TLP:WHITE

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Maandmonitor

juni 2021

Maandelijks analyseert het NCSC de belangrijkste ontwikkelingen op het gebied van digitale veiligheid. Dit document beschrijft deze ontwikkelingen voor de maand juni 2021. Naast de feitelijke ontwikkelingen zijn in dit document ook links naar de bronnen [🖱] en commentaren van het NCSC opgenomen.

Achterblijvende weerbaarheid benadrukt wederom het belang van basismaatregelen

Op 28 juni is het Cybersecuritybeeld Nederland 2021 (CSBN 2021) uitgebracht. Het CSBN biedt inzicht in de incidenten van het afgelopen jaar en de belangen die hierdoor zijn geraakt, de bron waar de dreiging van uitgaat, evenals weerbaarheid verhogende maatregelen. Het afgelopen jaar is – onder andere vanwege het noodgedwongen thuiswerken – door COVID-19 het aanvalsoppervlak groter geworden. Ook is het aantal incidenten rondom cybercrime toegenomen, waarbij ransomware, datadiefstal en denial-of-service een belangrijke rol speelden. Daarnaast hebben geopolitieke motieven hun weerslag gehad op de digitale dreiging in de vorm van economische spionage, desinformatie en (voorbereiding op) digitale sabotage. Naast deze groeiende dreiging neemt de complexiteit van digitale processen en de afhankelijkheid van ketenpartners toe, onder andere door een brede inzet van cloud computing. Terwijl digitale processen alsmaar complexer worden, blijken basismaatregelen niet of onvoldoende genomen te worden. [🖱1]

- De observatie dat basismaatregelen vaak niet genomen worden is niet nieuw. In voorgaande CSBN's wordt al aangegeven dat de security hygiëne niet overal op orde is.
- Het NCSC heeft tegelijkertijd met het CSBN een handelingsperspectief uitgebracht. In de 'Handreiking Cybersecuritymaatregelen' worden de basismaatregelen die elke organisatie zou moeten treffen nader toegelicht, inclusief de organisatorische inbedding ervan. [🖱2] Deze maatregelen helpen onder andere om aanvallen zoals in het CSBN beschreven tegen te gaan. Zo helpt versneld installeren van securityupdates misbruik van recent bekendgemaakte kwetsbaarheden tegen te gaan. Dit is belangrijk gezien deze kwetsbaarheden steeds sneller worden misbruikt door aanvallers. Daarnaast is het maken en het regelmatig testen van back-ups van belang voor een adequate bescherming tegen de groeiende ransomware dreiging. Verder maakt de interesse die uitgaat van statelijke actoren om vitale processen te saboteren het essentieel om netwerksegmentatie toe te passen. Naast deze en andere basismaatregelen benadrukt de handreiking ook het belang van een goed ingericht raamwerk voor risicomanagement, waaruit aanvullende maatregelen volgen die aansluiten bij de specifieke risico's voor een organisatie. Het CSBN 2021 sluit hierop aan en benadrukt dat risicomanagement instrumenteel is voor het verhogen van de weerbaarheid. Bestuurders zijn daarbij de eindverantwoordelijken voor een adequate omgang met digitale risico's.

Ransomware-aanval gemeente Luik past in trend aanvallen op lokale overheden

De Belgische stad Luik is op 21 juni het slachtoffer geworden van een gerichte aanval met ransomware. Hierdoor zijn gemeentesystemen deels onbereikbaar geworden en is de dienstverlening aan burgers ernstig verstoord. Onder andere de bevolkingsadministratie en bijbehorende dienstverlening (geboorten, begrafenissen en huwelijken) zijn niet beschikbaar. Verder meldt de gemeentelijke website dat het stadsarchief niet bereikbaar is. Volgens de Waalse Radio- en televisieomroep RTBF eisen de aanvallers losgeld. RTBF claimt informatie te hebben waaruit zou blijken dat de criminelen losgeld eisen en de site speculeert dat het om Ryuk-ransomware gaat. Onduidelijk is of er data gestolen is. Op dit moment zijn bepaalde diensten van de stad nog steeds niet bereikbaar. [🖱3] [🖱4]

- In het Cybersecuritybeeld 2021 (CSBN) concludeert de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) voor het eerst dat ransomware een dreiging vormt voor de nationale veiligheid. [🖱5]
- De aanval op de gemeente Luik staat niet op zichzelf. Lokale overheden worden wereldwijd regelmatig slachtoffer van een ransomware-aanval. Een studie van Barracuda Networks uit 2020 onthulde dat 44 procent van alle ransomware-aanvallen in het Verenigd Koninkrijk werd uitgevoerd richting een lokale overheid. [🖱6] Een eerdere analyse liet zien dat 45 procent van de aanvallen op lokale overheden kleinere gemeenten tot 50.000 inwoners betreft. Dit is volgens de onderzoekers geen toeval omdat kleinere gemeenten minder middelen te besteden hebben aan digitale veiligheid. Tegelijkertijd zijn kleinere gemeenten wel kapitaalkrachtig genoeg

om stevige losgeldsommen te betalen en bestaan er pressiemiddelen zoals (dreigen met) data exfiltratie. Lokale overheden beschikken vanwege de uitvoering van hun wettelijke taak over veel gevoelige data zoals persoonsgegevens van burgers en concurrentiegevoelige gegevens van bijvoorbeeld projectontwikkelaars die in de gemeente investeren. [7]

- In Nederland zijn de gemeentes Lochem en Hof van Twente geraakt door ransomware in respectievelijk 2019 en 2020. Bij de gemeente Hof van Twente werden onder meer financiële systemen en vertrouwelijke informatie over jeugdzorg, omgevingsvergunningen, werk en inkomen versleuteld. Ook de back-up systemen raakten versleuteld. De impact op de dienstverlening was groot en heeft zich nog maanden na de versleuteling in december 2020 gemanifesteerd. [8]

Aanpak cybercriminaliteit

De afgelopen maand kende veel nieuws met betrekking tot de aanpak van cybercriminaliteit. Zo presenteerde de Europese Commissie haar visie op een nieuw op te richten Joint Cyber Unit. Deze zal tot taak hebben het voorkomen en bestrijden van grote cyberincidenten en -crises. [9] Ook tijdens de G7-top stond cybersecurity op het programma. De deelnemende landen hebben in hun slotverklaring Rusland opgeroepen om werk te maken van de aanpak van diverse vormen van cybercriminaliteit met ransomware in het bijzonder. De Amerikaanse regering onderstreepte dit laatste expliciet in een afzonderlijke verklaring. [10] [11]

Er waren verschillende successen in de operationele aanpak van cybercriminaliteit te melden deze maand, naast de arrestatie van een ontwikkelaar van Trickbot, zijn enkele phishingdomeinen offline gehaald die gebruikt werden door de vermoedelijke actoren achter de SolarWinds-aanvallen. Maar ook vele andere frauduleuze websites die onder andere de handel in gestolen inloggegevens faciliteerde zijn door opsporingsinstanties onderuitgehaald. [12] [13] [14] Ook zijn in diverse landen, waaronder Nederland, servers van DoubleVPN in beslag genomen. [15]

Naast het afronden van diverse onderzoeken is het afgelopen maand ook gekomen tot een veroordeling van een lid van FIN7-groep. Deze groep staat ook bekend als Carbanak of Cobalt Group. Tevens hebben de makers van de Avaddon-ransomware aangekondigd hun activiteiten te staken en hebben de decryptiesleutels beschikbaar gesteld. [16] [17]

Nadat ook de Babuk ransomware groep eind april had aangekondigd te stoppen, is eind juni de tool gelekt waar zij hun ransomware mee maakten. Nu deze zogeheten *builder* is beschikbaar is, is het de verwachting dat andere kwaadwillenden deze malware gaan gebruiken in hun aanvallen. [18] [19]

Tot slot nam de Landelijke Eenheid van de Nederlandse politie deel aan de internationale operatie *Trojan Shield* en leverde zo een belangrijke bijdrage aan het onderscheppen en leesbaar maken van berichtenverkeer tussen criminelen. [20] [21] [22]

- De hernieuwde verve waarmee de Verenigde Staten zich richten op de aanpak van ransomware hangt samen met het bericht dat het Amerikaanse ministerie van Justitie deze onderzoeken dezelfde prioriteit geeft als de aanpak van terrorisme. [23]
- Echter bleek ook deze maand weer dat arrestaties van verdachte cybercriminelen niet altijd het beoogde effect hebben, zoals eerder dit jaar ook het geval was in het Flubot-onderzoek. Er is kort na de arrestaties van betrokkenen bij de Clop-ransomware, hier toch weer verhoogde activiteit van waargenomen. [24] [25] [26] [27]
- Een vergelijkbare situatie deed zich eerder voor met het Mariposa-botnet waar deze zelfs is gebruikt om onderzoekers die betrokken waren bij de arrestaties met een DDoS aan te vallen. [28]
- Uit analyse van het eerste tertaal door beveiligingsbedrijf ESET blijkt dat er met het ontmantelen van het Emotet-botnet een gat is geslagen in de distributienetwerken van malware. Nu een grote speler van het toneel is verdwenen, verkennen andere groepen ook distributiemethoden via malspam. [29]

Overig nieuws Nederland

Politie publiceert stappenplan cybercrime [30] ■ Russen zaten in 2017 in Nederlandse politiesystemen [31] ■ Overheid gaat specifieke dreigingsinformatie met niet-vitale bedrijven delen [32]■ 'Tientallen websites overheid voldoen niet aan veiligheidsrichtlijnen [33] ■ Kabinet wil telecomproviders verplichten om telefoonspoofing aan te pakken [34] ■ Z-CERT: Zorgen om opmars malafide javascriptfiles [35] ■ Open Brief: Overstappen naar de Cloud, bezint eer ge begint [36]