Jaargang 2 Mei 2018

Veilig Digitaal Magazine

- *Hackersgroep GOLD LOWELL zit achter je geld aan*
- *Nederlander gaat massaal gebruikmaken van nieuwe privacyrechten*
- *Coprocessor-aanvallen: een verborgen dreiging*
- *General Data Protection Regulation (GDPR)*
- *Zo verwijder je alles wat Google van je weet*
- *VVD wil superspoedprocedure om seks- en naaktfilmpjes offline te krijgen*
- *Windows wachtwoord achterhalen met Ophcrack*

INDEX

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

Nederlander gaat massaal gebruikmaken van nieuwe privacyrechten

Nederlanders gaan massaal gebruikmaken van de rechten die de nieuwe privacywet hen biedt. Via de nieuwe Algemene Verordening Gegevensbescherming (AVG) die eind mei 2018 van kracht wordt, krijgen burgers onder meer het recht om al hun persoonlijke gegevens in te zien, te verwijderen, en om onjuiste persoonlijke gegevens te corrigeren.

“Gewezen op hun nieuwe rechten, wil meer dan 80% in actie komen. Dat betekent dat bedrijven en instanties hun borst kunnen natmaken”, aldus Koos Wolters, privacy expert van KPMG. In het licht van het aanstaande referendum over de vernieuwde Wet op de inlichtingen- en veiligheidsdiensten is het ook opvallend dat bijna de helft van de Nederlanders privacy inlevert voor veiligheid.

Bedrijven en instanties moeten alle zeilen bijzetten.
Uit dit opinieonderzoek blijkt dat minder dan 20% van de Nederlanders op dit moment op de hoogte is van de nieuwe wetgeving die in mei van kracht wordt. Wolters: “Als straks het besef doorklinkt welke rechten burgers krijgen, zullen organisaties alle zeilen bij moeten zetten om aan alle eisen te voldoen. Immers, organisaties die hun maatregelen op orde hebben, genieten meer vertrouwen bij consumenten waardoor zij sneller toegang krijgen tot persoonsgegevens.”

Nederlanders willen vooral weten wie wat verzamelt. Meer dan 80% vindt dat bedrijven en instanties die beschikken over bijzondere persoonsgegevens dit duidelijk moeten vermelden en moeten garanderen dat dit volledig privacyproof gebeurt.

Veiligheid belangrijker dan privacy.
Nederlanders vinden hun veiligheid belangrijker dan hun privacy. Bijna de helft (46%) van de Nederlanders is van mening dat de overheid meer bevoegdheden zou moeten krijgen om de criminaliteit terug te dringen, ook als dit ten koste zou gaan van de privacy.
Wolters: “Andersom is slechts 25% bereid om veiligheid in te leveren voor privacy. Overigens vindt een meerderheid van de Nederlanders dat de overheid er goed in geslaagd is de juiste balans te vinden in het borgen van veiligheid en privacy.”

Zorgen om bescherming medische gegevens .
Uit het onderzoek van KPMG blijkt dat Nederlanders zich met name zorgen maken om de wijze waarop wordt omgegaan met hun medische gegevens. 70% heeft twijfels over het gebruik van dit soort persoonlijke informatie, vooral in het elektronisch patiëntendossier (EPD).
Wolters: “90% heeft nog nooit het eigen EPD ingezien. Veel mensen zetten bovendien vraagtekens bij de veiligheid van hun gegevens bij de huisarts. Minder dan de helft van de Nederlanders denkt dat medische gegevens die worden bewaard door de huisarts of dokter goed beschermd zijn.”

Hackersgroep GOLD LOWELL zit achter je geld aan

Het gevaar van cyberaanvallen blijft alsmaar groeien. In de afgelopen een tot twee jaar zijn vooral ransomware-aanvallen ongekend populair. Criminele individuen en particuliere hackersgroepen, maar ook overheidsinstanties zitten achter deze aanvallen. Ook al hebben deskundigen vaak een vaag idee wie achter de aanvallen zitten en waar zij vandaan komen, het is buitengewoon lastig om precies aan te duiden wie de slechteriken zijn en hoe zij werken. Hiervoor is niet alleen een groot monitoring-network noodzakelijk maar het traceerwerk vraagt ook om tijd.

Secureworks, een leverancier van beveiligingsoplossingen dat gebruikmaakt van globale informatie over cyberaanvallen, achterhaalt regelmatig het gedrag van hackersgroepen. Zo zijn de onderzoekers van Secureworks Counter Threat Unit (CTU) eind 2015 begonnen financieel gemotiveerde campagnes te traceren waarbij de GOLD LOWELL genoemde groep gebruikmaakte van SamSam ransomware (ook wel bekend als Samas en SamsamCrypt).
Volgens het onderzoek van de CTU scant en exploiteert GOLD LOWELL bekende kwetsbaarheden in internetsystemen om een eerste voet aan de grond te krijgen in het netwerk van een slachtoffer. De cybercriminelen zetten vervolgens de SamSam ransomware in en eisen betaling om de data van het slachtoffer te ontsleutelen.

Geld, niet spionage
Het gebruik van bepaalde scan-and-exploit technieken van hackers om toegang te krijgen tot het netwerk van slachtoffers laat zien dat de aanvallen gericht zijn op systemen en protocollen die eerder door organisaties dan door particulieren worden gebruikt. De aanvallers mikken vooral op de netwerkrand en kiezen hun slachtoffers zorgvuldig om de kans op een succesvolle afpersing te verhogen. Bij de meeste slachtoffers van GOLD LOWELL die bekend zijn bij de CTU gaat het om kleine tot middelgrote organisaties. Sommige deskundigen beweerden na bekende SamSam-aanvallen in 2016 en 2018 dat GOLD LOWELL zijn pijlen vooral richt op de zorgsector. De verspreiding van de door Secureworks waargenomen activiteiten van de groep laat echter zien dat GOLD LOWELL zich niet beperkt tot een bepaalde branche of type organisatie.

De methode van GOLD LOWELL om eerst netwerktoegang te verkrijgen voor SamSam te installeren houdt potentieel een groot gevaar in voor het misbruik van de vertrouwelijke data op de systemen van de slachtoffers.
De anaslyse van de CTU geeft echter aan dat GOLD LOWELL financieel is gemotiveerd. De onderzoekers hebben geen indicatie gevonden dat de netwerktoegang misbruikt wordt voor spionage of datadiefstal.

Handige hackers
GOLD LOWELL gebruikt een combinatie van algemeen beschikbare en zelf ontwikkelde tools met publiek beschikbare exploits en technieken. Dat de groep een eigen ransomware toolkit wist te ontwikkelen suggereert dat de ontwikkelaars binnen de groep veel verstand hebben van encryptie en Windows netwerkomgevingen.

De aanvallers hebben laten zien dat zij in staat zijn om toegang te krijgen via internetsystemen, hun privileges naar hogere niveaus binnen het netwerk te escaleren en horizontaal binnen het netwerk uit te breiden.
In tegenstelling tot vele andere criminele activiteiten die gebruikmaken van ransomware vergen de methodes van GOLD LOWELL manuele interactie via het toetsenbord om een directe relatie op te bouwen tussen de aanvaller en zijn slachtoffer.

Om voor het betalen van het losgeld vertrouwen op te bouwen bieden de aanvallers hun slachtoffers test-decryptie van bepaalde data aan.

Wie zijn de slechteriken?
Taalfouten in GOLD LOWELL's losgeldeisen en communicatie tijdens de transacties doen vermoeden dat Engels niet de moedertaal van de aanvallers is. Tot vandaag de dag is de toeschrijving van de aanvallen aan een bepaalde groep onzeker omdat zij een beroep doen op publiek beschikbare tools, diensten en infrastructuren.

De consistentie van de methoden en tools die tijdens de SamSam-aanvallen sinds 2015 werden gebruikt zijn echter een indicatie dat GOLD LOWELL één groep is of een verzameling van nauw verbonden hackers.

Wat te doen?
De activiteiten van GOLD LOWELL zijn tussen 2015 en 2018 significant toegenomen. Dit geeft aan dat hun 'businessmodel' nog steeds goed werkt. Over de jaren heen heeft de groep haar methodes lichtjes aangepast.
Zij maakt nog steeds gebruik van publiek beschikbare tools maar heeft zijn eigen knowhow en programma's verder uitgebouwd om succesvol te blijven. De aanvallers komen het netwerk via internetsystemen binnen.

Daarom adviseren de CTU-onderzoekers aan organisaties om de security-protocollen voor deze systemen hoogste prioriteit te geven.

Software updates, regelmatige penetratietests, monitoren voor abnormaal gedrag en toegangscontrole staan boven aan de lijst van security-maatregelen.

Organisaties moeten ook hun weerbaarheid tegen ransomware-incidenten in kaart brengen. Denk eraan om noodplannen op te stellen en te testen, regelmatig back-ups van belangrijke data aan te maken en deze goed te beschermen.

Wifihackers richten pijlen op protocollen als Zigbee en bluetooth

Het uitvoeren van geavanceerde aanvallen op wifinetwerken is al lang niet meer weggelegd voor hackers met uitgebreide technische kennis.

Op internet staan allerlei toegankelijke tools waarmee zelfs amateurs een man-in-themiddleaanval op 802.11-netwerken kunnen opzetten en informatie kunnen stelen.

De bijna 3 miljoen online videohandleidingen en andere educatieve filmpjes rondom wifihacking maken het nog makkelijker om dit te leren.
Ook andere draadloze standaarden worden kwetsbaarder voor hackers. Dit hangt samen met de brede beschikbaarheid van software-defined radio's (SDR), een radiofrequentietechnologie die een apparaat in staat stelt om te communiceren met een groot frequentiebereik.

De eerste SDR-aanvalstools zijn al opgedoken, zoals HackRF One van Great Scott Gadgets. Op YouTube zijn talloze 'how to'-video's te vinden met instructies voor bijvoorbeeld het openen van autodeuren en het spoofen van gps-signalen.

Hackers kunnen hun hart ophalen, want het aantal producten met een draadloze verbinding blijft maar groeien. Van slimme auto's en alarmsystemen tot gasmeters en pacemakers: stuk voor stuk zijn ze interessant.voor hackers.

WatchGuard voorziet een breed scala aan nieuwe aanvalsmethoden waarbij met SDR-technologie data worden onderschept van devices die gebruikmaken van protocollen als Zigbee, Sigfox, bluetooth, RFID en LoRa.

Opkomst cyberverzekeringen stuwt ransomware

Cyberverzekeringen winnen aan populariteit. Zo'n cyberverzekering kan bijvoorbeeld worden afgesloten om de schade na een datalek te dekken, of de juridische kosten van een eventuele rechtszaak. Ook zijn er speciale pakketten rondom afpersing via internet, bijvoorbeeld een besmetting met ransomware. In sommige gevallen betaalt de verzekeraar zelfs het losgeld.

Deze verzekeringen zijn een welkome aanvulling op goede security. Zeker voor kleine bedrijven kan een ransomwarebesmetting een enorme financiële impact hebben.
Downtime, gegevensverlies of het betalen van losgeld kan een faillissement inluiden. Met een cyberverzekering kunnen middelgrote en kleine bedrijven de kosten van een securityincident beperken en ervoor zorgen dat ze snel weer 'back in business' zijn.

Toch kan de opkomst van cyberverzekeringen op lange termijn ook averechts werken.

Uit onderzoeken blijkt dat ongeveer een derde van de ransomwareslachtoffers het losgeld betaalt. Ransomware is dus een zeer effectieve afpersingsmethode gebleken. Dit heeft ertoe geleid dat criminelen een hoger bedrag vragen, waardoor juist weer minder mensen tot betaling overgaan.
Om hun businessmodel in stand te houden, richten ransomwarecriminelen zich vooral op mensen van wie ze weten dat die betalen.

WatchGuard voorziet dat afnemers van cyberverzekeringen vaker slachtoffer worden van ransomware. Zij zijn interessante doelwitten omdat de kans groot is dat het losgeld wordt betaald, aangezien de verzekeraar de kosten mogelijk vergoedt. Logisch gevolg is dat aanbieders van dergelijke verzekeringen strengere eisen gaan stellen aan de security van klanten.

Kabinet wil verplichte eisen voor Internet of Things-apparaten

Het kabinet wil Europese eisen aan huishoudelijke en andere apparaten die met internet worden verbonden. De Europese Commissie werkt weliswaar aan regels, maar daar hoeven fabrikanten zich niet aan te houden. Nederland wil verplichte eisen, onder andere tegen cybercrime.

D66-Kamerlid Kees Verhoeven vindt dat Internet of Things-apparaten nu nog vaak te makkelijk kunnen worden overgenomen door hackers.
Die kunnen op die manier privacygevoelige informatie verzamelen, de eigenaar daarmee afpersen of de apparaten inzetten voor cyberaanvallen.

Hij dringt daarom bij staatssecretaris Monica Keijzer van Economische Zaken aan op verplichte eisen voor cyberveiligheid. Donderdag zal hij de reden ook toelichten tijdens de door de VBN georganiseerde Security Summit 2018, waaraan 250 specialisten op veiligheidsgebied deelnemen. Verhoeven noemt het hoog tijd dat er harde, verplichte eisen komen aan met internet verbonden thermostaten, koelkasten en webcams.

Onveilige apparaten staan volgens hem al in onze huiskamers, terwijl we te maken hebben met cybercriminelen die elke dag met geavanceerdere aanvallen komen. Het kabinet wil het komende jaar ook in EU-verband kijken in hoeverre fabrikanten van onbeveiligde apparaten aansprakelijk gesteld kunnen worden voor een hack.

Sneller webbrowsen met Cloudfare DNS

Het DNS wordt ook wel 'het telefoonboek van het internet' genoemd. Dit Domain Name System zorgt er namelijk voor dat de url die je invoert wordt gematcht met het ip-adres van de website die je bezoekt. Net zoals in een regulier telefoonboek naam en nummer zijn gekoppeld. Deze onderliggende techniek is dus een cruciaal onderdeel van de werking van het internet.

Volgens Cloudflare laden websites veel sneller via het eigen DNS dan via de DNS van de gemiddelde provider - respectievelijk binnen 15 milliseconden en 68 milliseconden. Wil je het eens proberen via deze weg, volg dan deze stappen (op Windows 10):

DNS VERANDEREN

Ga naar **Instellingen**, **Netwerk en internet** en klik daar op **Adapteropties wijzigen.** Klik dan met de rechtermuisknop op je huidige internetverbinding en kies **Eigenschappen**. Klik in dit lijstje op **Internet Protocol versie 4 (TCP/IPv4)** en vervolgens rechtsonder op **Eigenschappen**. Kies **De volgende DNS-serveradressen gebruiken** en stel daar het volgende in:

Voorkeurs-DNS-server: 1.1.1.1
Alternatieve DNS-server: 1.0.0.1

Volg dezelfde stappen voor I**nternet Protocol versie 6 (TCP/IPv6)**, maar voer daar de volgende getallen in:

Voorkeurs-DNS-server: 2606:4700:4700::1111
Alternatieve DNS-server: 2606:4700:4700::1001.

Klik een paar keer op OK en herstart je browser. Mocht je tegen problemen aanlopen, dan kun je altijd weer de **automatische IP-instellingen** aanvinken.

Veiligdigitaal.com heeft het uitgeprobeerd en het werkt. Het surfen en lade van webpaginas gaat merkbaar sneller.

Wees gewaarschuwd: eventuele veranderingen in uw DNS instelling doet u op eigen risico!

Coprocessor-aanvallen: een verborgen dreiging

Gesprekken over IT-beveiliging worden gedomineerd door botnets, ransomware, DDoS-aanvallen, kwetsbaarheden in Internet of Things-apparatuur, open source-software en de discutabele staat van informatiebeveiliging. De relevantie van deze vraagstukken is onbetwist. Er ligt echter ook een slapende, en daardoor bijzonder risicovolle, dreiging op het gebied van coprocessors op de loer.

Coprocessors zijn speciaal ontwikkeld en inmiddels onmisbaar om de performance van de huidige uitgebreide en efficiënte smartphones op peil te houden. Ze nemen specialistische en resource-intensieve taken, zoals cryptografische processen of het beheer van mobiele en WiFi-radio's, weg van de hoofdprocessor. Tegelijkertijd houden ze ook de ontwikkeling van smartphones eenvoudig. Coprocessors zijn hiermee essentieel geworden binnen de evolutie van smartphones.

Kwetsbaarheden in firmware

Er zit echter ook een addertje onder het gras. Coprocessors functioneren doorgaans op basis van hun eigen firmware en die is - net als elke andere computercode - vatbaar voor cyberaanvallen. Omdat coprocessors gebruikmaken van een bevoorrechte, rechtstreekse communicatielijn naar de hoofdprocessor, kunnen cybercriminelen met een gehackte coprocessor andere beveiligingsmechanismen omzeilen. Dit is inmiddels geen theoretische dreiging meer. Project Zero, een team van beveiligingsanalisten bij Google dat de taak heeft om zero day-kwetsbaarheden te vinden, heeft 'proof of concepts' die laten zien hoe iOS en Android devices aangevallen kunnen worden door misbruik te maken van kwetsbaarheden in WiFi-coprocessors. Moderne besturingssystemen maken gebruik van diverse technieken om de beveiliging te versterken, zoals de toepassing van digitale certificaten of het elimineren of beperken van speciale rechten en 'sper user'-accounts. Ook worden voor applicaties nauwkeurig sandbox-omgevingen gehanteerd. Het leeuwendeel van deze verbeteringen richt zich echter op computercode die op de hoofdprocessor draait en gaat voorbij aan firmware van de coprocessor(s).

Coprocessors worden nog vaak over het hoofd gezien

IT-beveiliging is een kat-en-muisspel. Naarmate er meer kwetsbaarheden geïdentificeerd en verholpen worden, zoeken cybercriminelen ook weer nieuwe ingangen. Coprocessors vormen een dergelijk nieuw en relatief onbeschermd kanaal en zijn daarmee een aantrekkelijk doelwit. Het opzetten van een dergelijke aanval is niet zo moeilijk omdat coprocessors zijn ontwikkeld om te worden gebruikt door verschillende Original Equipment Manufacturers (OEM's). Deze fabrikanten hebben toegang nodig tot de firmware en documentatie van de coprocessors om die op te kunnen nemen in het ontwerp van hun devices.

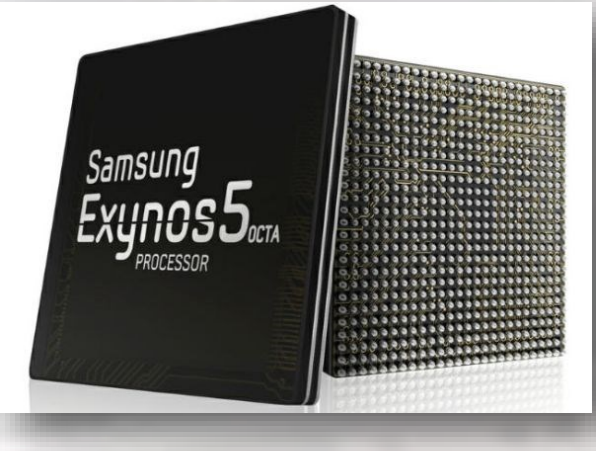
Deze documentatie is weliswaar niet openbaar of open source, maar is redelijk eenvoudig te verkrijgen.
Het Project Zero-team van Google begon het onderzoek met het raadplegen van productgegevensbladen op de website van een chipfabrikant.
Dit soort informatie geeft cybercriminelen een voorsprong bij het identificeren van kwetsbaarheden.

Einde oefening
Als een hacker toegang heeft tot de firmware van coprocessors, is het einde oefening. Dit biedt hen toegang tot alle apps en alle data en databases waar die apps gebruik van maken.
Dan hebben we het over logingegevens, GPS-data, contactgegevens, bankrekeningen en eigenlijk alles wat er maar op het mobiele apparaat te halen valt.
Daarnaast kan het IP-adres van mobiele apparaten worden gebruikt voor hacking-activiteiten en kunnen deze devices zelfs worden ingezet voor spionagedoeleinden.

Cyberaanvallen volgen doorgaans een voorspelbaar, gebaand pad. Gevorderde hackers identificeren en misbruiken kwetsbaarheden en, hoewel ze hun methoden en tools zo lang mogelijk geheim proberen te houden, zullen die vroeg of laat algemeen bekend worden. Net als met alle hackerstactieken zullen aanvallen op de firmware van smartphones naar verloop van tijd worden 'gedemocratiseerd' zodra meer mensen inzicht krijgen in de kwetsbaarheden en aanvalsmethoden.

Aanvankelijk zullen deze aanvallen op nauwgedefinieerde data gericht zijn en worden uitgevoerd door cybercriminelen met specifieke doelstellingen.

Zodra de technieken op brede schaal bekend worden, zullen de aanvallen een opportunistisch karakter krijgen, die worden gedaan door hackers met wisselende vaardigheidsniveaus en motieven, gewoon omdat het kan.
Kwetsbaarheden in coprocessors vertegenwoordigen kansen voor cybercriminelen. En ze zullen deze vroeg of laat benutten. Het probleem met aanvallen via de coprocessors is dat de slachtoffers zich pas zullen realiseren wat er is gebeurd nadat de schade is aangericht.



General Data Protection Regulation (GDPR).

Binnenkort krijgen alle organisaties die actief zijn in de EU te maken met nieuwe dataprotectiewetgeving: de General Data Protection Regulation (GDPR).

1. *Wat houdt de nieuwe wetgeving in?*
Doel van de GDPR is nieuwe regels introduceren die gelden voor alle landen in de Europese Unie. De wetgeving gaat over de beveiliging en het beheer van persoonlijke gegevens, zowel van klanten als van werknemers. Overal in de EU zijn bedrijven al bezig met de nieuwe normen. In Nederland werd bijvoorbeeld op 1 januari 2016 de meldplicht datalekken ingevoerd.

2. *Wat betekent de nieuwe wet voor bedrijven?*
In 2018 - als de GDPR van kracht wordt - moeten bedrijven kunnen aantonen dat de data die ze in datacenters of een cloud buiten de EU opslaan, voldoet aan de eisen van de nieuwe wetgeving. Bovendien moeten ze datalekken melden binnen 72 uur. De manier waarop persoonlijke data gebruikt en opgeslagen wordt, verandert dus nogal. Het is bijvoorbeeld zaak de data zo dicht mogelijk bij de medewerkers op te slaan. Zo zijn problemen met netwerkperformance te voorkomen en hebben gebruikers probleemloos toegang tot de informatie die ze nodig hebben voor hun werk.

3. *Welke bedrijven krijgen hiermee te maken?*
In eerste instantie geldt de GDPR voor organisaties met meer dan 250 werknemers die meer dan vijfduizend records per jaar verwerken. Later is de wetgeving ook van toepassing op het midden- en kleinbedrijf, ongeacht hun grootte en het aantal records dat ze verwerken.

4. *Welke gevolgen kleven er aan niet voldoen aan de GDPR?*
Na datalekken hebben bedrijven natuurlijk altijd te maken met reputatieschade. Maar als ze niet voldoen aan de wetgeving staan hen ook forse boetes te wachten. De exacte bedragen zijn nog niet bekend, maar reken op maximaal één miljoen euro of twee procent van de wereldwijde omzet - net wat hoger is.

Man verdient miljoenen met nep-afspeellijsten

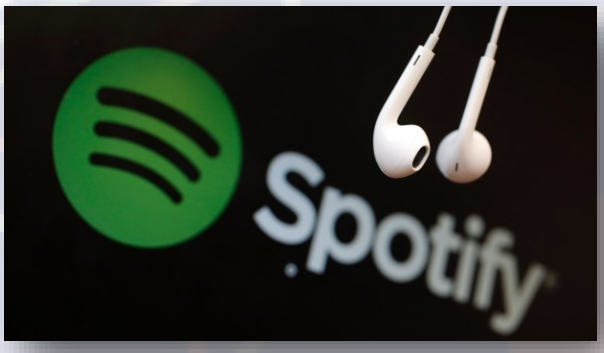
Een opmerkelijke zwendel is ontdekt bij muziekstreamplatform Spotify. Journalisten van Music Business Worldwide analyseerden hoe een Bulgaarse oplichter de afgelopen maanden mogelijk miljoenen dollars verdiende met (ruim duizend) nepaccounts, afspeellijsten vol onbekende artiesten – en natuurlijk wat slimme software.

De truc werd voor het eerst in september 2017 opgemerkt, met de vondst van twee verdachte afspeellijsten: Soulful Music en Music from the Heart. Die stonden vol met onbekende artiesten en nummers die allemaal een seconde of 35 à 40 duurden.
Toch stonden die play lists hoog genoteerd op Spotify, hoger dan de lists van erkende artiesten en maatschappijen. Soulful Music haalde op een gegeven moment zelfs de top-twintig in de VS.

Ook opvallend was dat de lijsten bijna vijfhonderd nummers telden – en dat al die muziek afkomstig was uit … Bulgarije. Volgens Spotify luisterden er elke maand niet meer dan 1200 mensen naar de lijsten – nep-accounts zoals later bleek.
De (onbekende) Bulgaar achter deze zwendel speelde vanaf die accounts 24/7 de lijsten af, aangestuurd door een bot.

Met een investering van zo'n twaalfduizend dollar per maand (1200 accounts x het abonnementstarief) wist hij, volgens MBW, ruim vier ton per maand te verdienen: per dag zijn zo'n 60 duizend liedjes te spelen, maal die 1200 accounts, maal de prijs die Spotify betaalt (0,004 dollarcent voor iedere keer dat een nummer is afgespeeld). En dat voor één playlist.

MBW noemt het opvallend dat Spotify de fraude zelf niet wist op te sporen. Hoewel de Bulgaar gewoon voor zijn accounts betaalde, manipuleerde die wel het streamingmodel.



Nieuwe brancheorganisatie Cyberveilig Nederland opgericht

Verschillende cybersecurity dienstverleners kondigen de oprichting van brancheorganisatie Cyberveilig Nederland aan. Zij willen de digitale weerbaarheid van Nederland vergroten, alsmede de kwaliteit en transparantie binnen de groeiende security sector verhogen. Computest, Fox-IT, Guardian360, Hoffmann, Motiv, Northwave, QSight IT en Zerocopter sluiten zich aan bij de organisatie.

Cyberveilig Nederland ziet de noodzaak vanwege het feit dat 97,1 procent van de Nederlandse bevolking toegang heeft tot internet. Daarmee behoort ons land tot de digitale voorhoede van Europa. Deze digitalisering brengt echter grote economische en maatschappelijke kansen met zich mee. Om de kansen te benutten moeten we blijvend kunnen vertrouwen op onze informatie en informatiesystemen. Daarom is meer aandacht voor security een must.

Vorig jaar droegen WannaCry en NotPetya bij aan een wake-up call ten aanzien van de digitale kwetsbaarheid van Nederlandse organisaties, waardoor de initiatiefnemers een sterkere vraag naar cybersecurity-dienstverlening opmerken. Daarbij ontbreekt echter transparantie en een garantie voor kwaliteit. Deze elementen bestempelt de organisatie als cruciale elementen om het vertrouwen in de sector te waarborgen.
Samenwerking en leiding

Om bij te kunnen dragen aan een digitaal veiligere samenleving wil Cyberveilig Nederland in gesprek met vertegenwoordigers van de overheid, zoals het National Cyber Security Centrum. De partijen zijn bijvoorbeeld al met FME de mogelijkheden aan het verkennen om samen te werken. Hierbij staan het verder versterken en cyberveilig maken van de technologische industrie centraal.

Petra Oldengarm zal Cyberveilig Nederland leiden. Zij was tot voor kort Director Cybersecurity bij Hoffmann en is al jaren actief in het werkveld van informatiebeveiliging. Ze zal worden bijgestaan door Liesbeth Holterman, die hiervoor belangenbehartiger cybersecurity was voor ICT en technologie belangenorganisaties en jarenlang voor de overheid in het veiligheidsdomein werkte. De acht initiatiefnemers rekenen erop dat meer leveranciers zich aan zullen sluiten bij Cyberveilig Nederland.

Slingshot-malware is zeer verfijnd en al zes jaar actief

Onderzoekers van Kaspersky Lab hebben ontdekt dat er al zes jaar malware rondgaat die gericht is op routers. Deze schijnt zeer goed ontwikkeld te zijn en bespioneert computers via MikroTik-routers. Volgens de onderzoekers van Kaspersky zijn twee elementen van de malware "meesterwerken" door de zeer verfijnde techniek die erachter schuilgaat.

De malware is Slingshot gedoopt en is zeer waarschijnlijk ontwikkeld door een overheid. Allereerst vervangt de malware een library-bestand met een versie met malware daarin. Vervolgens downloadt dat bestand andere componenten, waarna een tweeledige aanval gelanceerd wordt op computers zelf.

Tweeledige aanval

De eerste van die aanvallen Canhadr, draait low-level kernel code die effectief gezien de indringer vrij spel geeft, waaronder toegang tot de opslag en het geheugen van een computer. Het tweede deel heet GollumApp en focust zich op het gebruikersniveau en bevat code die ervoor zorgt dat de malware zo lang mogelijk actief kan blijven.

Kaspersky noemt die twee elementen "meesterwerken" en doet dat met goede reden. Slingshot slaat delen van de malware op in een versleuteld virtueel bestandssysteem en zorgt ervoor dat alle modules versleuteld worden. Daarnaast schakelt de malware zichzelf uit als een virusscanner actief is. Sterker nog, volgens de ontwikkelaars is de code bewapend tegen veruit de meeste detectiemethodes.

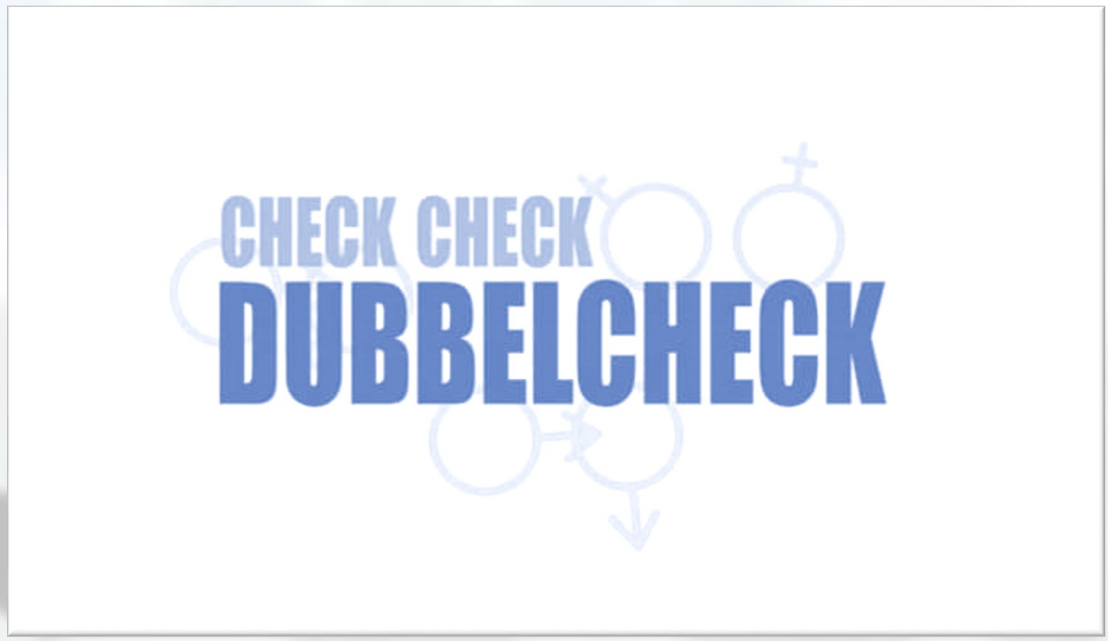
Niets is veilig

Slingshot, dat al sinds 2012 actief is, kan verder zo'n beetje alle mogelijke data stelen. Denk aan toetsenbordaanslagen, netwerkverkeer, wachtwoorden en kan screenshots maken. Het is niet zeker hoe Slingshot dat voor elkaar krijgt, maar volgens Kaspersky zijn er meerdere verschillende manieren waarop het dat doet.

Het feit dat de code zo verfijnd is en al zo lang actief is, wijst er volgens Kaspersky op dat Slingshot ontwikkeld is door overheden. Daarnaast denkt de firma dat de code door een Engelstalig land ontwikkeld is. Een recente firmware-update van MikroTik zou Slingshot (voorlopig) uitgeschakeld hebben.

INDEX

ONLINE KOPEN? DOE DE CHECK !



Voordat u met iemand zaken doet via een handelssite of webshop, kunt u controleren of er meldingen over deze (ver)koper zijn gedaan.

U kunt zoeken aan de hand van de volgende gegevens:

- IBAN-nummer (gebruik alleen letters en cijfers, bijv. NL05123412341234123400)
- E-mailadres (niet van toepassing voor Marktplaats-adressen - lees meer)
- Telefoonnummer (gebruik alleen cijfers, bijv. 0201234567)
- De url van een webwinkel (bijv. www.eenwinkel.nl)

Let op!
Als uw zoekactie naar mogelijke meldingen over de (ver)koper niets oplevert, wil dit NIET zeggen dat u geen enkel risico loopt bij een verdere transactie. U kunt aan de check dan ook geen rechten ontlenen. Het wil alleen zeggen dat er op dit moment geen (negatieve) meldingen bekend zijn. Blijf dus altijd alert en gebruik uw gezonde verstand. Wanneer iets te mooi is om waar te zijn, dan is dat meestal ook zo!
Krijgt u WEL te horen dat er negatieve meldingen zijn over de (ver)koper met wie u zaken wilt doen, denk dan goed na of u door wilt gaan met de verdere transactie. Vraag eventueel extra waarborgen van de persoon met wie u zaken doet.

Check de verkoper **Check de webshop** **Iban check** **Stop heling check**

Tot 160 miljard dollar per jaar wordt witgewassen door cybercriminelen

Tot 160 miljard euro aan opbrengsten van cybercriminaliteit worden op jaarbasis wereldwijd witgewassen. Cybercriminelen maken hiervoor gebruik van onder meer cryptovaluta, digitale valuta in videogames en online betalingssystemen zoals PayPal.

Dit blijkt uit onderzoek van Dr. Mike McGuire, hoogleraar Criminologie aan de Britse Surrey Universiteit. Het onderzoek is gesponsord door Bromium, een bedrijf gespecialiseerd in applicatie-isolatie met behulp van op virtualisatie gebaseerde beveiliging. De resultaten van het onderzoek zijn verzameld in het rapport 'Into the Web of Profit'.
McGuire meldt dat cybercriminelen voorheen vooral op bitcoin vertrouwde om opbrengsten van hun activiteiten wit te wassen. Het onderzoek wijst echter uit dat cybercriminelen bitcoin steeds vaker links laten liggen en kiezen voor onbekendere valuta zoals Monero, die meer anonimiteit bieden. De belangrijkste reden hiervoor is de toegenomen focus van autoriteiten op bitcoin, die de cryptovaluta nauwer zijn gaan monitoren.

In-game valuta
Ook blijkt dat cybercriminelen in toenemende mate in-game valuta inzetten om geld wit te wassen. Vooral in China en Zuid-Korea blijkt deze werkwijze relatief vaak te worden gehanteerd. Zo wijst McGuire op de arrestatie van een criminele groepering die 38 miljoen dollar heeft witgewassen via videogames.

Ook PayPal en andere online betalingsdiensten worden echter ingezet om geld wit te wassen. Hierbij worden doorgaans een groot aantal kleine transacties gedaan in een poging geautomatiseerde beveiligingsmechanismen te omzeilen. Ook worden online marktplaatsen en veilingwebsites zoals eBay ingezet om geld wit te wassen.

"We hebben in dit onderzoek geïnvesteerd om een betekenisvolle discussie te kunnen voeren over het verstoren van de economische systemen en slechte security practices die cybercriminaliteit wereldwijd mogelijk maken, aangezien dit veel te eenvoudig is", legt Gregory Webb, CEO van Bromium, uit. "Het is vandaag de dag eenvoudig voor aanvallers om machines te infecteren, data te stelen, bedrijven en individuen te gijzelen in ruil voor losgeld en dit om te zetten in cash. De toename in het gebruik van ongereguleerde, virtuele valuta maakt dit nog eenvoudiger.
We moeten het probleem op een andere manier te lijf gaan. Opsporingsinstanties, de cybersecurity industrie en zowel de publieke als private sector moeten waakzaam zijn voor verstorende cybercriminaliteit. Het beschermen van applicaties die toegang hebben tot gevoelige data is een absolute vereiste. We hebben een geheel nieuwe aanpak voor cybersecurity nodig om te voorkomen dat deze cijfers blijven stijgen."

Logingegevens populairste doelwit van cybercriminelen

Bij datalekken richten cybercrimininelen zich vooral op logingegevens (42%), gebruikersaccounts met speciale rechten (31%) en klantgegevens (31%). Dit blijkt uit onderzoek van SANS Institute. De impact van beveiligingsincidenten zat voor geraakte organisaties meer op het gebied van verlies aan vertrouwen van klanten (50%), zorgen op juridisch vlak (46%) en imagoschade (42%), dan op gebied van verkoop of boetes. Meer inzicht in informatiestromen en de mate van gevoeligheid van data is noodzakelijk om bedrijfsgegevens effectiever te beschermen.

De focus op persoonlijke gegevens onderstreept de waarde van toegangsgegevens voor cybercriminelen. Deze data is net zo gewild als de 'gevoelige' bedrijfsgegevens die worden getarget met ransomware of wipeware voor financieel gewin of uit vernietigingsdrang. De verkregen privileges bij het misbruiken van accounts met speciale rechten gebruiken kwaadwillenden vaak om hun aanvallen te intensiveren en verspreiden, waardoor ze nog meer gevoelige informatie kunnen verzamelen.

Weten waar cybercriminelen op uit zijn is het halve werk. Het is belangrijk voor bedrijven om waardevolle bedrijfsgegevens en informatiestromen in kaart te brengen. Dit maakt het mogelijk om een bedrijfsbreed beveiligingsbeleid te ontwikkelen dat door mensen, processen en technologie kan worden ondersteund. Zonder deze basis is het onmogelijk om beveiligingsregels af te dwingen. Dit blijkt de grootste uitdaging te zijn bij een evenwichtige bescherming en beschikbaarheid van data.

De onderzoeksresultaten wijzen erop dat dit geen makkelijke opgave is. Meer dan de helft van de respondenten (63%) zegt moeite te hebben met het afdwingen van beleidsregels gedurende de volledige levenscyclus van gevoelige data. Andere problemen houden verband met een gebrek aan medewerkers en middelen (62%) en het in kaart brengen van alle toegangswegen tot gevoelige data (51%).

"Data die betrekking heeft tot toegang heeft wellicht nog meer en betere beveiliging nodig, gezien dit onderzoek heeft aangetoond dat persoonsgegevens en accounts met bijzondere toegangsrechten de meest voorkomende oorzaak van datalekken zijn.", zegt Barbara Filkins, SANS Analyst Program Research Director en auteur van het onderzoeksrapport.
"Het uittekenen van datakaarten en -stromen is misschien niet ideaal, maar het proces illustreert een belangrijk uitgangspunt. Een foto – of in dit geval een kaart – zegt meer dan duizend woorden als je wilt begrijpen waar je het beste kunt beginnen met het beschermen van data."

Telegram moet versleutelde berichten aan Rusland tonen

Chatapp Telegram moet de Russische geheime dienst toegang geven tot versleutelde berichten die via de dienst zijn verstuurd.
De populaire chatapp Telegram moet zijn zogenoemde decryptiesleutel aan de Russische geheime dienst FSB geven, meldt persbureau TASS.

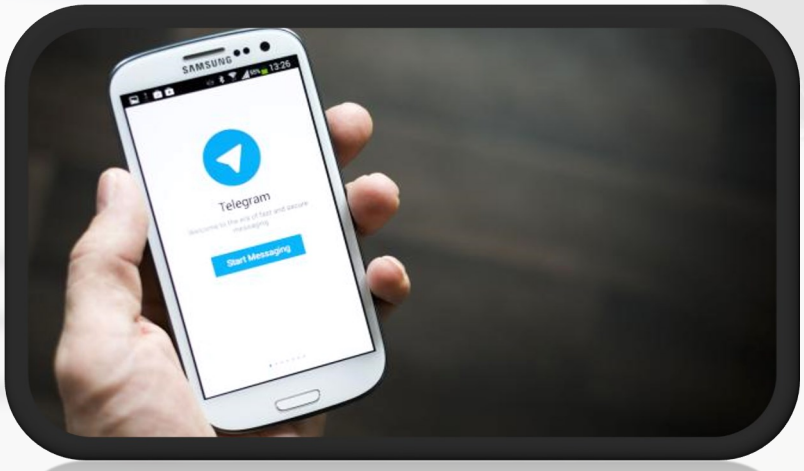
De FSB is al langer op jacht naar de sleutel, waarmee de inhoud van onderschepte berichten kan worden ingezien. Zonder die sleutel zijn berichten onderweg van de zender naar de ontvanger onleesbaar versleuteld.

De FSB wilde de sleutel in 2017 al hebben, maar Telegram weigerde en kreeg een toen een boete van bijna 12.000 euro. Telegram-oprichter en Russische ondernemer Pavel Durov ging tegen de eis in beroep. Het Russische hooggerechtshof heeft de eis nu afgewezen, waardoor Telegram als nog wordt gedwongen de FSB toegang te geven.

Vrijheid en privacy
Blijft Telegram weigeren, kan het bedrijf opnieuw een boete verwachten. Ook is een volledige blokkade van Telegram in Rusland een mogelijkheid. "Dreigingen om Telegram te blokkeren tenzij het privédata afstaat, zal zijn vruchten niet afwerpen. Telegram zal staan voor vrijheid en privacy", schrijft Telegram-oprichter Durov op Twitter.

Rusland wil toegang tot Telegram uit oogpunt van terrorismebestrijding. Volgens de Russische overheid gebruiken terroristen de app om op een versleutelde manier te communiceren. Zo werd Telegram volgens Rusland gebruikt door daders achter de bomaanslag in op metro van Sint-Petersburg in april 2017.
Telegram heeft wereldwijd 180 miljoen gebruikers.

Gebruikt U Telegram?
Stap dan over naar Signal !



Nieuwe ransomware vernietigt backups om herstel te bemoeilijken

Een nieuwe vorm van ransomware genaamd Zenis versleutelt niet alleen data op getroffen systemen, maar probeert ook gericht backups van slachtoffers te vernietigen. De ransomware heeft al meerdere slachtoffers gemaakt.

Op het moment van schrijven is er nog geen manier gevonden om versleutelde data te ontsleutelen. Michael Gillespie van MalwareHunterTeam is de ransomware echter aan het analyseren om kwetsbaarheden op te sporen die decryptie mogelijk maken. De partijen adviseren slachtoffers het geëiste losgeld dan ook niet te betalen.

Remote Desktop Services

Het is niet zeker hoe Zenis wordt verspreid. MalwareHunterTeam en Bleeping Computer melden echter dat de ransomware mogelijk via gehackte Remote Desktop Services wordt verspreid. Zodra de ransomware zich op een systeem heeft genesteld, verwijdert de malware Volume Shadow Copies, schakelt het Startup Repair uit en worden logbestanden gewist. Vervolgens stopt de ransomware verschillende processen, waaronder task manager en backupprocessen.

Nadat het systeem op deze wijze is voorbereid begint Zenis met het versleutelen van bestanden. Hierbij richt de ransomware zich op een breed scala aan bestanden, variërend van foto's, video's en muziekbestanden tot tekstdocumenten, spreadsheets en presentaties. Ook worden cryptowallets versleuteld. Bij het versleutelen van een bestand wordt de bestandsnaam van bestanden gewijzigd om identificatie van specifieke bestanden te bemoeilijken. Hierbij wordt de volgende bestandsnaam gehanteerd: Zenis-[twee willekeurige karakters].[twaalf willekeurige karakters]. Als voorbeeld noemt Bleeping Computer een bestand genaamd test.jpg, dat door de ransomware de bestandsnaam Zenis-4Q.4QDV9txVRGh4 toegewezen kan krijgen.

Backups vernietigen

Bij het versleutelen van data zoekt Zenis gericht naar bestanden die gerelateerd zijn aan backups. Deze bestanden worden door de ransomware driemaal overschreven en vervolgens verwijderd. Dit maakt het voor slachtoffers moeilijker data uit een backup terug te halen.

MalwareHunterTeam en Bleeping Computer adviseren gebruikers waakzaam te zijn voor verdachte bestanden en daarnaast zeker te stellen dat Remote Desktop Services correct is geconfigureerd. De partijen adviseren zeker te stellen dat computers die Remote Desktop Services draaien niet direct verbonden zijn met internet en bij voorkeur achter een VPN zijn geplaatst.

Ook raden de partijen aan Remote Desktop Services correct te configureren om brute force aanvallen te bemoeilijken en beveiligingssoftware te installeren die het gedrag van bestanden analyseert om onder meer ransomware vroegtijdig op te merken. Tot slot wordt gebruikers geadviseerd zeker te stellen dat hun systeem volledig up-to-date is om zeker te stellen dat aanvallers geen misbruik kunnen maken van bekende en gepatchte beveiligingsproblemen.

Cryptojacking is met 8.500 procent toegenomen

2017 was misschien wel het jaar van de cryptocurrency. De waarde van Bitcoin ging door het dak, en ook andere munten zoals Ethereum zagen enorme waardestijgingen. Dit maakt dat ook hackers de kans zien om geld te verdienen in deze lucratieve handel.

Cryptojacking

Het bedrijf achter Norton, Symantec, heeft nu onderzoek gedaan naar de manier waarop hackers gebruik maken van computers van onwetende gebruikers om cryptocurrencies te verkrijgen. Dat heet 'cryptojacking' en vergt slechts de injectie van enkele regels code in een website of applicatie om de rekenkracht van een computer te gebruiken voor het 'mijnen' van cryptomunten.

De praktijk wint in snel tempo aan populariteit. In het laatste kwartaal van 2017 steeg het aantal detecties van cryptojacking met 8500 procent. In de laatste drie maanden van vorig jaar maakte cryptojacking 16 procent uit van alle online aanvallen die door Symantec werden geblokkeerd. Dat gebeurde in pieken die niet toevallig overeen kwamen met pieken in de waarde van Bitcoin en andere cryptomunten.

Cryptojacking kan lijden tot computers die enorm vertraagd worden Om nog te zwijgen van een hogere energierekening door de extra verbruikte stroom. Verder, als het gaat het om apparaten zoals telefoons en laptops, kan het de levensduur van de batterij ernstig verminderen. Op grotere schaal kunnen de gevolgen voor bedrijven die te maken krijgen met cryptojacking bijzonder ernstig zijn. Als dit niet op tijd wordt opgemerkt kan het bijvoorbeeld lijden tot een volledige uitschakeling van het bedrijfsnetwerk. Verder kunnen de clouddiensten van bedrijven overbelast raken, uiteindelijk allemaal met het gevolg dat bedrijven extra onvoorziene kosten maken.

Nederland

Wat opvallend is, is dat in Nederland 1,8 procent van alle coinminer detecties wereldwijd plaatsvindt. Nederland staat hiermee op de zevende plaats in Europa. Waarom Nederland zoveel coinmining detecties heeft, is niet bekend. Wat verder opvalt, is dat het vaak moeilijk is om te zien of computers worden gebruikt voor coinmining. Dat computers vertragen is immers vaak genoeg te wijten aan verouderde hardware. Daarnaast is er ook niet altijd iets te zien aan het stroomverbruik. Volgens Symantec proberen criminelen het proces immers zo aan te pakken dat de eindgebruikers geen enorme veranderingen merken in hun energieverbruik.

Bron: Norton Symantec

Zo verwijder je alles wat Google van je weet

Google maakt er geen geheim van dat het bedrijf ontzettend veel over je weet. Het bedrijfsmodel is immers gebaseerd op adverteren op maat van de gebruiker. Met de juiste knowhow achterhaal je hoe Google jou volgt. Zo verwijder je alles wat Google van je weet!

Scannen

Dat Google zoveel over je weet, komt niet alleen door het gebruik van deze zoekmachine, maar ook door de brede waaier aan diensten die stevig ingeburgerd zijn. Uiteraard heeft Google je zoekgeschiedenis opgeslagen.

Deze gegevens vind je terug in je Google-account. Log in en klik op het account-icoontje zodat je naar Mijn account kunt gaan. Vervolgens selecteer je bij het onderdeel Persoonlijke info en privacy de optie Mijn activiteit. Klik op Menu (de drie verticale stippen) en selecteer Activiteitsopties. Begin bij het onderdeel Web- en app-activiteit en klik op Geschiedenis beheren.
Hier staat hoe je de zoekmachine hebt gebruikt. Om deze informatie te wissen, kies je in het menu links de opdracht Activiteit verwijderen op basis van. Hier heb je de mogelijkheid om op basis van onderwerp alles op te ruimen, of op basis van een bepaalde periode. Wil je meteen helemaal schoon schip maken met deze zoekgeschiedenis, dan selecteer je Onbeperkt bij het datummenu.

Spraak en audioactiviteit

Toch zijn hierdoor niet alle data verwijderd. Je locatiegeschiedenis, je apparaatgegevens en spraakcommando's moet je apart aanpakken.

Ga hiervoor terug naar de Activiteitsopties via het menu. Hier vind je de knoppen naar de geschiedenis van de locaties, apparaat, spraak, audio en YouTube.
Veel gebruikers realiseren zich niet dat Google elke gesproken zoekopdracht vastlegt. Maak je gebruik van die functie, dan kun je via de geschiedenis van Spraak- en audioactiviteit precies luisteren naar wat je hebt gezegd en hoe je hebt gezegd.

Locatiegeschiedenis

Ook de Locatiegeschiedenis is iets speciaals. Klik je hier op Geschiedenis beheren, dan kom je op een kaart waar al je bezochte plaatsen te zien zijn. Om deze informatie te verwijderen, selecteer je rechtsonder het icoontje Instellingen en kies je Volledige locatiegeschiedenis verwijderen.
Hier kun je er ook voor zorgen dat Google het bijhouden van deze data tijdelijk stopzet met de opdracht Locatiegeschiedenis onderbreken.

Vier keer meer malware op Windows 7-pc's dan op Windows 10

In een rapport van Webroot lezen we dat 15% van alle gescande malware op Windows 10-systemen gevonden werd, tegenover 63% op Windows 7. Kijken we enkel naar bedrijfs-pc's, dan verkleint het verschil van 0,04 malwarebestanden per Windows 10-toestel, vergeleken met 0,08 malwarebestanden per Windows 7-pc.

De trend van meer malware op Windows 7-machines geldt zowel voor particuliere gebruikers als binnen bedrijven. Er werden minder malwarebestanden gescand in 2017 vergeleken met 2016, toch zijn de resultaten frappant wanneer je beide besturingssystemen vergelijkt. 15% van alle gescande malware werd op Windows 10-systemen gevonden, tegenover 63% op Windows 7.

Marktaandeel

Het grote verschil wordt nog frappanter wanneer je weet dat 54% van alle geteste toestellen Windows 10-devices zijn, tegenover 33% Windows 7. De overige systemen zijn Windows 8 (8%), Vista (1%) en XP (1%).

Wanneer we naar zakelijke gebruikers kijken, wordt het verschil kleiner met 0,04 malwarebestanden per Windows 10-toestel, vergeleken met 0,08 malwarebestanden per Windows 7-pc. Webroot laat in zijn rapport weten dat ondanks dat Windows 10 niet alle veiligheidsproblemen oplost, het een stap in de goede richting is. Gecombineerd met geavanceerde endpointbeveiliging dat gedragdanalyse en machine learning toepast kan een Windows 10-machine heel wat cyberaanvallen weren.

Licentiepakket

Het is belangrijk om te benadrukken dat niet alle Windows 10-licenties de volledige beveiligingssuite hebben. Windows Defender Advanced Threat Protection, een cloud-gebaseerde malwaredetectietool, is niet beschikbaar voor thuisgebruikers en kleine bedrijven. Pas vanaf een E5-volume licentiedeal zit het pakket er standaard in.

Volgens cijfers van Microsoft gebruikt 18% van Windows 7-gebruikers de meegeleverde Windows Defender, tegenover 50% bij Windows 10-gebruikers.

Zo gaat de ‘helpdeskfraude’ in z’n werk

1 Een persoon, die vaak met een sterk Indiaas accent spreekt, zegt u op te bellen namens Microsoft. Uw pc is niet in orde, luidt de boodschap. Gelukkig kunnen de problemen verholpen worden.

2 De beller zorgt voor ‘bewijs’ dat uw pc problemen heeft. Ze vragen u een aantal opdrachten uit te voeren die foutmeldingen veroorzaken.

3 Ze gaan de problemen verhelpen, zeggen ze. U moet daarvoor naar een website waarmee ze uw computer op afstand kunnen besturen. Supremocontrol.com is daar een voorbeeld van. De beller geeft inloggegevens door. Hiermee geeft u de controle over uw computer uit handen. Op afstand kunnen ze nu vrijwel alles met uw pc uithalen, maar dat zeggen ze er natuurlijk niet bij. Alles doen ze zogenaamd om u te helpen.

4 Zonder dat u iets doet ziet u de muis over uw scherm gaan. Zogenaamd is de Microsoftbeller uw pc aan het opschonen.

5 Om vervolgens te checken of de computer vrij is van kwaadaardige software dient u in te loggen bij internetbankieren. Hier zit hem de truc, want de beller krijgt dus ook toegang tot uw bankrekening. Zonder dat u het doorheeft boeken ze geld over van uw spaarrekening naar uw betaalrekening. Wat ze echter beweren is dat u geld van Microsoft heeft gekregen dat u vervolgens moet overmaken naar een bepaalde rekening. Ook zijn verhalen bekend waarbij ze vragen het geld via een geldtransferkantoor als Western Union of MoneyGram over te schrijven naar het buitenland. In weer een andere variant vragen ze u te betalen voor een abonnement om gedurende een aantal jaren beschermd te zijn tegen kwaadaardige software. Op het moment dat u denkt bijvoorbeeld € 80,- te betalen blijkt later dat er een bedrag van € 800,- is afgeschreven.

Windows wachtwoord achterhalen met Ophcrack

Het kan iedereen wel eens gebeuren dat je opeens je wachtwoord kwijt ben van bijvoorbeeld je Windows systeem. Vaak installeren gebruikers de computer opnieuw als ze hun wachtwoord zijn vergeten, maar er zijn meerdere oplossing mogelijkheid waarbij je de data kan behouden.

Het is namelijk mogelijk om met behulp van speciale software en een beetje moeite, je inlogwachtwoord te achterhalen. De handleiding is alleen bedoeld voor mensen welke hun wachtwoord zijn vergeten, niet om ongevraagd toegang te verlenen tot een account.

Er zijn diverse mogelijkheden waarmee je een wachtwoord kan resetten waaronder met de volgende tools:

- OphCrack LiveCD
- Recovery
- Reïnstal op andere schijf

HOE WERK OPHCRACK?

Ophcrack is een livecd variant waarmee je in de meeste gevallen een wachtwoord kan restoren als je oude wachtwoord niet meer werkt. Om een Live CD te maken is wel een pc vereist met een actieve internet verbinding. Op de computer moet eerst Ophcrack gedownload worden. Doormiddel van onderstaande stappenplan is het maken van een Live CD zo gebeurd.

1. Download Ophcrack
2. Brand de ISO op een CD/DVD

3. Als het branden is gelukt stopen we de Live CD in de computer en zorgen dat deze vanaf de DVD zal gaan opstarten. Als het programma draait komt de tekst Ophcrack Graphic Mode in beeld, hier drukken we op enter aangezien wij kiezen voor de optie Ophcrack Graphics. Nu draait het programma en zal het wachtwoord binnen enkele uren proberen te unlocken. Afhankelijk van het wachtwoord kan het enkele minuten tot uren duren.

Firefox-extensie houdt Facebook-tracking tegen

Mozilla heeft een extensie voor Firefox gelanceerd, waarmee je kunt voorkomen dat Facebook je op andere websites kan volgen.

Als je deze extensie met de naam Facebook Container installeert, worden je Facebook-cookies weggegooid. Je kunt Facebook gewoon blijven gebruiken (het tabblad waarin Facebook is geopend, krijgt dan een speciale blauwe kleur), maar als je vervolgens op een link klikt of een ander adres intypt, worden deze url's buiten de Facebook-container geladen. Zo voorkom je dat Facebook bijvoorbeeld kan volgen (tracken) naar welke producten je hebt gezocht en Facebook je vervolgens weer advertenties voor die producten voorschotelt.

Gebruik van de extensie heeft wel gevolgen voor het functioneren van sommige sites. Diensten waarbij je nu inlogt met Facebook, werken niet meer. Hetzelfde geldt voor Like-buttons buiten Facebook en voor Facebook-reactiemogelijkheden op andere sites.

Onrust

Met de nieuwe extensie speelt Mozilla handig in op de onrust die er de afgelopen week is ontstaan over het gebruik van Facebook-gegevens. Vorig weekend onthulden The Guardian en The New York Times dat Cambridge Analytica de gegevens van 50 miljoen Facebook-gebruikers had buitgemaakt. Het bedrijf gebruikte deze informatie onder meer tijdens de Amerikaanse presidentsverkiezingen van 2016.

De onthullingen leidden tot woede bij gebruikers en politici van over de hele wereld. Dit weekend bood Facebook-CEO Mark Zuckerberg in paginagrote advertenties in verschillende kranten zijn verontschuldigingen aan voor het geschonden vertrouwen.

Google verbiedt extensies die cryptocurrencies minen

Google heeft bekend gemaakt dat het stopt met Chrome-extensies die cryptocurrencies minen. Tot nu toe bood de Chrome Web Store uiteenlopende extensies die dit mogelijk maakten, op voorwaarde dat cryptomining de enige functie was én dat gebruikers hier volledig van op de hoogte waren.

Problematisch was volgens Google echter dat ongeveer negentig procent van de extensies die cryptocurrencies minen en door ontwikkelaars in de Chrome Web Store geplaatst werden, niet voldeden aan die regels. Extensies die niet voldeden werden al standaard afgewezen of uit de winkel verwijderd, maar nu blijkt dat Google het makkelijker vindt om helemaal te stoppen met dergelijke extensies.

Extensies worden verwijderd

Vanaf vandaag worden er geen nieuwe cryptomining extensies meer geaccepteerd in de Chrome Web Store. De extensies die zich op dit moment wel nog in de Store bevinden, worden in juni verwijderd.

"Het extensies-platform biedt krachtige mogelijkheden die onze ontwikkelaarsgemeenschap ertoe in staat gesteld heeft een levendige catalogus van extensies op te bouwen, die gebruikers ertoe in staat stelt het meeste uit Chrome te halen," begon Google in een statement.

"Helaas hebben sommige van deze mogelijkheden softwareontwikkelaars aangetrokken die probeerden het platform te misbruiken ten koste van de gebruikers. Dit nieuwe beleid zorgt ervoor dat Chrome-gebruikers van de voordelen van extensies kunnen blijven genieten, zonder dat ze zichzelf hoeven bloot te stellen aan verborgen risico's."

Geheime miningscripts

Het minen van cryptocurrencies is een populaire manier om geld op te halen. Er zijn een aantal voorvallen geweest van cryptojacking, waarbij bedrijven als Tesla en Showtime gehackt werden en hun computersystemen gedwongen om cryptocurrencies te minen.

Dat Google nu met deze nieuwe beleidsmaatregel komt, past binnen de noodgedwongen beleidsmaatregelen die genomen worden om dit soort situaties te voorkomen.

Bron: Google

EU-wetsvoorstel: “E-evidence” binnen tien dagen naar politie

Volgens een (nog vertrouwelijk) wetsvoorstel zouden techbedrijven als Facebook en Twitter binnen tien dagen moeten voldoen aan informatieverzoeken van de politie en opsporingsdiensten.

In noodgevallen zouden ze dat zelfs binnen zes uur moeten doen, schrijft Euractiv dat het wetsvoorstel in handen kreeg. Het gaat daarin om ‘elektronisch bewijs’ dat nodig is voor politieonderzoek.

Niet interessant is dan wáár de data is opgeslagen of waar het bedrijf gevestigd is. Het voorstel behelst behalve sociale netwerken ook cloud-diensten, dns-registraties en zelfs digitale marktplaatsen en peer-to-peer transacties. A

anleiding voor de nieuwe wet is de ‘exponentiële stijging’ van het gebruik van online diensten en apps. Niet verwonderlijk is dat er veel kritiek is op het voorstel, vooral van burgerrechtengroeperingen.

VVD wil superspoedprocedure om seks- en naaktfilmpjes offline te krijgen

De VVD wil wettelijk gaan regelen hoe slachtoffers van privacyschending beter beschermd kunnen worden.

Volgens Kamerlid Sven Koopmans gaat het om slachtoffers van wraakporno, internetpesten, sextortion, shaming, exposing maar ook van verborgen camera's in kleedkamers, sauna's en toiletten en zelfs van drones boven je huis.
Allemaal zaken die 'niet altijd te voorkomen zijn' maar die, als het gebeurt, 'heel zwaar beboet' moeten worden, vindt Koopmans. Daders van zulke feiten noemt hij, verwijzend naar Orwell, 'little brothers'.

Over wat je zelf online publiceert, mag je niet klagen, aldus Koopmans. 'Maar van wat anderen stiekem van jou filmen heb je geen weet. Niemand kan zich verschuilen voor verborgen camera's, dataprofilering en gezichtsherkenningssoftware'.

De VVD wil verder dat zulk materiaal sneller en gemakkelijker offline gaat, bijvoorbeeld via 'één simpel formulier' en niet meer via aparte procedures per provider of platform. Als zaken voor de rechter komen, moet dat met 'superspoed', ook als de dader onbekend is.

Politie plaatst twee keer onterecht privacygevoelig beeld op sociale media

'In ieder geval twee keer' heeft de politie de afgelopen maanden onterecht privacygevoelig beeldmateriaal op sociale media geplaatst. Minister Ferd Grapperhaus (JenV) schrijft dat aan de Kamer.

Daar werden vragen gesteld naar aanleiding van het tv-programma De Monitor dat het sociale-mediabeleid van de politie onderzocht. Na al die ophef zette de politie een formulier online voor mensen die vinden dat ze onterecht in een politiefilmpje staan.

Sinds november 2017 zijn dertien van die verzoeken gedaan, waarvan in twee gevallen geconcludeerd is dat er 'inderdaad onterecht' privacygevoelige informatie online was gezet. Vijf verzoeken werden niet in behandeling genomen, zes onderzoeken lopen nog. De Monitor vond in 163 politiefilmpjes overigens 31 privacy-schendingen.

Verzoek om gepubliceerd beeldmateriaal te verwijderen

De politie publiceert foto's en video's voor allerlei doelen. Soms worden foto's of video's gepubliceerd door agenten die willen laten zien wat politiewerk inhoudt. Dit zijn zogeheten 'blogs' en 'vlogs'. Daarin komen soms burgers in beeld. Hoewel de politie er naar streeft om niet onnodig personen herkenbaar in beeld te brengen, kan het toch voorkomen dat het gebeurt. Bent u zelf in beeld en wilt u hiertegen bezwaar maken, dat kan. Gebruik dan het onderstaand formulier. Nadat u het formulier heeft ingevuld en verstuurd, ontvangt u van de politie bericht over de behandeling van uw verzoek. Desgewenst wordt u (alsnog) onherkenbaar gemaakt op beeld of wordt de opname offline gehaald.

Cyberspace

De politie Midden-West-Brabant onderzoekt een facebook-account van een 'rechercheur'. Via dat account, niet van de politie zelf dus, zijn 'storende' berichten verstuurd. In die berichtjes ging het over 'politiezaken' maar onduidelijk is waarover precies. Wel is duidelijk dat échte politiemensen zich gekwetst voelen door de toon van die berichtjes. Het gebruik van het politielogo is strafbaar, net als je voordoen als agent, aldus een woordvoerder. Omdat Facebook niet zomaar ip-adressen afgeeft, vraagt de politie het account te 'rapporteren'.

———————————————

Het 'boek' bestaat al jaren, is vrij simpel te vinden maar op het Binnenhof is deze week 'geschokt' gereageerd op het bestaan van een online handleiding voor pedofielen. RTL Nieuw vond de handleiding weer eens, dit keer op het darkweb – en dan zijn alle rapen gaar. CDA, GL en PVV willen nu een verbod op (bezit en verspreiding) het boek. Minister Ferd Grapperhaus (Justitie) zegt wel iets in zo'n verbod te zien. Hij wil 'tot het uiterste gaan' om dat voor elkaar te krijgen 'omdat kindermisbruik een kind in zijn grondrechten aantast'. De handleiding beschrijft 'op bijna pedagogische wijze' over het winnen van vertrouwen maar ook over het uitwissen van dna-sporen na het misbruik, is bijvoorbeeld in Groot-Brittannië al verboden.

———————————————-

Minister Ferd Grapperhaus (VenJ … eehh JenV) wil nog in 2018 een start maken met het actieprogramma Kindveilig Internet. Dat bevat extra maatregelen tegen het verspreiden van kinderporno op internet. 'Het is schokkend hoe de afgelopen jaren het aantal meldingen van online kinderporno is toegenomen met de voortschrijdende digitalisering van de samenleving', aldus Grapperhaus die pleit voor een 'hardere en stevigere aanpak dan voorheen'. Onderdeel van het programma is mogelijk een lijst van 'bad hosters', internetbedrijven die verdienen aan kinderporno en andere illegale content. Enkele ministeries, de TU Delft en het bedrijfsleven werken verder aan een meetmethode om te zien hoe de techbedrijven omgaan met kp-meldingen. Dat aantal steeg van 2014 op 2017 van drieduizend naar achttienduizend.

———————————————

Na een hack gaan momenteel op internet lijsten rond met namen, mail - en ip-gegevens van duizenden gebruikers van websites en platforms waar liefhebbers van bestialiteit rondgaan. De zaak geef aan dat wat je ook doet online, er altijd een kans is dat de sites gehackt worden, zegt beveiligingsexpert Troy Hunt van Have I Been Pwned. De lijst bevat zo'n drieduizend unieke mailadressen, accountgegevens van één specifieke dierenpornosite; de naam ervan is niet bekendgemaakt.

———————————————

In de kop van Noord-Holland zijn in een maand tijd zeker 21 auto's leeggeroofd. De boeven wisten de elektronische sleutels te hacken en gingen er vandoor met airbags en navigatiesystemen. Het scannen gebeurde soms door deuren en muren heen, meldt Bureau NH. Een autobedrijf in de regio meldt 'een complete chaos' en adviseert de sleutels veilig te bewaren, bijvoorbeeld in een koekblik.

———————————————--

Ook al is de mail zeer doorzichtig, weet negen op de tien Nederlanders niet eens hoe aan bitcoins te komen en hebben veel geadresseerden niet eens een webcam – de recente stroom aan porno-mailtjes houdt de gemoederen aardig bezig. De politie zou al 'enkele honderden meldingen' hebben ontvangen. Volgens Quote hebben de oplichters op één bitcoinadres inmiddels al vele duizenden euro's aan afpersgeld verzameld, en hebben ze nog meer bitcoinadressen in beheer. Op één adres kwam al ruim een halve bitcoin binnen, goed voor een paar duizend euro. Wie het spoor verder volgt, ziet meerdere bitcoinadressen en veel meer geld. Onduidelijk, ook voor Quote, is wie het eindpunt van al die betalingen is. 'Maar op al die adressen staan bitcoins. Allemaal afkomstig van chantage?'

———————————————--

De politie Zeeland-West-Brabant heeft in totaal drie mannen opgepakt die worden verdacht van witwassen en internetfraude. De verdachten (20 en 23, allen uit Roosendaal) benadeelden elf personen door middel van smishing: phishing via sms. Het resultaat is hetzelfde: argeloze gebruikers loggen in op een nepsite en laten daar hun inloggegevens achter.

Rechtspraak

De politierechter in Den Bosch heeft een man (22, uit Tilburg) veroordeeld tot 120 dagen celstraf (waarvan 37 voorwaardelijk) voor smaad, stalking en bedreiging van zijn ex-vriendin. De verdachte, boos dat zij de relatie verbrak, had onder meer onder haar naam seksadvertenties op internet gezet. De vrouw werd tientallen keren gebeld door mannen die haar naam lazen op een erotische website. In mails schreef de verdachte zijn ex dat hij haar 'binnenkort kapot zou maken'. Bemiddeling tussen politie en verdachte mislukte: de man kwam niet opdagen. De politierechter sprak van een 'verwerpelijke vorm van pesten' en legde naast de celstraf ook verplichte therapie en een contactverbod op.

———————————————-

Van de Raad van State hoeft de politie niet bekend te maken hoe vaak de spyware is gebruikt waarmee computers van verdachten kunnen worden geïnfecteerd. De zaak, aangespannen door Bits of Freedom, speelt al enkele jaren. BoF deed een Wob-verzoek, de politie gaf info maar niet voldoende voor BoF dat daarop naar de rechter stapte. In 2016 gaf een rechtbank BoF gelijk, waarop de korpschef beroep aantekende en de zaak uiteindelijk bij de Raad van State terecht kwam. Die oordeelt nu dat het openbaar maken van sommige documenten onderzoeken naar strafbare feiten kan belemmeren.

———————————————-

Een man (57, Wieringerwerf) die dreigmails stuurde naar ambtenaren van de gemeente Hollands Kroon, is door de rechter in Alkmaar veroordeeld tot veertig uur werkstraf en het betalen van smartegeld aan drie ambtenaren. De verdachte had ruzie met zijn achterburen, een gevalletje rijdende rechter eigenlijk, en daarna met de gemeente die hem sommeerde een illegaal bouwwerk in zijn tuin weer af te breken. In een boze mail bedreigde hij handhavers van de gemeente met de dood.

———————————————-

De rechtbank Groningen heeft zes verdachten die in 2013 op grote schaal met DigiD-gegevens fraudeerden, veroordeeld tot celstraffen. De zes dupeerden honderden studenten: hun gegevens werden gebruikt om nieuwe DigiD-codes aan te vragen en toeslagen te regelen. De Belastingdienst keerde bijna vier ton onterecht uit. Hoofdverdachte Frits T., ex-belastingambtenaar, kreeg 2,5 jaar, de andere vijf verdachten kregen straffen tot twee jaar.

———————————————-

Ene Mezdi, actief in/op Temptation Island, is zijn rijbewijs voorlopig kwijt. Hij moet verder 1134 boete betalen en een educatieve maatregel volgen. De man (21) reed knetterhard op de A32 bij Heerenveen, rechts inhalend en over de vluchtstrook, en streamde dat live op instagram. RTL Nederland zond de beelden later landelijk uit, waarna de politie een onderzoek startte. In een tweet meldt de politie dat Mezdi's rijbewijs is ingevorderd. Zelf lijkt hij daar niet mee te zitten: op instagram reageerde hij met 'wereldnieuws'.

———————————————-

De bitcoins konden van niets anders afkomstig zijn dan van diefstal, vond de rechtbank. En dus werden zes mannen veroordeeld voor witwassen tot celstraffen van één tot drie jaar. In de zaak stonden twee groepen terecht, handelaren en hun klanten. Drie handelaren (21, 25 en 27, uit Arnhem en Krimpen aan den IJssel, hoog opgeleide ict-ers en actief in de financiële wereld, namen de bitcoins aan, om ze te om te zetten in contant geld. Het ging om transacties van een ton tot tien miljoen. Ze gebruikten een zogeheten mixerdienst, software om bitcointransacties te verhullen. De drie klanten (29, 39 en 44) betaalden 10% commissie – waar 1% gebruikelijk is – om hun inkomsten uit drugshandel op het darkweb wit te wassen. Ze vielen op door grote cash-opnames.

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 tele-foon
- Documentaire: Veiligheid en privacy
- Herken een nep-hotspot
- Gebruik wachtzinnen
- Drive-by-downloads voorko-men
- Hoe herken je een phishing mail
- Beveiligd internetbankieren
- Privacy—ik heb toch niets te verbergen
- Mousejack

Help wanted:

- Grooming
- Sexting
- Webcammis-bruik
- Bedreigd/ gechanteerd
- Kinderporno
- Nepprofiel