Z-Cert: ransomware blijft grootste cyberdreiging zorg

2 februari 2021

In dit allereerste Cyberdreigingsbeeld voor de zorgsector beschrijft Z-Cert de belangrijkste dreigingen voor de Nederlandse zorgsector: van DDoS-aanvallen tot ransomware en van CEO-fraude tot phishing. Zij put hierbij uit meldingen van deelnemers, informatie van (inter)nationale partners en kennisinstituten, eigen bevindingen, interviews met deskundigen en (open)bronnen research. Stichting Z-CERT is sinds 2017 het expertisecentrum op het gebied van cybersecurity in de zorg.

Cybersecurity is een kwestie van goed managen, benadrukt Z-Cert. Elke Raad van Bestuur van een zorginstelling dient kennis te hebben van relevante cyberdreigingen voor de zorgsector, zodat zij kunnen sturen op preventie, detectie en response. Daarnaast zou een Raad van Bestuur moeten aansturen op een security bewuste cultuur binnen hun organisatie.

Actualiteit van Covid-19

Cybercriminelen spelen slim in op de actualiteit van Covid-19, aldus het rapport. Zo gingen aanvallers tijdens de eerste COVID-19 piek actief op zoek externe toegang die extra opengezet werden in verband met thuiswerken. Ook speelden cybercriminelen in op de angst voor corona door phishingcampagnes met Covid-19 als thema.

De COVID-19 crisis bracht naast uitdagingen ook veel kansen, stelt Wim Hafkamp, directeur Z-CERT. Zo kwam in korte tijd het ZorgDetectieNetwerk van de grond: een digitaal netwerk dat

collectieve veiligheid biedt aan zorginstellingen die zijn aangesloten. “Een soort groepsimmuniteit dus”, aldus Hafkamp. “De dreiging voor de een is immers een waarschuwing voor de ander.”

Hafkamp stelt dat tijdens de eerste lockdown ook de samenhorigheid van de securitysector in actie te zien was. ‘Vele tientallen security-organisaties sloten zich aan bij het initiatief ‘Wij helpen ziekenhuizen’ dat ziekenhuizen in nauw overleg met Z-CERT kosteloos hielp de digitale dienstverlening veilig te houden van dreigingen. Zelfs hackers ‘beloofden’ geen ziekenhuizen aan te vallen in deze periode uit piëteit met de slachtoffers van de pandemie.’

Ransomware grootste cyberdreiging

De grootste dreiging op dit moment in de zorgsector is en blijft voorlopig ransomware. Dat bleek vorig jaar onder meer uit grote ransomware-incidenten bij een Duits en Tsjechisch ziekenhuis en een bedrijf dat betrokken is bij onderzoek naar een Covid-19 vaccin. Cybercrimegroepen zijn steeds professioneler en beter georganiseerd. De dreiging loopt deels via de leveranciersketen. Hier is het gevaar is dat één aanval bij een leverancier impact heeft op meerdere zorginstellingen.

De deelnemers van Z-CERT rapporteerden geen ransomware-aanvallen met grote impact het afgelopen jaar. Dit betekent niet dat de deelnemers geen doelwit waren. De dreiging blijkt uit het feit dat Nederlandse zorginstellingen:

- Veel gescand worden door kwaadwillenden.
- Malware ontvingen die geconfigureerd was om ransomware te downloaden.
- Op grote schaal malware (Emotet) per mail ontvingen. Emotet is vaak een voorbode van ransomware. Ook werd andere malware ontvangen die gebruikt wordt bij ransomware-aanvallen.

Preventie ransomware

Er zijn drie preventieve maatregelen die de kans om slachtoffer te worden van ransomware aanzienlijk verkleinen, aldus Z-Cert:

- *Remote Desktopprotocol*: hiermee kan er op afstand gewerkt worden. Bij veel grote ransomware-incidenten werd er misbruik gemaakt van RDP. Zorg ervoor dat RDP niet direct ontsloten is aan het internet. De kans op misbruik van buitenaf wordt zo sterk verminderd.
- *Stop of reguleer Office macro’s*: dit zijn kleine programma’s binnen Officebestanden die vaak gebruikt worden om onder andere malware te downloaden en uit te voeren. Z-CERT raadt aan om macro’s afkomstig van het internet niet toe te staan en gebruik van macro’s uit te faseren. Als een organisatie toch bepaalde macro’s nodig heeft, reguleer het gebruik daarvan dan.
- *Applicatiewhitelisting*: het tegenovergestelde van blacklisting. Geen onveilige applicaties op een ‘verboden lijst’, maar een lijst met veilige applicaties. Dit voorkomt dat niet-goedgekeurde applicaties uitgevoerd kunnen worden, zoals malware. Investeer tijd in het implementeren en onderhouden van applicatiewhitelisting. De kans dat malware die afkomstig is van het internet uitgevoerd kan worden is hiermee bijna tot nul te brengen.

Overige cyberdreigingen

Andere cyberdreigingen die in het rapport genoemd worden, zijn:

Financiële fraude: pogingen hiertoe zijn bijvoorbeeld valse facturen, CEO-fraude en malafide pogingen om rekeningnummers van medewerkers en leveranciers te veranderen. Z-Cert raadt aan medewerkers van financiële afdelingen regelmatig te attenderen op dit soort fraude en af te spreken dat te allen tijde de vastgestelde fraude-resistente procedures gevolgd worden en dat niet gezwicht wordt voor hoge druk.

DDoS-aanvallen op de zorgsector komen niet vaak voor. De drempel om een aanval uit te voeren, is echter laag. Ook concentratierisico's zijn relevant. Als veel zorginstellingen gebruik maken van hetzelfde datacenter dan kan een DDoS-aanval veel impact geven. Zorginstellingen zouden hun cyberweerbaarheid tegen DDoS-aanvallen op orde moeten hebben.

Datalekken: deze komen op diverse manieren tot stand: malware (zoals via Emotet in 2020), credential phishing, menselijke fouten en kwetsbaarheden in webapplicaties. Als een zorginstelling zich onvoldoende beveiligd heeft tegen malware en credential phishing, kan een aanvaller de gestolen data of de infrastructuur van de getroffen zorginstelling gebruiken om andere zorginstellingen aan te vallen. Deze aanvallen zijn effectiever dan normaal omdat een aanvaller dan zeer vertrouwd over komt. Het niet verlengen van domeinnamen waar in het verleden mail op binnen kwam kan leiden tot grote datalekken. Wij adviseren om domeinnamen waar mail op binnen kwam niet te laten verlopen om misbruik door derden te voorkomen.

Citrix: kwetsbaarheden in veel gebruikte thuiswerkoplossingen zoals Citrix kunnen op het moment dat ze bekend worden gemaakt het risico op cyberincidenten sectorbreed verhogen. Bij een sectorbrede impact kunnen politiek en media een rol spelen in de besluitvorming. Z-CERT adviseert om gepubliceerde best practices tijdig op te volgen en monitoring te regelen.

Cyberspionage: internationaal waarschuwden veel nationale cybersecurity-autoriteiten (zoals het NCSC in Nederland) voor verhoogde interesse door statelijke actoren in Covid-19 onderzoek. Bij Z-CERT zijn in 2020 geen cyberspionage-incidenten gemeld. Het delen van dreigingsinformatie via het ZorgDetectieNetwerk zal het zicht hierop naar verwachting doen toenemen. Investeren in de algehele cyberweerbaarheid van een organisatie heeft een positief effect op de weerbaarheid tegen statelijke actoren.

Stichting Z-CERT is het expertisecentrum op het gebied van cybersecurity in de zorg. Sinds januari 2021 voorziet het 168 zorginstellingen van actuele dreigingsinformatie. Samen met de deelnemers, het NCSC, Health I-SAC, brancheorganisaties, leveranciers, andere CERT's vormt Z-Cert een netwerk om samen cyberuitdagingen aan te pakken. Z-CERT is in 2017 opgericht op initiatief van de Nederlandse Vereniging van Ziekenhuizen (NVZ), Nederlandse Federatie van Universitair Medische Centra (NFU) en de Nederlandse ggz.

Lees hier het volledige Cyberdreigingsbeeld voor de Zorg.