaris van de plaatselijke moskee maar werd na zijn arrestatie uit het bestuur gezet. Hij radicaliseerde enkele jaren geleden, speelde strijdliederen in zijn auto, hing een IS-vlag in de slaapkamer en postte regelmatig extremistische teksten op facebook. Het OM vond dat vrijheid van meningsuiting 'nooit een vrijbrief mag zijn voor het plegen van een misdrijf' en klaagde de man aan. Tegen de politie zei T. dat hij achter zijn uitspraken blijft staan. 'Het is hoe ik erover denk'. De rechtbank wil met de boete vooral duidelijk maken dat zijn gedrag strafbaar is.

De vloggende rapper Boef, echte naam Soufiane Boussaadia, is door de politierechter veroordeeld tot tachtig uur werkstraf (de helft voorwaardelijk, proeftijd twee jaar) voor het beledigen van een politieagent. De rapper had, september 2016, in een van zijn vlogs opgeroepen tot een vechtpartij in Tilburg. Hij werd daarvoor opgepakt en vastgezet. Een uur na zijn vrijlating, zette hij een video online waarin hij dreigde seks te hebben met de dochter van een rechercheur. Naar eigen zeggen was dat 'artistieke vrijheid' maar daar geloofde de rechter geen snars van. 'Alles wat ik doe is kunst', probeerde Boef nog maar tevergeefs. Hij moet de agent verder 150 euro schadevergoeding betalen. Het OM had, behalve de schadevergoeding, honderd

uur werkstraf en twee weken voorwaardelijke celstraf geëist.

De kinderrechtter in Middelburg heeft drie tieners veroordeeld tot werkstraffen van tachtig uur voor een inbraak in een strandtent. De verdachten (twee van 16 uit Vlissingen, een van 15 uit Middelburg) hadden bij de inbraak niet door dat ze werden gefilmd. Toen de eigenaar van de strandtent dreigde die (herkenbare) beelden op facebook te zetten als ze zich niet zouden melden, keerden ze terug en bekenden. Een vierde verdachte die niets gestolen had, werd vrijgesproken. De buit bedroeg overigens niet meer dan 35 euro. Wel was er voor vijf mille schade aangericht. De jongens moeten daarom 2500 euro schadevergoeding betalen.

De agent die in 2015 op facebook een foto plaatste waarin hij zwarte Amerikanen vergeleek met apen, is in hoger beroep vrijgesproken. Agent Hans V. (52, uit Gent) zette, augustus 2015, een foto online waarop zwarte Amerikanen op een politiebureau dansten plus een waarop bavianen die auto besprongen. 'Zoek de verschillen', schreef hij daarbij. 'Die apen kan je nog iets aanleren. Die zwarten uit de jungle niet'. Bij een andere foto, van een vluchteling uit Syrië, schreef hij dat deze 'onderweg was naar een levenslange all-inclusive vakantie in Nederland en België'. Volgens het parket zijn er voldoende aanwijzingen voor discriminatie, maar de rechtbank sprak hem vrij. Het hof van beroep heeft die uitspraak nu bevestigd. 'Niet bewezen is dat hij tot haat wilde aanzetten'. De agent moet voorlopig nog 'binnendienst' doen en kreeg al een tuchtstraf.

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 vervolghandelingen		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 internetverkeer	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 toegangscode 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 veiligheid](#)
4. [High Tech Crime](#)
5. [Data in onderwijs](#)
6. [Cybersurveillance](#)
7. [Techtrends in onderwijs](#)
8. [Veilig internetten](#)
9. [MKB cyber secure](#)
10. [Cyberellende bij Tek Tok](#)
11. [Standaarden en keurmerken](#)
12. [Operation Hijg Tech Crime](#)
13. [Kraak van de Maand](#)

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](#)
[Webinar Computercriminaliteit](#)
[Mousejack](#)
[Gegijzeld door Ransomware.](#)
[Wat nu?](#)
[Telefonische phishing](#)

Help wanted:

[Grooming](#)
[Sexting](#)
[Webcammisbruik](#)
[Bedreigd/gechanteerd](#)
[Kinderporno](#)
[Nepprofiel](#)



Handig

Phishing- / valse e-mails melden:

ABN AMRO Bank: valse-email@nl.abnamro.com

ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

ICS- / ABN AMRO creditcards: valse-email@icscards.nl

[Tips](#) voor veilig handelen op Marktplaats

Internetoplichting: controleer vooraf de (bank)gegevens van de verkoper via

www.mijnpolitie.nl/miocheck

Komt de verkoper voor op de website [Opgelet op internet](#) ?

[Malware ID](#) website met info omtrent verwijderen van infecties

[PCrisk](#) verwijderingsrichtlijnen voor spyware en virussen

[Cookie Verwijderen](#) kennisdatabase voor het verwijderen van adware, hijackers, ransomware, toolbars en pop-ups

Computer [woordenboek](#)

Secure Computing [Naslag](#)

Veel meer handige tips vindt u op de Secure Computing [website](#).