TLP:AMBER YOUR ORGANIZATION ONLY

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Maandmonitor – maart 2020

Maandelijks analyseert het NCSC de belangrijkste ontwikkelingen op het gebied van digitale veiligheid. Dit document beschrijft deze ontwikkelingen voor de maand maart 2020. Naast de feitelijke ontwikkelingen zijn in dit document ook links naar bronnen (🖱) en commentaren van het NCSC (💬) opgenomen. Zie de "NCSC Maandmonitor Bijsluiter" voor meer uitleg over dit product en de verspreidingsvoorwaarden.

COVID-19-gerelateerde digitale aanvallen

Naast dat COVID-19 ons allemaal zowel op persoonlijk als op professioneel vlak beïnvloedt en bezighoudt, heeft de pandemie ook op digitaal gebied impact. In de afgelopen weken zijn uiteenlopende digitale aanvallen waargenomen met COVID-19 thematiek waarbij verschillende modus operandi zijn toegepast. Wereldwijd worden veel COVID-19-gerelateerde phishingcampagnes waargenomen. In februari waarschuwde de Wereldgezondheidsorganisatie (WHO) al voor phishingcampagnes met COVID-19-thematiek. [🖱1] Via phishing worden verschillende ransomwarevarianten verstuurd zoals Ryuk, Netwalker en Maze. [🖱2] [🖱3] [🖱4] Ook de zorgsector werd daarmee aangevallen, ondanks dat sommige actoren achter ransomwarevarianten hadden aangegeven tijdelijk geen digitale aanvallen uit te voeren op de zorgsector. [🖱5]
In een aantal Europese landen zijn digitale aanvallen gericht op de zorgsector waargenomen. [🖱6] Daarbij kregen Franse ziekenhuizen te maken met een DDoS-aanval, [🖱7] werd ransomware 'Netwalker' gedetecteerd bij Spaanse ziekenhuizen [🖱8] en werd een Tsjechisch ziekenhuis slachtoffer van ransomware. [🖱9] De Nederlandse zorgsector lijkt vooralsnog geen slachtoffer te zijn geworden van digitale aanvallen. Ook worden COVID-19 thema's ingezet voor malafide applicaties, [🖱10] malware [🖱11] en zelfs besmette e-boeken [🖱12] om slachtoffers te maken. Daarmaast was er een phishingcampagne opgericht waarbij een 'antibacteriële betaalpas' werd aangeboden. [🖱13]
In Nederland zijn voorbeelden bekend bij (overheids)partijen van COVID-19-gerelateerde phishingaanvallen. Statelijke actoren [🖱14] spelen ook in op de huidige zorgen binnen de maatschappij en voeren aan COVID-19-gerelateerde digitale aanvallen uit. Eerder leidde een vermeende Russische digitale aanval en een desinformatiecampagne zelfs tot rellen in Oekraïne. [🖱15] Het door COVID-19 zwaargetroffen Iran heeft een applicatie ontwikkeld voor burgers om te controleren of de symptonen die ze hebben, overeenkomen met COVID-19. Iran zou de applicatie behalve voor legitieme doeleinden, mogelijk ook gebruiken om op de achtergrond meer informatie te verzamelen over gebruikers. [🖱16] In Nederland is een soortgelijke applicatie ontwikkeld door het OLVG, met het verschil dat deze applicatie enkel gebruikt wordt voor legitieme doeleinden. [🖱17]

💬 *Zowel criminelen als statelijke actoren spelen handig in op de actualiteit om hun doelen te bereiken. Actoren maken hierbij vaak gebruik van het opportunisme om aanvallen te laten slagen. Gebruik maken van grote manifestaties zoals de Olympische Spelen werden al eerder misbruikt voor digitale aanvalscampagnes bijvoorbeeld. [🖱18] Vanzelfsprekend ging en gaat veel aandacht uit naar de digitale weerbaarheid van de zorgsector. Hoewel uiteenlopende digitale aanvallen internationaal worden waargenomen, zijn bij het NCSC nog geen noemenswaardige meldingen binnengekomen. Digitale aanvallen op de Nederlandse zorgsector lijken vooralsnog geen impact te hebben gehad. Wel is de samenwerking met Z-CERT geïntensiveerd. De berichtgeving dat een Spaans ziekenhuis geraakt zou zijn door ransomware, wordt door het Spaanse CERT ontkracht. Anders dan dat de berichtgeving deed vermoeden, ging het om een potentiële ransomware-aanval en geen daadwerkelijke besmetting.*

Vrije keuze voor communicatiemiddelen brengt risico's met zich mee

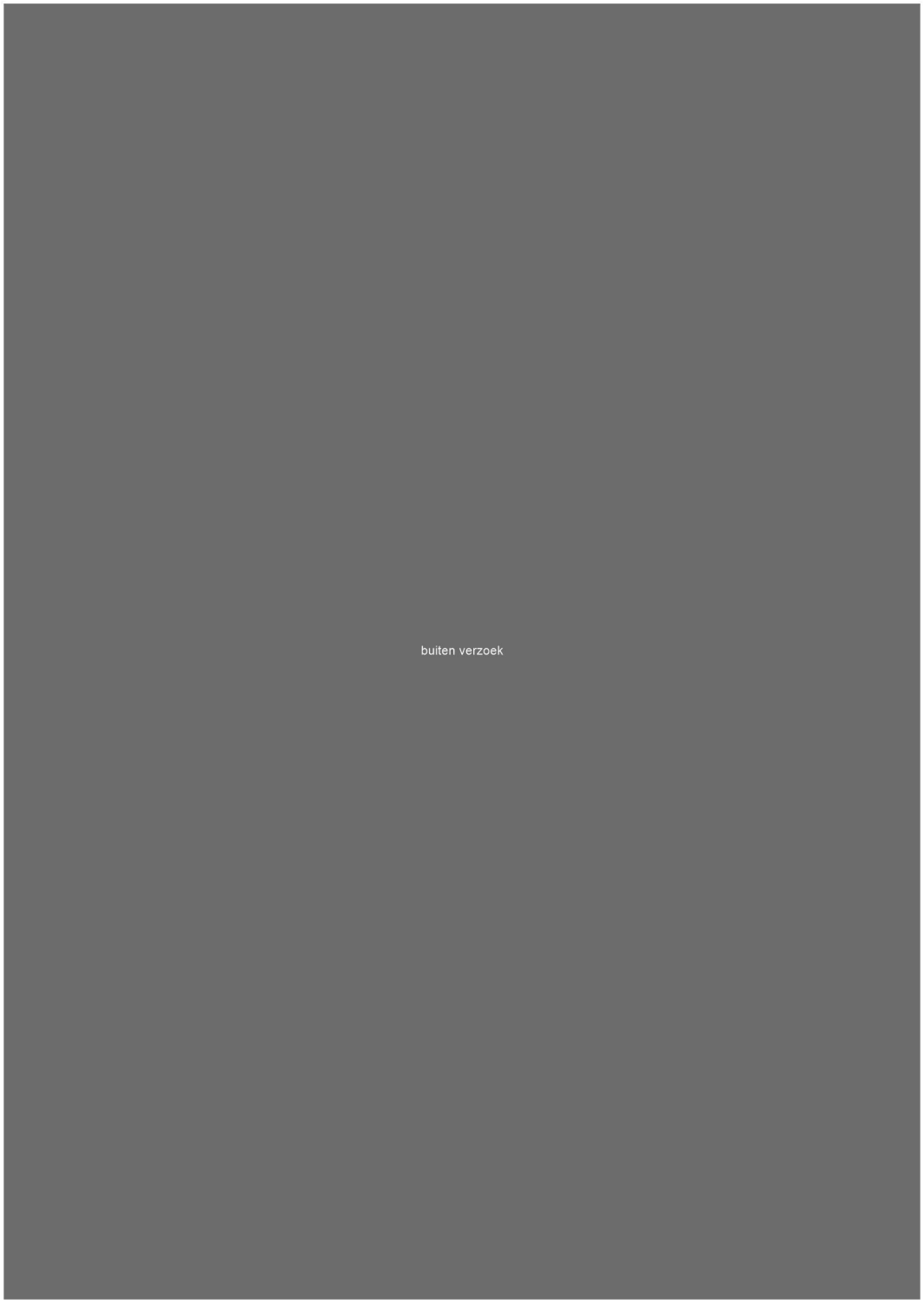
Vanwege het grote aantal werknemers dat in deze periode is gaan thuiswerken, worden op grote schaal digitale communicatiemiddelen geïnstalleerd om met elkaar in contact te blijven. Met name het videobellen is sterk toegenomen. [🖱19] Als organisaties daar geen software in de werkomgeving voor aanbieden, dan kiezen gebruikers vaak zelf voor een alternatief communicatiemiddel. Organisaties staan hierbij voor een uitdaging; de zelfgekozen platformen voldoen niet altijd aan het beveiligingsbeleid van de organisatie. De drempels die het werken op afstand opwerpen en het niet faciliteren van de benodigde middelen kunnen ook leiden tot gebruikersgemak, waarbij wordt gekozen voor een gemakkelijke manier of bekende applicatie. Bijvoorbeeld om vertrouwelijke informatie met elkaar te kunnen delen, echter gaat dit dan niet altijd op meest veilige manier of volgens de geldende interne beveiligingsrichtlijnen. Naast het in acht nemen van bepaalde veiligheidsmaatregelen tijdens het gebruik van communicatiemiddelen, geldt dit ook voor de omgang met privacywet- en regelgeving. Zo hebben de Autoriteit Persoonsgegevens en hun Europese evenknieën gewaarschuwd dat de beginselen van de privacywetgeving AVG van toepassing blijven en de coronacrisis geen excuus is om persoonsgegevens laagdrempeliger te verwerken of te verspreiden. [🖱20]

💬 *Het NCSC heeft in het verleden gezien dat organisaties worstelden met de opkomst van berichtenapps. In reactie daarop heeft het NCSC de factsheet 'Kies een berichtenapp voor uw organisatie' uitgegeven. [🖱21] Eén van de constateringen uit die factsheet is dat het tegenhouden van dergelijke diensten niet effectief is. Het aanbieden van een dienst die in de juiste configuratie aan het organisatiebeleid voldoet, is de meest effectieve manier om ervoor te zorgen dat (vertrouwelijke) informatie op de meest veilige wijze verstuurd wordt. Wanneer gebruikers dit niet aangeboden krijgen, zullen zij op zoek blijven naar*

mogelijkheden om hun doel toch te bereiken. De factsheet richt zich op berichtenapps, maar de aanbevelingen daaruit zijn evengoed van toepassing op andere diensten zoals videobellen en bestanden delen. Het NCSC heeft op de website een aantal overwegingen voor videobellen gepubliceerd. [22] Voor meer informatie over veilig thuiswerken, kunt u onze website raadplegen. [23]

buiten verzoek

buiten verzoek


buiten verzoek