VEILIGHEIDSCOALITIE
Midden-Nederland

Artikelen Digitale Veiligheid en Corona

Een bundeling van alle artikelen over digitale veiligheid uit de corona trendinventarisaties 1 t/m 10.
Klik op onderstaande titel om het volledige artikel te lezen.

Inhoud

1 Artikelen over digitale veiligheid en Corona

1.1 De klassieke criminaliteit is bijna gehalveerd

De criminaliteit is veranderd onder invloed van de coronamaatregelen, vertelt Jaap de Waard van het ministerie van Justitie en Veiligheid in een video-interview. Het Centrum van Criminaliteitspreventie en Veiligheid interviewde hem voor het vakblad Secondant. Er is een enorme daling van de klassieke, offline criminaliteit, maar de gelegenheid voor daders van cybercriminaliteit is gegroeid. Bekijk het interview of lees zijn artikel.
(Dit artikel is geschreven door het Centrum van Criminaliteitspreventie en Veiligheid, CCV).

1.2 Aanpassingsvermogen van criminelen: analyse Europol

Het regionaal samenwerkingsverband Noord-Holland 'Samen Veilig' wijst op een rapport van Europol dat een overzicht geeft van hoe criminelen zich razendsnel weten aan te passen aan de huidige crisissituatie. Het is gebaseerd op informatie dat Europol 24/7 ontvangt van de EU-lidstaten. Er is een stijging te zien van phishing mails, malware en online zoektochten naar kinderpornografie of oproepen in fora om met kinderen in contact te komen.

1.3 Jonge cyberdaders willen zich bewijzen

Jongens die hacken en DDoS-aanvallen uitvoeren, verschillen van jongens die crimineel gedrag vertonen op straat. Ze worden vooral gedreven door leer- en nieuwsgierigheid. Traditionele interventies passen jonge cyberdaders daarom niet zo goed. “Wie het om geld te doen is, is minder ontvankelijk voor een traject dat zich richt op prosociaal zijn.” Lees hier het artikel over jonge cyberdaders.

1.4 Coronafraude: nieuwe smoes met bestaande technieken

Het is 29 januari 2020. De Fraudehelpdesk (FHD) ontvangt de eerste melding van coronafraude. Een slachtoffer is online opgelicht bij de aankoop van mondkapjes. Half april staat de teller al op 1.050 meldingen waarin het coronavirus gebruikt werd voor oplichting. Zijn er nu meer fraudemeldingen door het coronavirus? En hoe spelen criminelen in op deze pandemie? CCV-adviseur Mila Cassée ging hierover in gesprek met Tanya Wijngaarde van de FHD. Lees hier!

1.5 Politie boekt succes in aanpak Ddos-diensten en waarschuwt jongeren

De politie heeft vorige week meerdere DDoS-diensten platgelegd. Er werd bij de actie samengewerkt met hostingbedrijven, registrars*, Europol, Interpol en de FBI. De coördinatie lag bij het cybercrimeteam van de politie Midden-Nederland. De DDoS-diensten, zogeheten *booters*, boden klanten aan om tegen betaling aanvallen tegen websites uit te voeren. Dat is meestal strafbaar, waarschuwt de politie de veelal jonge aanvallers. ‘Daders onderschatten de gevolgen van deze aanvallen voor slachtoffers. Ze realiseren zich bovendien niet dat de politie ze weet te vinden en hen een straf en flinke schadeclaim boven het hoofd hangt’, aldus Jeroen Niessen van het cyberteam.

*: Een registrar is een bedrijf dat in opdracht van bedrijven, instellingen of personen een domeinnaam registreert.

1.6 Criminelen maken (ook digitaal) volop misbruik van coronacrisis

Het is een bekend fenomeen dat criminelen inhaken op actuele gebeurtenissen. Dat gebeurt ook nu in de coronacrisis, zoals phisingsmails uit naam van het RIVM of babbeltrucs als boodschappenhulp. Tegen al deze vormen van criminaliteit kan niet vaak genoeg gewaarschuwd worden. Om mensen te wijzen op de gevaren van babbeltrucs adviseren we de politiebrochure ‘senioren en veiligheid’ opnieuw onder de aandacht te

brengen. Ook het waarschuwingsfilmpje 'veilig aan de deur' kan verspreid worden. Specifiek voor phishingmail adviseren we het waarschuwingsfilmpje van alert online te verspreiden en/of de tips van het digital trustcentre.

Phisingmail uit naam van het RIVM

Er zijn e-mails in omloop die afkomstig lijken van het Rijksinstituut voor Volksgezondheid en Milieu (RIVM). De e-mails beloven een update over corona, maar zijn in werkelijkheid bedoeld om de ontvangers te besmetten met malware of persoonlijke gegevens te ontfutselen. De 'RIVM'-phishing staat niet op zichzelf. Action Fraud, het nationale Britse kennisinstituut op het gebied van fraude, stelt dat coronaphishing uit naam van overheidsinstanties cybercriminelen al ongeveer een miljoen euro zou hebben opgeleverd. (bron: digital trustcentre).

Babbeltruc zogenaamde boodschappenhulp

Criminelen gebruiken ook de ouderwetse babbeltruc om mensen geld en gegevens afhandig te maken. Kwetsbare inwoners krijgen zogenaamd boodschappenhulp aangeboden. Criminelen ontfutselen de bankpas en code en plunderen vervolgens de bankrekening.

1.7 Coronafraude: nieuwe smoes met bestaande technieken

Het is 29 januari 2020. De Fraudehelpdesk (FHD) ontvangt de eerste melding van coronafraude. Een slachtoffer is online opgelicht bij de aankoop van mondkapjes. Half april staat de teller al op 1.050 meldingen waarin het coronavirus gebruikt werd voor oplichting. Zijn er nu meer fraudemeldingen door het coronavirus? En hoe spelen

criminelen in op deze pandemie? CCV-adviseur Mila Cassée ging hierover in gesprek met Tanya Wijngaarde van de FHD. Lees hier!

(Dit artikel is geschreven door Het Centrum van Criminaliteitspreventie en Veiligheid, Het CCV)

1.8 Vijf keer zo veel aangiftes WhatsAppfraude in Midden-Nederland

Het cyberteam Midden-Nederland ziet een toename van het aantal whalingszaken via WhatsApp. Sinds 6 maart hebben in de regio 74 mensen aangifte gedaan, ruim vijf keer zo veel als in dezelfde periode vorig jaar. Volgens de politie wordt er misbruik gemaakt van de coronacrisis. Vooral mensen van 60 jaar en ouder met volwassen kinderen zijn het slachtoffer. Opvallend is dat de cybercriminelen hun best doen om over te komen als de echte kennis die geld vraagt omdat hij of zij in nood zit en niet meer bij zijn geld kan. Dit wordt ook wel 'whaling' (walvisvangst) genoemd. Whaling is een techniek waarbij de crimineel zich voordoet als een bekende van het beoogde slachtoffer, en de communicatie is gepersonaliseerd. De crimineel gebruikt hier bijvoorbeeld informatie voor van social media. Lees het persbericht om meer over de werkwijze van criminelen te lezen en tips om slachtofferschap te voorkomen.

Oproep aan gemeenten

De politie vraagt gemeenten in Midden-Nederland het persbericht via sociale mediakanalen te verspreiden. Aanvullend kan specifiek voor WhatsApp buurpreventiegroepen onderstaand bericht door gemeenten worden gebruikt. Voor vragen hierover: neem contact op met Martijn Simons, programmamanager Digitale Veiligheid bij Bureau RVS.

De politie waarschuwt voor fraude van criminelen via WhatsApp. Krijgt u een appje waarin een bekende om (veel) geld vraagt? Bel deze persoon dan altijd op om te checken of dit verzoek echt is. Is het een nieuw telefoonnummer? Bel dan ook het oude nummer! Klik niet op linkjes en deel nooit uw persoonlijke gegevens of pincode. Bent u slachtoffer van WhatsApp-fraude bel dan 0900 8844. Of kijk voor meer informatie op www.politie.nl.

1.9 €15.000,- kwijt door truc met QR-code

Criminelen spelen listig in op de coronacrisis, zo ondervond 'Frank' aan den lijve. In tijden van corona moet je elkaar steunen, dacht hij toen een buitenlandse toerist in Rotterdam hem om hulp vroeg. Zij kon niet met de bus omdat daar geen contact geld wordt aangenomen, waarop hij vervolgens zijn hulp aanbood. Hij wist niet dat hij via een uiterst gewiekste truc met een QR-code een kleine 15.000 euro zou kwijtraken.
Het verhaal van Frank laat zien dat criminelen met slinkse trucs proberen een slaatje te slaan uit de coronacrisis. Het Parool schreef er een uitgebreid artikel over en sprak behalve met 'Frank' ook met collega's van de politie en de fraudehelpdesk.

1.10 Opsporing Verzocht Cyber?

Vorige week was het al even in het nieuws. De politie roept de hulp in van techplatform Tweakers in het onderzoek 26Ramsey. Een complex onderzoek naar grootschalige factuurfraude waarbij bedrijven voor minimaal €100.000 worden opgelicht en werkzoekende vrouwen worden misleid om voor de daders aan de slag te gaan. In dit filmpje legt het Cyberteam Midden-Nederland uit hoe de daders werken en waarom de politie de hulp van Tweakers goed kan gebruiken. Het gaat om een pilot van zes maanden waarin 100 geselecteerde tweakers gevraagd worden om in het onderzoek mee

te denken. De komende tijd worden er behalve 26Ramsey, nog meer onderzoeken naar het platform gebracht.

1.11 Voor het eerst meer cybercrimedelicten dan woninginbraken

De coronacrisis heeft geleid tot een ongekende toename in het aantal geregistreerde cybercrime-incidenten in Nederland. Waar in maart de politie nog 696 incidenten registreerde, waren dat er in april 870 en maar liefst 1869 in mei 2020. Het is voor het eerst dat het aantal cybercrimedelicten het aantal woninginbraken overstijgt (1869 cybercrimedelicten versus 1344 woninginbraken). Dit blijkt uit een analyse van de nieuwste landelijke cybercrimestatistieken door VPNgids.nl. Voor de analyse is gebruik gemaakt van data afkomstig van de politie, het Centraal Bureau voor de Statistiek en inzichten van verscheidene cybersecurity experts. De analyse geeft tevens de mogelijkheid om op gemeenteniveau in te zoomen op het aantal geregistreerde cybercrime-incidenten in de eerste maanden van 2019 en 2020. Lees hier de gehele analyse.

1.12 Praktische hulp en goede voorbeelden

1.12.1 Tips tegen computerinbraken

We zijn met z'n allen veel meer thuis en daardoor ook meer online op het eigen netwerk. Het risico dat criminelen inbreken op onze computers is daarmee ook een stuk groter geworden. De gemeente Rotterdam waarschuwt haar inwoners met een eenvoudig maar duidelijk filmpje. Voor de volledigheid hebben we de 10 tips uit het filmpje hieronder op een rij gezet.

Let op: tip 7 is aangevuld met informatie van de fraudehelpdesk. Dit omdat een website controleren op betrouwbaarheid helaas iets moeilijker is geworden nu criminelen in staat

zijn foute websites te bouwen die alsnog over een groen slotje beschikken en beginnen met https. Gelukkig heeft de fraudehelpdesk een simpele tool ontwikkeld om websites op betrouwbaarheid te toetsen. Gebruik onderstaande tips in de publieksvoorlichting zodat inwoners van jouw gemeente minder snel slachtoffer worden van corona-gerelateerde digitale criminaliteit.

1. Gebruik de nieuwste software en installeer updates
2. Installeer een antivirusprogramma
3. Maak wachtzinnen in plaats van wachtwoorden
4. Maak alleen verbinding met vertrouwde wifi-netwerken
5. Open geen onbekende berichten en/of bestanden
6. Installeer apps alleen via erkende winkels
7. Controleer het adres van websites. Dit kan via de fraudehelpdesk.
8. Verbreek de verbinding bij onbetrouwbare oproepen. Vaak gaat het om buitenlandse nummers.
9. Bedenk goed wat je met wie deelt online
10. Maak regelmatig back-ups

1.12.2 Tips tegen online oplichting in coronatijd

Criminelen verzinnen van alles om ons als mensen op het verkeerde been te zetten. Ze hopen dat we in een onbewaakt ogenblik toehappen, bijvoorbeeld als we stress hebben of snel tussendoor iets moeten regelen. Juist op dat soort momenten zijn we immers kwetsbaar. Ook over oplichtingspraktijken in coronatijd heeft de gemeente Rotterdam een filmpje gemaakt. Gebruik onderstaande tips in de publieksvoorlichting zodat inwoners van jouw gemeente minder snel slachtoffer worden van corona-gerelateerde digitale criminaliteit.

1. Antibacteriële bankpassen bestaan niet
2. Check wie een beveiligde link stuurt. Je werkgever of een crimineel
3. De GGD vraagt telefonisch en per mail niet om informatie en komt ook niet zomaar langs
4. Mensen die op straat vragen een QR-code te scannen: doe het niet
5. Let op voor valse webshops die boodschappendiensten, mondkapjes en coronatesten aanbieden
6. Een uitkering aanvragen doet je niet via Whatsapp. Negeer en verwijder zo'n bericht.

1.12.3 Make your home a cybersafe stronghold

Interpol en het European Cybercrime Center hebben voor het grote publiek een treffende preventieposter gemaakt onder de titel 'Make your home a cybersafe stronghold'. Vanuit bureau RVS (programma digitale veiligheid) en het cyberteam van de Politie wordt deze poster vertaald en binnenkort ter beschikking gesteld. De Engelstalige versie vind je alvast hier.

1.12.4 Jongeren veilig online

Vanwege de coronacrisis zitten veel jongeren thuis. Hierdoor zijn ze nog actiever online en dit brengt gevaren met zich mee. Juist in deze periode is het belangrijk om hier alert op te zijn. Maar hoe kun je er als ouder en jongere voor zorgen dat je veilig online bent? Hiervoor heeft het bureau HALT de poster 'Veilig Online' gemaakt. Deze poster geeft praktische tips. Daarnaast geeft de website van bureau HALT informatie over sociale media en jongeren.

1.12.5 Preventie van (digitale) criminaliteit gericht op jongeren nu extra belangrijk

Preventie van digitale criminaliteit gericht op jongeren is in deze crisis extra belangrijk. Veel jongeren zitten thuis en gaan experimenteren. Ze realiseren zich vaak niet dat ze strafbaar bezig zijn. Volgens Theo van der Plas, programmadirecteur Digitalisering en Cybercrime bij de Nationale Politie, zijn ze vaak maar één klik verwijderd van cybercrime. Hij wijst daarom op de positieve alternatieven, waar jongeren hun skills kunnen testen in een uitdagende, maar veilige spelomgeving. Voorbeelden zijn Hack the box, Certified Secure of OWASP juice shop.

1.12.6 Gamechangers: jongeren en wijkagenten samen tegen cybercrime

Vorige week heeft de politie de campagne ‘Gamechangers’ gelanceerd. Via speciale games wil de politie jongeren uit de cybercriminaliteit houden. Gamechangers stelt jongeren tussen de 12 en 18 jaar voor online uitdagingen. Ze leren hun vaardigheden op een veilige manier te testen en waar mogelijk te verbeteren. Tegelijkertijd doen ze kennis op over wat wel en niet strafbaar is op het internet. Aan de campagne doen ook wijkagenten mee die al op meerdere plekken tegen jongeren spelen. Het idee is om in contact te komen met jongeren en hen te weerhouden van het plegen van criminaliteit. Dat maakt het spel een gamechanger in dubbel opzicht; de betrokkenheid van wijkagenten laat zien dat een veilige wijk ook een digitaal veilige wijk betekent. Gemeenten kunnen helpen om ‘gamechangers’ tot een succes te maken door via (sociale) media de gamechangers te promoten.

Ben jij een gamer? Doe dan mee aan de Gamechangers FIFA CUP!

Houd je van technologie, games én challenges? En wil jij jezelf en jouw digitale skills verbeteren en anderen verslaan? Ga jij de uitdaging aan? Dan ben jij een Gamechanger en is dit platform speciaal voor jou!

1.12.7 Samen aan de slag met Digitale Veiligheid.

Digitale indringers en criminelen zijn voortdurend op zoek naar nieuwe manieren om gegevens van mensen (het nieuwe goud) te stelen en te misbruiken. Als Veiligheidscoalitie kunnen we dit een stuk moeilijker maken. Bijvoorbeeld door concreet aan de slag te gaan met interventies uit het recent verzonden Programma Digitale Veiligheid. Denk hierbij bijvoorbeeld aan digitale buurtpreventie, speciaal voor jongeren ontwikkelde games, de organisatie van (digitale) ondernemersbijeenkomsten of masterclasses voor bestuurders en adviseurs. Linde van der Meer (projectleider Digitale Veiligheid) en Martijn Simons (programmamanager Digitale Veiligheid) nemen hiervoor deze zomer contact op om te bekijken hoe we interventies succesvol in kunnen zetten.

2 Artikelen veilig thuiswerken

2.1 Wereld in een digitale versnelling

De coronacrisis heeft grote impact op onze digitale veiligheid. We maken met elkaar noodgedwongen een snelle digitale transformatie door. We gebruiken massaal thuiswerkvoorzieningen en online vergadertools en leren daar nu langdurig en intensief mee te werken. Dat is een uitkomst om het werk door te laten gaan. Na de coronacrisis zal de mate waarin we digitaal werken op een hoger niveau blijven dan voor de crisis. We zijn er vertrouwd mee geraakt en hebben ervaren hoe eenvoudig en efficiënt het is.

2.2 Criminelen misbruiken persoonsgegevens voor coronavergoeding

De afgelopen weken was er in deze nieuwsbrief veel aandacht voor veilig internetten en veilig thuiswerken. Onder andere door te verwijzen naar de website veiliginternetten.nl

en het speciale webdossier over veilig thuiswerken van het Nationaal Cyber Security Centrum. Een voorbeeld uit Duitsland maakt duidelijk hoe belangrijk deze onderwerpen zijn. In de deelstaat Noordrijn Westfalen konden bedrijven via een speciale website een coronavergoeding aanvragen om zo de effecten van de crisis te verzachten. Criminelen haakten aan bij de actie en maakten een kopie van de originele website waarop gebruikers hun gegevens invullen om vervolgens een vergoeding aan te vragen. Door bewoners van de deelstaat met een actieve phishing-campaign naar de nepsite te lokken, maakten de criminelen de gegevens van bedrijven buit en vulden deze vervolgens zelf in op de originele site waarbij enkel de bankgegevens werden gewijzigd naar die van de criminelen. Het gevolg is mogelijk tientallen miljoenen euro's schade en duizenden mensen die nu geen coronavergoeding ontvangen.

2.3 Zoom-bombing: Wat is dat nou weer?

De populaire video-app Zoom is de laatste weken negatief in het nieuws. Zoom zou onvoldoende transparant zijn over de wijze waarop men met persoonsgegevens omgaat. Ook zou er sprake zijn van ernstige beveiligingslekken. Op 8 april kwam daar het nieuws bij dat kinderen van een school in Zoetermeer tijdens de les via Zoom pornobeelden te zien kregen. Eerder die week berichtte The Washington Post al dat schoolorganisaties in de VS het gebruik van Zoom aan banden leggen omdat onbevoegden gesprekken binnendringen en via de functie waarmee het beeldscherm wordt gedeeld, racistische en pornografische beelden laten zien.

Dit fenomeen wordt ook wel 'Zoom-bombing' genoemd. Volgens de Autoriteit Persoonsgegevens zijn dit soort diensten vaak gratis omdat aanbieders gegevens van gebruikers gebruiken voor andere doeleinden zoals marketing. Ook komt het voor dat gegevens aan derden worden verkocht. Als dat gebeurt, zijn gebruikers de controle kwijt

over hun eigen gegevens en is het onduidelijk wat er allemaal nog meer mee gebeurt. Reden genoeg dus om waakzaam te zijn op dergelijke zogenaamde ‘gratis’ diensten. Gratis bestaat in dit geval dus niet.Wil je weten hoe je dat kunt voorkomen? Bekijk dan de tips van het NCSC over veilig videobellen en online vergaderen.

2.4 Veilig digitaal thuiswerken

Met de cyberincidenten van Maastricht en de gemeente Lochem nog vers in het geheugen, wordt digitale veiligheid in alle instructies rondom thuiswerken serieus genomen. We beseffen dat veilig thuiswerken op dit moment cruciaal is om het werk nog enigszins door te laten gaan. Er wordt dan ook massaal gehoor gegeven aan de adviezen van het Nationaal Cyber Security Center (NSCS) om de digitale hygiëneregels in acht te nemen. Zoals tijdig updates uitvoeren, alert zijn op phishingmails en malafide coronasoftware, vertrouwelijk informatie niet via berichtenapps of videoconferences te delen enzovoorts. Door de coronacrisis neemt de bewustwording over veilig digitaal werken een enorme vlucht. Bekijk de website. Ook via de media is er veel aandacht voor ‘veilig thuiswerken’. Zo maakte ‘1Vandaag een mooie reportage over internetcriminelen en thuiswerken. Journalist Huib Modderkolk, Aleid Wolfsen van de Autoriteit Persoonsgegevens en Hielke Bontius van het NCSC gaan in op veilig videobellen, het belang van updates en het voorkomen van spionage en misleiding. Bekijk hier de reportage.

2.5 Luister of kijk terug: online event digitaal thuiswerken en digitale criminaliteit

Op 18 juni gingen Iris Meerts, Remco Spithoven, Marianne Junger, Mike Jansen en Jetse Fluitman het gesprek aan over digitale veiligheid en thuiswerken. Het gesprek werd begeleid door tech- en internetexpert Danny Mekić. Centraal stond de koppeling tussen veilig digitaal thuiswerken en digitale criminaliteit.

De gasten haken in op drie thema's. Hoe verandert de rol van informatiebeveiliging door het toenemend aantal thuiswerkenden, op welke manier maken hackers misbruik van de coronacrisis en menselijk gedrag en wie is verantwoordelijk voor veilig digitaal thuiswerken?

Nadat de technische mankementen waren opgelost, keken meer dan 100 mensen live mee. Alle kijkers bedankt voor jullie geduld en flexibiliteit! Heb je het gemist maar wil je toch nog kijken? Dat kan! Bekijk de video of luister het als podcast (kijk- en luistertijd: 1 uur en 6 minuten).

2.6 Cybersecuritybeeld 2020: dreiging onverminderd groot

Het cybersecuritybeeld 2020 laat zien dat de digitale risico's voor Nederland onverminderd groot en niet fundamenteel veranderd zijn. Ook de weerbaarheid blijkt nog lang niet overal op orde te zijn. Partijen zijn daardoor extra kwetsbaar voor cyberincidenten. Dat geldt zeker wanneer onvoldoende basismaatregelen zijn getroffen, die eerste barrières opwerpen tegen aanvallen, schade beperken en herstel eenvoudiger maken wanneer zich toch incidenten voordoen. Het securitybeeld gaat hierbij specifiek in op het belang van cyberveilig gedrag en cyberhygiëne van medewerkers. In het programma Digitale Veiligheid zijn deze focuspunten ook benoemd. De komende maanden en jaren geven we hier via masterclasses en webinars gericht aandacht aan.

Verder gaat het cybersecuritybeeld vooral in op: 1. De nationale veiligheid en het risico van (voorbereidingen voor) sabotage en spionage door statelijke actoren. 2. Het risico van (grootschalige) uitval van digitale diensten, processen of systemen. 3. Het risico van cyberaanvallen door criminele actoren die het te doen is om economisch gewin. Vooral afpersing door de inzet van ransomware blijkt succesvol. Mogelijk is er onder criminelen sprake van toenemende intenties en capaciteiten om procesbesturingssystemen van vitale processen te raken. Ransomware, maar ook informatiediefstal of digitale manipulatie door criminelen heeft primair impact op de organisatie die daarvan het slachtoffer is. Toch ondervinden ook andere diensten, processen, systemen en organisaties die daarvan afhankelijk zijn of daarmee in verbinding staan de gevolgen'. Als voorbeeld worden de criminele cyberaanvallen op de gemeente Lochem en de Universiteit Maastricht benoemd die laten zien hoe groot de gevolgen kunnen zijn voor organisaties, hun medewerkers en burgers. Het rapport over de cyberaanval op de Universiteit Maastricht kun je hier downloaden.

2.7 Praktische hulp en goede voorbeelden

2.7.1 Keuzehulp videobellen

Als je gebruik maakt van videobellen, wil je wel dat de privacy en veiligheid van jou en je organisatie serieus worden genomen. Daarom heeft de Autoriteit Persoonsgegevens (AP) bij 13 veelgebruikte videobel-apps gekeken naar de belangrijkste privacyaspecten. Denk hierbij aan welke gegevens de app verzamelt, wat de app daarmee doet en of de communicatie beveiligd is. De AP krijgt namelijk veel vragen over privacy bij zulke apps, nu mensen massaal zijn gaan videobellen tijdens de coronacrisis. De AP biedt daarom

een keuzehulp om verschillende videobel-apps te vergelijken. Opmerking hierbij is wel dat er geen uitgebreid, technisch onderzoek is gedaan naar de apps. Men is afgegaan op wat bedrijven zelf zeggen over wat hun videobel-apps met gegevens doen, bijvoorbeeld in hun privacyverklaring.

2.7.2 Initiatieven veilig thuiswerken: praktische tips voor werknemers en ondernemers

Vanuit het veiligheidsnetwerk heeft Jonathan van Eerd in samenwerking met cybercrimeinfo.nl een praktische video gemaakt die ingaat op veilig thuiswerken. Hij gaat in op de belangrijkste regels om slachtofferschap te voorkomen. Van veilig wachtwoordgebruik en software-updates tot het delen van gegevens en het voorkomen van helpdeskfraude.

- Bekijk de video op Youtube

Op de website www.werkthuisveilig.nl vind je allerhande praktische informatie voor organisaties en medewerkers. Daarnaast heeft het Nationaal Cyber Security Center op 1 april 2020 een factsheet gepubliceerd over de uitval van thuiswerksoftware. De factsheet bevat een uitgebreid handelingsperspectief over hoe organisaties zich op een dergelijk scenario kunnen voorbereiden.

2.7.3 Tips voor het MKB

Nu thuiswerken de komende weken de standaard is, doen ondernemers steeds meer online. Het aantal online bestellingen neemt toe en applicaties voor werken op afstand draaien overuren. Ondernemers communiceren ook steeds meer op afstand: veel mkb'ers zien hun medewerkers, klanten en leveranciers niet langer in levende lijve. Daarom publiceerde het SIDN-fonds 8 tips voor ondernemers.

1. Doe een phishing simulatie
2. Gebruik multi-factor authenticatie (MFA)
3. Wees creatief met voorlichting
4. Beperk niet-essentieel gebruik van je bedrijfsnetwerk
5. Wees voorzichtig met IoT-devices
6. Beperk het aantal applicaties dat je gebruikt voor thuiswerken
7. Zorg ervoor dat software up-to-date is
8. Zorg voor een goede virus- en malwarescanner

In de blog 'Zo laat je je medewerkers veilig thuiswerken' legt SIDN bovenstaande tips verder uit.

2.7.4 Speciale webpagina over corona en veilig internetten

Het netwerk stelt regelmatig de vraag hoe bewoners en ondernemers extra gewaarschuwd kunnen worden voor internetcriminaliteit. Het advies is om de website veiliginternetten.nl te bezoeken en daarin speciaal de pagina over Corona en digitale veiligheid. Vanuit de eerder dit jaar gelanceerde campagne 'Maak het ze niet te makkelijk' is voor gemeenten aanvullend handig materiaal beschikbaar voor verschillende (sociale media) kanalen.

3 Artikelen over data, privacy en kunstmatige intelligentie

3.1 Wees nu soepeler én strenger in toezicht op privacy

De Autoriteit Persoonsgegevens maakte 20 maart bekend dat het minder streng toeziet op een aantal privacyregels. Goed te verdedigen, zegt hoogleraar bedrijfsethiek aan de Erasmus Universiteit en partner bij KPMG Muel Kaptein in ToeZine. Tegelijkertijd stelt hij: “Omdat onze privacy in crisistijd meer onder druk staat, moet er extra aandacht zijn voor het toezicht erop.” Lees hier het interview!

3.2 Corona en kunstmatige intelligentie

Een melding als je te dicht bij iemand met griep staat en code rood bij koorts. Drones die je aanspreken als je geen mondkapje draagt. Een paar maanden terug ondenkbaar. Maar nu de dagelijkse praktijk in China. 1Vandaag maakte een reportage over ‘slimme data’ en het coronavirus. Ook buiten China worden met big data (overheidsdata, nieuwsberichten, vluchtgegevens etc.) in rap tempo algoritmes gemaakt die voorspellen hoe het coronavirus zich in de toekomst verspreidt zodat tijdig maatregelen getroffen kunnen worden. Dat kan mensenlevens sparen. Ten tijde van een crisis legitiem en begrijpelijk. Maar hoe houden we na de crisis het overzicht en de controle op deze ontwikkelingen in relatie tot publieke waarden als rechtvaardigheid, veiligheid, gezondheid en privacy. Door de crisis zal het gesprek hierover in een stroomversnelling raken. Ook wat toepassingen op veiligheidsgebied betreft. Bekijk hier de reportage.

3.3 Digitaal in contact: denk ook een beetje aan je data

Het SIDN-fonds roept op tot een kritische blik ten opzichte van alle grote platformen waar in deze crisis meer dan ooit gebruik van wordt gemaakt. Nu we massaal thuis werken en leren, blijven we dankzij legio technische mogelijkheden digitaal met elkaar in

contact. Skype, Teams, Zoom, Google Hangouts, WhatsApp, Signal, Facebook, Instagram en YouTube zijn veelgebruikte platformen. Het is uiteraard fijn dat deze mogelijkheden er zijn maar het maakt ons ook afhankelijk van commerciële technologiebedrijven, die vaak hun eigen (commerciële) belang hebben bij het ter beschikking stellen van deze platformen. Dat deze partijen over onze data beschikken hoeft geen groot probleem te zijn als het over 'onschuldige' informatie gaat. Het wordt echter een ander verhaal in het geval van vertrouwelijke informatie. Het is belangrijk jezelf dan de vraag te stellen welk platform het beste is voor jouw specifieke situatie. Met name wanneer het gaat om publieke domeinen als de zorg of het onderwijs is het goed om hier met een kritische blik naar te kijken". De blog 'Digitaal in contact; denk ook een beetje aan je data' geeft stof tot nadenken.

3.4 Wat zeggen deskundigen over de Corona-apps?

In het programma Digitale veiligheid 2020-2022 zijn publieke waarden een belangrijk element, met specifieke aandacht voor 'veiligheid' en 'privacy'. Vanwege de zogenaamde Corona-apps is de discussie over onze (digitale) veiligheid en privacy actueler dan ooit. Tijdens de persconferentie van 7 april jl. kondigde minister De Jonge aan dat het kabinet de inzet van twee apps overweegt. De eerste betreft een zogenaamde 'tracking- en tracing app' en de tweede een gezondheidsapp waarbij gegevens worden gedeeld met medisch specialisten. Deze apps roepen grote maatschappelijke vragen op over de gevolgen voor onze privacy en (digitale) veiligheid. Meer dan 60 wetenschappers verenigden zich en schreven een brief aan het kabinet waarin ze hun zorgen en standpunten toelichten. Het verdient aanbeveling deze te lezen. Want de argumenten die deze wetenschappers naar voren brengen zijn ook relevant voor

veiligheidsprofessionals. Bijvoorbeeld als de vraag op tafel komt in hoeverre we big data slim in willen zetten om onze wijken en buurten veiliger te maken.

- Technologie is zelden *de* oplossing voor een bepaald probleem. Gewaakt moet worden voor techno-solutionisme; de overtuiging dat voor elk probleem een technologische oplossing gevonden kan worden. De mogelijkheid moet blijven bestaan om te besluiten de apps niet in te zetten.
- Effectiviteit en betrouwbaarheid van de apps is van enorm belang; ineffectiviteit en onbetrouwbaarheid kan juist leiden tot een groter risico op besmetting. Het creëert dan immers slechts 'schijnveiligheid'.
- De apps hebben impact op meer dan (data)privacy alleen. Ze raken ook aan de vrijheid van vereniging, het recht op veiligheid, het recht op gezondheid en het recht op non-discriminatie.
- Fundamentele rechten en vrijheden kunnen niet zomaar opzij gezet worden. Daarvoor

3.5 Nationale DenkTank: over de digitale samenleving en gegevens als het 'nieuwe goud'

Ben je breed geïnteresseerd in de toekomst van onze digitale samenleving? Lees dan het advies van de Stichting de Nationale DenkTank. Deze stichting wil Nederland helpen bij het oplossen van actuele, taaie, maatschappelijke vraagstukken. Dit doet zij door jonge denkers aan de slag te laten gaan met een bepaald onderwerp en door bruggen te slaan tussen wetenschap, overheid en bedrijfsleven. Het afgelopen jaar heeft de DenkTank nagedacht over een gezonde, weerbare, inclusieve en eerlijke digitale samenleving. Het is een breed en fris advies dat ingaat op hoe we in een digitale samenleving mee kunnen komen, gezond blijven, menselijk contact blijven houden, onze kinderen kunnen opvoeden enzovoorts.

Data: het nieuwe goud

Ook gaat het advies in op de cybercrimeparadox. Zo gelooft 55% van de mensen dat ze voldoende maatregelen nemen tegen cybercriminaliteit, maar ondertussen gebruikt maar een fractie daarvan de daarvoor noodzakelijke cruciale password manager (17%) en veilige VPN verbinding (12%) (Newcom survey). Hier is dus nog een hoop werk aan de winkel. Maar het allerbelangrijkste punt van de DenkTank is toch wel dat wij met elkaar als individuele gebruikers van data beter beschermd moeten worden en vooral de controle moeten terug krijgen over onze data, ook wel het 'nieuwe goud' genoemd. Want uiteindelijk is dat het beste voor onze digitale veiligheid. Lees hier het rapport en de factsheet.

3.6 Gaan we niet te ver in ons digitale leven?

In het 'nieuwe normaal' vertrouwen we ons hele hebben en houden toe aan Amerikaanse platforms, maar we hebben geen idee wat er gebeurt met de datastroom. Hoogleraar Ronald Leenes vertelt in Secondant over de gevaren van het beeldbellen in de coronacrisis voor onze privacy. "In één klap geven wij onze levenssfeer op om door te kunnen gaan alsof er niks aan de hand is." Lees hier meer.

(Dit artikel is geschreven door Het Centrum van Criminaliteitspreventie en Veiligheid, Het CCV).

3.7 Wees nu soepel én strenger in toezicht op privacy

De Autoriteit Persoonsgegevens maakte 20 maart bekend dat het minder streng toeziet op een aantal privacyregels. Goed te verdedigen, zegt hoogleraar bedrijfsethiek aan de

Erasmus Universiteit en partner bij KPMG Muel Kaptein in ToeZine. Tegelijkertijd stelt hij: “Omdat onze privacy in crisistijd meer onder druk staat, moet er extra aandacht zijn voor het toezicht erop.” Lees hier het interview!

(Dit artikel is geschreven door het Centrum van Criminaliteitspreventie en Veiligheid, CCV)

3.8 Camera’s in coronatijd; zegen of vloek?

Is er een digitale oplossing met cameratoezicht om de opkomende drukte in onder meer binnensteden in goede banen te leiden? Een vorm van crowdcontrol, maar dan voor het handhaven van de anderhalve meter maatregel. Steeds meer gemeenten zoeken daarnaar en onze technologische vooruitgang maakt het mogelijk. Adviseur cameratoezicht van Het CCV Rodney Haan zoekt in dit artikel naar antwoorden.

(Dit artikel is geschreven door Het Centrum van Criminaliteitspreventie en Veiligheid, Het CCV).

3.9 Start promotie-onderzoek Wybren van Rij over de invloed van digitalisering in het veiligheidsdomein

Ik ben Wybren van Rij, docent Integrale Veiligheidskunde aan de Hogeschool Utrecht.

Vanaf september start ik een promotieonderzoek naar de toenemende invloed van digitalisering in het veiligheidsdomein. In hoeverre speelt (grootschalige) dataverzameling en analyse daarin een rol en wat zijn de verwachtingen voor de toekomst? Bijvoorbeeld bij de aanpak van ondermijning, de aanpak van ernstige overlast of bij toezicht en handhaving? En wat betekent dat eigenlijk voor publieke waarden als rechtvaardigheid, inclusie en autonomie? En hoe kunnen we hier als veiligheidsprofessionals met elkaar op een verantwoorde manier mee omgaan? De komende maanden en jaren ga ik hierover graag met jullie en bureau RVS (Programma Digitale Veiligheid) in gesprek. De voortgang en resultaten van mijn promotieonderzoek wil ik regelmatig via bureau RVS met jullie delen, bijvoorbeeld via artikelen en workshops.

Ben je benieuwd naar het onderzoek van Wybren van Rij of heb vragen/ideeën? Neem contact op met Martijn Simons, programmamanager Digitale Veiligheid.

3.10 Praktische hulp en goede voorbeelden

3.10.1 Heej, ben jij wel degene die belt?

Stel je voor, als burger bel je de gemeente om een rijbewijs te verlengen of een wijziging in een subsidieaanvraag door te geven. Dit zijn strikt persoonlijke zaken, dus je zult eerst moeten aantonen wie je bent. Tegenwoordig kom je telefonisch of via de website een heel eind. Maar is dit betrouwbaar genoeg en hoeveel privacy moet je prijsgeven om aan te tonen dat jij het echt bent? Uiteindelijk moet je toch naar de balie in het gemeentehuis komen om je in persoon te laten zien. Lastig allemaal. Zeker in coronatijd. Dus... is het ook mogelijk je identiteit te bewijzen zonder fysiek contactmoment?

App met gewaarborgde identiteit

De gemeenten Nijmegen, Arnhem en de regio Drechtsteden denken van wel. Ze werken samen aan de ontwikkeling van ID-Bellen: een app op de mobiele telefoon die straks jouw gewaarborgde identiteit bevat. Via de app bepaal je zelf aan welke partijen je welke identiteitsgegevens beschikbaar stelt. De gemeente helpt je hiermee op weg. Die geeft van tevoren aan welke gegevens zij nodig heeft om jouw identiteit op afstand vast te stellen. Bijvoorbeeld voor het afnemen van gemeentediensten. Dit kan dan telefonisch, via de ID-Bellen app. Je hoeft je niet te melden bij de balie op het stadskantoor. ID-Bellen maakt gebruik van IRMA, van de Stichting Privacy By Design. De afkorting staat voor ‘I Reveal My Attributes’. Vrij vertaald betekent dit ‘Ik geef mijn identiteitsgegevens vrij’. De IRMA-app werkt als een ‘online paspoort’ waarin je op een veilige manier jouw

persoonlijke en vertrouwelijke gegevens bewaart. Op verzoek kan je deze deels onthullen.

Programma Digitale Veiligheid monitort ontwikkelingen

IRMA is één van de initiatieven die we binnen het programma Digitale Veiligheid monitoren. Dat doen we niet voor niets. Het is namelijk een initiatief dat zowel de veiligheid als privacy van mensen versterkt en digitale criminaliteit kan voorkomen. En dat is precies wat we met het programma Digitale Veiligheid beogen. Wil je meer weten of heb je vragen? Check de factsheet en/of neem contact op met Martijn Simons, Programmamanager Digitale Veiligheid. Advies: bespreek de factsheet met je CISO en je bestuurlijk portefeuillehouder ICT. Want goede ideeën verdienen navolging.

Beluister de podcast met Bart Jacobs, hoogleraar computerbeveiliging

Wil je meer weten over de achtergronden van IRMA? Luister dan de podcast van BNR-nieuwsradio met Bart Jacobs, hoogleraar computerbeveiliging en de drijvende kracht achter IRMA.

3.10.2 Smart City en de veiligheidsprofessional'

Veiligheidsprofessionals worden in toenemende mate geconfronteerd met slimme technieken om wijken, buurten en bedrijventerreinen veiliger te maken. Van de inzet van slimme camera's, sensoren en buurtapps tot het inzetten van voorspellende algoritmen bij het politiewerk; al deze technieken bieden ongekende mogelijkheden.

Toch kan je je als veiligheidsprofessional ongemakkelijk voelen bij deze materie. En dat is goed te begrijpen. Want hoe kun je nu voldoende kritisch zijn op nieuwe veiligheidsoplossingen als je voor je gevoel geen grip op de materie hebt? Laat staan dat

je dan een goede belangenafweging kunt maken? In het programma Digitale Veiligheid dat Bureau RVS in juni naar alle partners verstuurt, besteden we hier aandacht aan.
Wil je nu al aan de slag met Smart City? Doe dan mee met de online cursus 'Hoe manage je privacy in een Smart City' ' van de Erasmus universiteit Rotterdam. In de cursus die op 29 juni en 1 juli plaatsvindt van 12.00h tot 14.00h worden alle gewenste en ongewenste gevolgen van de slimme stad onder de loep genomen, met een speciale focus op sociale veiligheid. De presentaties worden na afloop op de website geplaatst.

3.10.3 Podcasttip: Achter de klik. Ga mee op reis achter de oppervlakte van het internet.

Zit je thuis en zou je in deze coronatijd toch graag een bijzondere reis maken? Ga dan de uitdaging aan en reis mee met kunstenaar, ontwerper en onderzoeker Julia Jansen. Ze neemt je mee achter de oppervlakte van het internet. Ze laat je zien wat er gebeurt aan de andere kant van het scherm wanneer je klikt. Er gaat een heel nieuw online universum voor je open. Maar hoe zit het eigenlijk met de toegangsprijs? Tijdens de reis ontmoet je verschillende mensen, waaronder Marleen Stikker, internet pionier en oprichter van Waag, een onderzoeksinstituut voor kunst, technologie en samenleving en Kathalijne Buitenweg, Tweede Kamerlid van GroenLinks én voorzitter van de tijdelijke commissie digitale toekomst. In de afleveringen wordt ook ingegaan op de gevolgen van de coronamaatregelen voor onze digitale veiligheid.
Beluister hier de podcast!

3.10.4 Nieuwe voorbeelden van datagestuurd werken

Het CCV ging op bezoek bij een aantal gemeenten en sprak met hen over hun informatiepositie en informatievoorziening. Deze koplopende gemeenten en hun wijzen van data-gedreven werken voor veiligheid worden in dit artikel op een rij gezet. Het webdossier Informatiepositie bevat 2 nieuwe voorbeelden van datagestuurd werken, namelijk de Risico Radar Ondermijning en het Dashboards voor Zicht op ondermijning. Ze bieden allebei inspiratie en handvatten om ondermijning in jouw gemeente aan te pakken. Zie hier de voorbeelden.

(Dit artikel is geschreven door Het Centrum van Criminaliteitspreventie en Veiligheid, Het CCV).