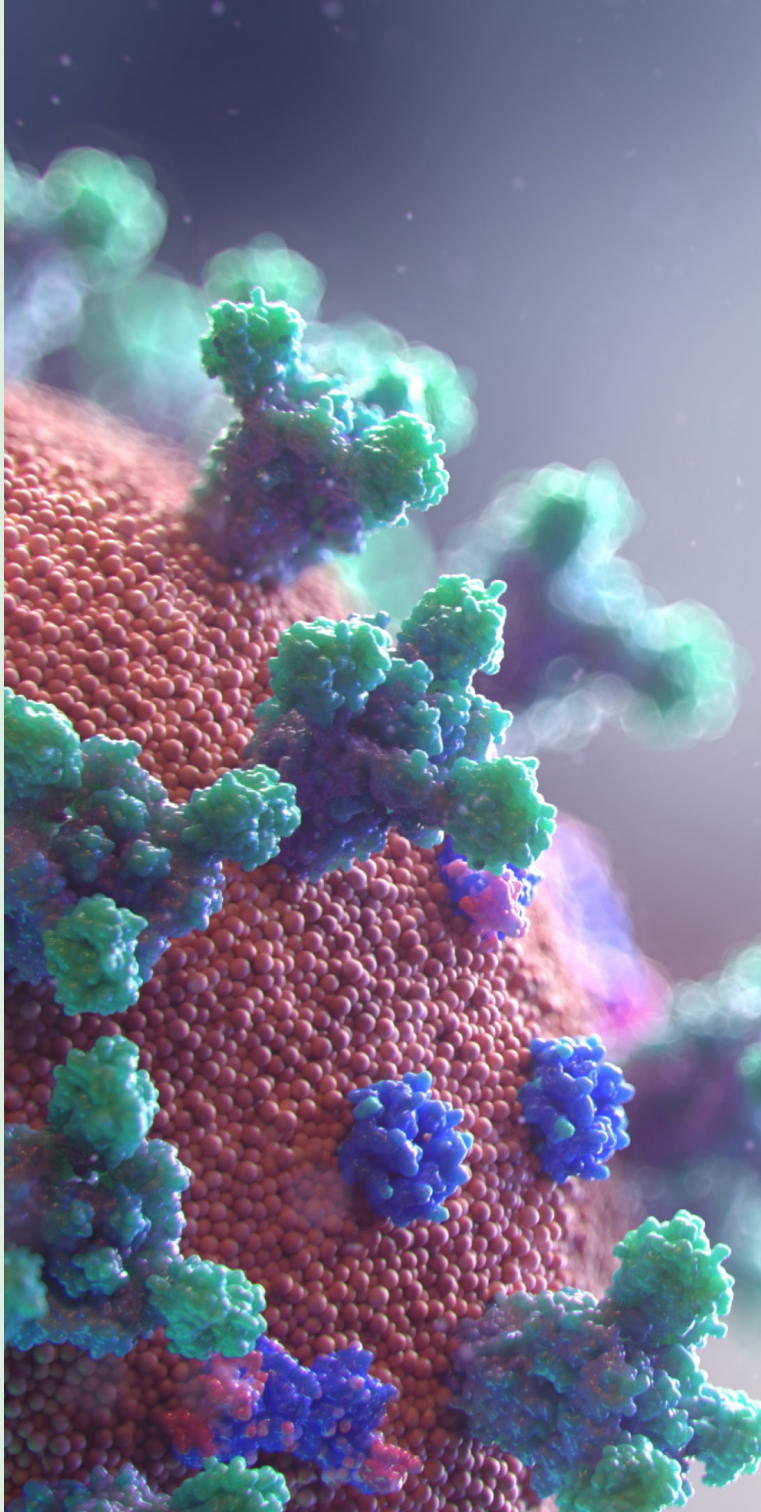
Cybersecurity Dreigingsbeeld Zorg 2020

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

CERT

De missie van Z-CERT is het versterken van de digitale veiligheid van de zorgsector



Inhoud

Colofon

Stichting Z-CERT is hét expertisecentrum op het gebied van cybersecurity in de zorg. Sinds januari 2021 voorziet Z-CERT 168 zorginstellingen van actuele dreigingsinformatie. Samen met de deelnemers, het NCSC, Health I-SAC, branche-organisaties, leveranciers, andere CERT's vormen we een netwerk om gezamenlijk uitdagingen als ransomware, phishing, datalekken of hacken 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. Z-CERT is een stichting en heeft geen winstoogmerk.

In dit allereerste Cyberdreigingsbeeld voor de Zorg beschrijven we de belangrijkste dreigingen voor de Nederlandse zorgsector. We putten hierbij uit meldingen van deelnemers, informatie van (inter)nationale partners en kennisinstituten, eigen bevindingen, interviews met deskundigen en (open)bronnen research.

Het dreigingsbeeld is opgebouwd uit columns, thema's en dreigingen. Door de hoofdstukken heen delen we onze ervaringen en tips in de hoop dat het de lezer inspireert, aanzet tot denken en het nemen van maatregelen.

Voorwoord

Voor u ligt het allereerste Cyberdreigingsbeeld voor de Zorg. Een rapport dat tot stand kwam in een jaar waarin we ons allemaal meer dan ooit bewust werden van onze eigen kwetsbaarheid. We spraken over groepsimmuniteit, vaccins, social distancing en mondkapjes. We namen maatregelen om niet alleen onszelf maar ook onze medemensen te beschermen tegen een onzichtbare dreiging.

Ook bij Z-CERT voelden we de gevolgen van het coronavirus. Dit rapport kwam grotendeels tot stand op zolderkamers, aan een keukentafel en in een geïmproviseerde werkkamer in wat tot voor kort een kinderkamer was. We pasten ons aan, zoals de mensheid zich altijd heeft aangepast. De COVID-19 crisis bracht naast uitdagingen ook veel kansen. Zo kwam in rap tempo het ZorgDetectieNetwerk van de grond. Een digitaal netwerk dat collectieve veiligheid biedt aan zorginstellingen die zijn aangesloten. Een soort groepsimmuniteit dus. De dreiging voor de een is immers een waarschuwing voor de ander.

Een crisis zoals deze vraagt om creativiteit en doorzettingsvermogen. De grootste kracht van een samenleving schuilt in weerbaarheid en een collectief vermogen om het virus aan te pakken. We hebben tijdens de eerste lockdown de samenhorigheid van de securitysector in actie gezien. 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.

> **“De grootste kracht van een samenleving schuilt in weerbaarheid en een collectief vermogen om het virus aan te pakken.”**

De coronacrisis bracht naast onzekerheid ook veel veerkracht. Thuiswerken werd het nieuwe normaal. En waar Nederland altijd al vooropliep qua digitalisering maakte dit nu een enorme vlucht. Opeens ging alles online. Van GGZ intakegesprekken tot teamvergaderingen. Maar specialisten weten dat digitalisering ook hand in hand gaat met dreiging. Dit document maakt inzichtelijk met welke dreigingen de zorgsector te maken heeft. Van DDoS aanvallen tot malware en van CEO-fraude tot phishing. We zijn trots op het eerste Cyberdreigingsbeeld voor de Zorg en hopen dat het nieuw licht werpt op deze wereld van off en online virussen.

Namens het gehele Z-CERT team wens ik u veel leesplezier en nieuwe inzichten toe.
Blijf veilig, blijf gezond.

Wim Hafkamp
directeur Z-CERT

‘Het begint met het ontdekken van de mogelijke risico’s en hierop actief monitoren.’

column

Jonathan Bouman
‘De hackende huisarts’

“U bent al verzekerd vanaf € 490,- per jaar!” **roept de folder mij toe, het is een Cyber & Data Risks verzekering die het losgeld betaalt, mocht ik als huisarts gehacked worden. Met de Universiteit van Maastricht in het achterhoofd twijfel ik, de Universiteit betaalde recent 197.000 euro losgeld aan hackers. Heb ik deze verzekering nodig? Loop ik digitaal gevaar als huisarts en zo ja, op welke manier?**

Een belangrijk onderdeel van mijn werk is het afwegen van kansen en risico’s; is de pijn op de borst een hartinfarct of gewoon maagzuurbranden? Is dat ene vlekje een gewone moedervlek of toch een gevaarlijk melanoom? Om dit goed te kunnen doen maak ik gebruik van wetenschappelijk onderbouwde richtlijnen, mijn jarenlange ervaring en gezond verstand. Tijdens het consult leg ik de opties van diagnostiek of behandeling voor aan de patiënt. Daarbij bespreken we de voor- en nadelen waarna we de beste optie kiezen. Het zogenoemde informed consent.

Deze informed consent ontbreekt echter vaak als het gaat om digitale technologie. De eerste cybersecurity informed consent van simpele videobel software, een nieuw EPD of complexe AI triagesystemen moet ik nog ontdekken. Op dat soort momenten vertrouwt de patiënt mij en mijn collega’s dat we de juiste

keuzes hebben gemaakt. Maar hoe komen wij tot die keuzes? En wat doen we als het fout gaat en alle data op straat ligt?

Het begint met het ontdekken van de mogelijke risico's en hierop actief monitoren. Waar wij huisartsen veel mensen op een gegeven moment onderwerpen aan het Cardiovasculair Risico-managment protocol (CVRM) voor de controle van o.a. bloeddruk en cholesterol, zouden wij hetzelfde moeten doen met de IT systemen en processen waarop wij en onze patiënten dagelijks vertrouwen.

In de security wereld is dit bekend als Threat Modeling. Een prachtige methode hiervoor is afgelopen zomer tijdens het DEF CON 28 congres gepresenteerd: INCLUDESNODIRT.com (zoek hun presentatie maar op via Youtube).

Een simpele methode waarbij we gestructureerd de IT systemen/processen/apparaten in de zorg kunnen beoordelen en op risico's kunnen inschatten.

Wellicht is deze methode bij uitstek toe te passen samen met de IT georienteerde huisartsen, aka CMIO's. Dit is een exercitie die met enige regelmaat moet plaatsvinden op plekken waar met patiëntdata gewerkt wordt. De huisarts blijft tenslotte eindverantwoordelijk voor de zorg die zijn team levert, dus ook voor de IT die daarbij gebruikt wordt.

"De huisarts blijft eind-verantwoordelijk voor de zorg die zijn team levert, dus ook voor de IT die daarbij gebruikt wordt."

Na de Threat Modeling zouden we de ontdekte problemen moeten oplossen. Precies daar zit in de eerstelijns zorg de grootste uitdaging. Hoe doen we dit met de al bomvolle agenda's? Hoe krijgen we de juiste mensen bij elkaar die dit kunnen beoordelen en oplossen? Hoe bekostigen we dit? Wat doen we als het echt helemaal fout gaat en de hackers op de stoep staan, is er een draaiboek?

Het liefst zie ik een oplossing waarbij we kennis delen en krachten bundelen (Z-Cert & ZorgDetectieNetwerk), van elkaars fouten leren (onderwijs, volledige transparantie, coordinated vulnerability disclosure) en dat bestuurders in de zorg geld en formatie vrij maken voor structurele aanpak van dit probleem.

Voor nu hou ik de € 490 euro in mijn zak, een losgeldgarantie maakt de zorg niet veiliger.

dreiging

DDoS

Over het algemeen heeft de zorgsector veel minder DDoS aanvallen gezien in 2020 dan de financiële sector (Verizon, 2020). De financiële sector heeft last van cybercrimegroepen die DDoS-aanvallen gebruiken als afpersingsmiddel. Wie niet betaalt, kan een DDoS-aanval verwachten. Voor bedrijven die online diensten aanbieden, is dit een zeer vervelend scenario. Omdat veel vermogende organisaties die vaak doelwit zijn geweest, effectiever zijn geworden in het mitigeren van dit soort aanvallen, verschuift de aandacht van cybercriminelen deels naar organisaties die kwetsbaarder zijn (Europol, 2020). Dit zijn vaak kleinere organisaties, met een minder volwassen securityniveau.

Alhoewel de dreiging richting de zorgsector meevalt, is het zorgelijk dat deze tactiek actief gebruikt wordt door cybercrimegroepen. Het is zeer makkelijk om voor weinig geld een DDoS-aanval te kopen op het darkweb. Aanbieders van DDoS-aanvallen adverteren steeds vaker op reguliere sociale media (ENISA, 2020). De technische en organisatorische drempel om zo'n aanval uit te voeren is laag en we weten vanuit de "ransomwaresector" dat cybercriminelen niet terugdeinzen om zorginstellingen aan te vallen.

Nederland

In september melde het NCSC dat er sinds augustus 2020 een toename wordt waargenomen in intensiteit en aantal DDoS-aanvallen (NCSC NL, 2020). Internet serviceproviders (ISP's) waren regelmatig het doelwit van DDoS-aanvallen. De aanvallen op ISP's werden ook door enkele deelnemers van Z-CERT gevoeld. Ook hier speelt de ketenafhankelijkheid. Als een DDoS het datacenter raakt waar belangrijke data staan of de internet-provider waarvan een ziekenhuis afhankelijk is, heeft dat impact op de zorginstellingen en op onderlinge samenwerking.

Advies

We raden zorginstellingen aan om in het "Business Continuity Plan" aandacht te besteden aan DDoS-dreiging en op basis van een uitgebreide risk assessment de weerbaarheid op orde te brengen. Vaak zijn er afspraken nodig met bijvoorbeeld de internetprovider en specialistische bedrijven. Voor meer informatie voor een "DDoS mitigation plan" zie het whitepaper van CERT-EU (CERT-EU, 2017).

“ Het is zeer makkelijk om voor weinig geld een DDoS-aanval te kopen op het darkweb. Aanbieders van DDoS-aanvallen adverteren steeds vaker op reguliere sociale media. ”

thema

COVID-19

2020 was onmiskenbaar het jaar van Corona. COVID-19 heeft niet alleen haar weerslag gehad op het sociale verkeer, maar ook op het digitale. Cybercriminelen hebben hun werkwijze aangepast en maakten misbruik van de pandemie. Zo zag Z-CERT een toename van phishingcampagnes; een aanval die is gericht op het buitmaken van inloggegevens van systemen of andere gevoelige informatie. Actoren achter de phishingmails misbruikten de pandemie om ontvangers over te halen te klikken op een malafide link. De phishingmails hadden onderwerpen als; vaccins, medisch onderzoek, beschermingsmiddelen zoals gezichtsmaskers en facturen gerelateerd aan COVID-19. De effectiviteit van deze campagnes is in de Nederlandse zorgsector gelukkig beperkt gebleven.

Thuiswerken

Cybercriminelen zochten actief naar oplossingen voor externe toegang nadat mensen steeds meer gingen thuiswerken. Criminelen probeerden vervolgens middels het raden van wachtwoorden in te loggen op de systemen. Zorginstellingen hebben verhoogde aandacht gekregen van verschillende actoren vanwege de rol die zij spelen in de pandemie. Deze aandacht heeft de intensivering van samenwerking tussen cybersecuritybedrijven, het Nationaal Cyber Security Centrum en Z-CERT versneld. Dit heeft, onder andere geleid tot de creatie van het ZorgDetectieNetwerk in maart 2020 en de oprichting van Wij Helpen Ziekenhuizen.

De verhoogde risico's voor de zorgsector hebben tientallen cybersecuritybedrijven ertoe aangezet om, in het nationaal belang, de zorgsector tijdelijk kosteloos te ondersteunen bij incidenten en informatiebeveiligingsvraagstukken. **Wij Helpen Ziekenhuizen** heeft tijdens haar actieve periode verschillende keren zorginstellingen kunnen helpen. Z-CERT heeft hierbij gefungeerd als een filter.

Daarnaast hebben verschillende cybersecuritybedrijven aangeboden om de zorgsector, middels Z-CERT, te voorzien van dreigingsinformatie. Z-CERT heeft de aangeboden informatie gefilterd en relevante dreigingsinformatie geselecteerd.

dreiging

Financiële fraude

Zorginstellingen zagen in 2020 ook pogingen tot financiële fraude. Vaak kwam dezelfde poging bij meerdere zorginstellingen terug. Er zijn ruwweg drie typen fraude te onderscheiden waar de zorg-sector het afgelopen jaar melding van maakte:

1. CEO-fraude
Bij CEO-fraude verstuurt een aanvaller een mail namens de CEO waarin gevraagd wordt om geld over te maken. De fraudeur probeert in de mail druk uit te oefenen op de ontvanger. Denk aan: 'Ik zit in een vergadering. Ik wil dat je met spoed een taak uitvoert en reageert op mijn mail.' De fraudeur probeert vervolgens een mailwisseling op te zetten. Wat opvalt is dat de mails in foutloos Nederlands geschreven zijn. Het gaat dus mogelijk om Nederlandse criminelen.

2. Valse facturen
Een bekende manier van frauderen is het versturen van valse facturen. Daarbij worden ook bekende medische leveranciers nagebootst en heeft de aanvaller kennis van de context van zorginstellingen.

3. Frauduleuze verzoeken om rekeningnummers te wijzigen
Zorginstellingen krijgen verzoeken om het rekeningnummer van een medewerker of leverancier te wijzigen in een malafide rekeningnummer.

Advies
We raden aan medewerkers van financiële-afdeling periodiek te attenderen op deze typen fraude. Het is belangrijk dat betrokken medewerkers te allen tijde de intern afgesproken autorisatie procedures volgen voor het accorderen van facturen, betalingen en het wijzigen van rekeningen.
Hoge druk om het anders te doen (van bovenaf), moeten ze kunnen weerstaan. De interne autorisatie procedures en processen zijn over het algemeen zo opgezet dat fraude voorkomen wordt. De financiële afdeling moet niet reageren op mails/whats app/sms'jes/telefoontjes die binnenkomen over betalingen of andere wijzigingen, buiten de reguliere routes om en bij twijfel contact opnemen met hun managers en securityspecialisten.

Impersonatie
Bij impersonatie doet iemand zich voor als een bepaalde zorginstelling met als doel fraude te plegen. De zogenaamde zorginstelling stuurt dan een rekening naar een patiënt of een familielid van een patiënt. Ook worden soms ziekenhuizen nagebootst met nepwervingscampagne voor buitenlands personeel. Verpleegkundigen denken te solliciteren bij een Nederlands ziekenhuis, maar in werkelijkheid 'solliciteren' ze bij de fraudeur en maken ze geld over voor een visum dat ze nooit ontvangen. Soms worden zelfs hele websites van ziekenhuizen nagebootst. Zorginstellingen hebben hier niet direct financiële hinder van, maar moeten de casussen wel afhandelen.


KD-FINE®
Einmalinjektionskanüle
Hypodermic needle
Aiguille à usage unique
Ago ipodermica de uso único
Jednorázová injekční jehla
Jalowa igła iniekcyjna
Ac de unica folosinta
إبرة تحت الجلد
Engangs kanyle
Kanyle, subkutan, engangs
Kertakäyttöinen injektioneula
Injektionsnål för engångsbruk, subcutan
GREENFINE - JALOWA IGŁA INIEKCYJNA
REF:GT120X40
1.20 mm x 40 mm/18G
REF
900284

dreiging

Ransomware

Z-CERT ziet doelgerichte ransomware-aanvallen door cybercriminelen momenteel als de grootste dreiging voor de zorgsector. Ransomware tast onder meer de beschikbaarheid van data, operationele processen en patiëntveiligheid aan. Uit een internationaal onderzoek naar ransomware-incidenten blijkt dat volledig herstel van een organisatie van 100 tot 1000 medewerkers gemiddeld rond de 428.000 euro kost (Sophos, 2020). Ook komt het steeds vaker voor dat er gedreigd wordt met het lekken of veilen van data als een organisatie niet wil betalen.

Dreigingsbeeld ransomware

Voor de zorgsector is de dreiging voor aanvallen met ransomware hoog en permanent aanwezig. Dit jaar werd dit zichtbaar door grote ransomware-incidenten bij een Duits en Tsjechisch ziekenhuis en een bedrijf dat betrokken is bij onderzoek naar een COVID-19 vaccin. Dit waren geen Nederlandse zorginstellingen. Voor veel cybercriminelen maakt het niet veel uit of een ziekenhuis in Duitsland of Nederland staat, maar meer of ze een 'gaatje' kunnen vinden (Microsoft, 2020).

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
- Nederlandse zorginstellingen malware ontvingen die geconfigureerd was om ransomware te downloaden
- Nederlandse zorginstellingen 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.

> **"De geobserveerde professionalisering suggereert dat cybercriminelen werken aan het vergroten van hun aanvalscapaciteit en efficiëntie."**

Ook het Europese beeld laat zien dat dreiging van ransomware onverminderd hoog is (Europol, 2020). De professionalisering van de 'ransomwaresector' zet door. We zagen dit jaar samenwerkingsverbanden ontstaan tussen cybercrimegroepen die onderling kennis en infrastructuur uitwisselen en die actief nieuwe medewerkers rekruteren. Het idee van de 'zolderkamer hacker' is verouderd. Deze ransomwaregroepen doen meer denken aan goed georganiseerde gespecialiseerde IT-bedrijven die voortdurend innoveren. De geobserveerde professionalisering suggereert dat cybercriminelen werken aan het vergroten van hun aanvalscapaciteit en efficiëntie.

Dreiging vanuit leveranciers

Uit een onderzoek bleek dat 9% van de onderzochte ransomware-incidenten

veroorzaakt werd door gecompromitteerde leveranciers (Sophos, 2020). Er is een risico dat een digitaal incident bij een veel gebruikte leverancier sectorbrede impact kan hebben. Voorbeeld daarvan is het ransomware-incident bij Fresenius (Krebs, 2020). Fresenius levert dialyseapparatuur aan onder meer Nederlandse ziekenhuizen. Om onderhoud te plegen aan de geleverde apparatuur hebben de techneuten van Fresenius toegang tot de netwerken van vele zorgorganisaties in Nederland.

In reactie op de ransomwarebesmetting bij Fresenius adviseerde Z-CERT om de VPN-connecties dicht te zetten en wachtwoorden te resetten. Uiteindelijk heeft dit niet geleid tot incidenten bij zorginstellingen in Nederland.

Er zijn meerdere voorbeelden uit het buitenland bekend waarbij leveranciers van EPD's geraakt werden waardoor een groot aantal zorginstellingen gedurende langere tijd niet bij hun patiëntdata konden (Krebs, 2019, 2019a). Ook in Nederland kennen we een voorbeeld. Z-CERT beschouwt deze ketenafhankelijkheid als een concentratierisico.

Het is belangrijk dat zorginstellingen hun leveranciers niet blindelings vertrouwen maar eisen stellen aan hun informatiebeveiliging. Zo zou de leverancier periodiek moeten aantonen dat het de informatiebeveiliging op orde heeft, voldoet aan de geldende wet- en regelgeving en, wanneer van toepassing, in het bezit is van certificeringen zoals bijvoorbeeld de NEN 7510. Ook zouden leveranciers, wanneer deze bijvoorbeeld persoonsgegevens van zorginstellingen verwerken, periodiek pentests en vulnerability scans moeten uitvoeren. Deze afspraken moeten de partijen vastleggen in een verwerkersovereenkomst (AP, 2019).

> **“Het is belangrijk dat zorginstellingen hun leveranciers niet blindelings vertrouwen maar eisen stellen aan hun informatiebeveiliging.”**

We adviseren zorginstellingen om de IT-omgeving in te richten volgens het 'zero trust' principe (NCSC UK, 2019) . Hierbij houd je er van tevoren al rekening mee dat je leverancier gehackt is en ontwerp je je processen en IT-omgeving op zo'n manier dat een aanvaller snel opgemerkt zal worden en dat hij weinig schade aan kan richten.

De cyberweerbaarheid verhogen van de sector

Z-CERT verwacht dat met de invoering van drie maatregelen de cyberweerbaarheid aanzienlijk wordt verhoogd, zie het kader 'Drie gouden tips tegen ransomware'. Het mooie van deze maatregelen is dat met relatief weinig geld, de cyberweerbaarheid aanzienlijk verhoogd kan worden.

Drie gouden tips tegen ransomware

Remote desktopprotocol

Met het Remote Desktopprotocol (RDP) 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 verkleint u hiermee aanzienlijk.

Stop of reguleer Office macro's

Macro's 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 uw organisatie toch bepaalde macro's nodig heeft, reguleer het gebruik daarvan dan.

Applicatiewhitelisting

Applicatiewhitelisting is het tegenovergestelde van blacklisting. In plaats van onveilige applicaties op een 'verboden lijst' te zetten, maak je 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.

Duitsland, September 2020. Ziekenhuis: Uniklinik Düsseldorf
Het Academisch ziekenhuis van Düsseldorf (UKD) maakte op 10 september 2020 bekend te zijn getroffen door ransomware. Het ziekenhuis kan een tijd lang geen nieuwe patiënten opnemen en afspraken worden afgezegd. De spoedeisende hulp sluit de deuren om pas dertien dagen later weer open te gaan. Het UKD was gecompromitteerd via de Citrix kwetsbaarheid (CVE-2019-19781) ondanks een onderzoek naar mogelijke compromitatie.
Daarnaast werd er in de zomer nog een pentest uitgevoerd. Deze ransomware-aanval leek in eerste instantie bij te hebben gedragen aan het overlijden van een patiënt. Door het sluiten van de SEH moest een ambulance met deze patiënt uitwijken naar een ander ziekenhuis. Hoewel er medisch gezien niet is uit te sluiten dat het invloed heeft gehad (Wired, 2020), concludeerde men dat de patiënt hoe dan ook zou zijn overleden. Er zijn genoeg scenario's denkbaar waarbij uitval van systemen door ransomware kan leiden tot overlijden. Deze casus geldt als een ernstige waarschuwing. Saillant detail: de aanvallers waren in de veronderstelling dat ze een universiteit hadden gehackt. Pas na bemiddeling door de politie leverden ze de encryptiesleutel aan. De daders zijn tot op heden nog niet gepakt.

Frankrijk, November 2019. Ziekenhuis: Rouen University Hospital Center (Le Monde, 2019)
Zesduizend computers van het ziekenhuis raakten geïnfecteerd waardoor het zorgpersoneel moest teruggrijpen op pen en papier. Sommige afdelingen konden niet bij benodigde informatiesystemen zodat verpleegkundigen niet wisten welke medicijnen ze moeten toedienen. Artsen moesten opnieuw vaststellen welke medicijnen een patiënt nodig had.

Meer over ransomware

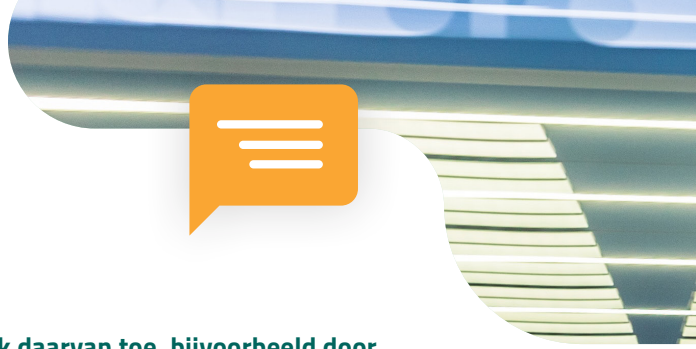
Bij aanvallen met ransomware wordt belangrijke data van een organisatie versleuteld. Een cybercrimineel dringt binnen op een netwerk en maakt de belangrijke data (waaronder vaak ook de back-ups) onleesbaar. Cybercriminelen vragen hoge prijzen voor deze de digitale sleutel die nodig is om versleutelde data weer toegankelijk te maken. De losgeldprijs verschilt per organisatie. Cybercriminelen doen soms eerst onderzoek naar de jaarcijfers en proberen op basis daarvan een reële schatting te maken wat een bedrijf kan betalen.

Experts in cybersecurity zijn niet eensgezind als het gaat om de aanpak van ransomware. Sommige bedrijven verzekeren zichzelf tegen digitale aanvallen. De verzekeraar betaalt in dat geval het 'losgeld'. Maar je hebt daarmee geen zekerheid dat je je bestanden weer volledig terugkrijgt. Daarnaast menen securityonderzoekers dat verzekeraars met deze methode het verdienmodel van de cybercriminelen in stand houden.

Indien betalen geen optie is, is het terugzetten van een goede recente back-up de enige methode. Maar het herstellen van de geraakte infrastructuur is duur en de disruptie van belangrijke processen levert vertraging van de normale workflow en dus verliezen op. Deze kosten kunnen soms net zo hoog zijn als de losprijssom.

> **“Een cybercrimineel dringt binnen op een netwerk en maakt de belangrijke data onleesbaar.”**

In sommige gevallen is de software van de cybercriminelen gekraakt en is het mogelijk om de sleutel te krijgen zonder geld te betalen aan de cybercriminelen. Ook kan het zijn dat de cybercrimegroep gestopt is en de sleutels heeft vrijgegeven of dat deze door de politie in beslag zijn genomen. Het project “No more ransom” stelt software ter beschikking om de versleutelde bestanden te ontsleutelen en is mede opgericht op initiatief van Team High Tech Crime van de Nederlandse politie.



thema

Citrix

Op het moment dat kwetsbaarheden publiek worden gemaakt, neemt het risico op misbruik daarvan toe, bijvoorbeeld door cybercriminelen en statelijke actoren. Vooral kwetsbaarheden in oplossingen voor het werken op afstand zijn populair omdat een aanvaller zichzelf toegang kan geven tot het interne netwerk van een organisatie en tot gevoelige data. Dit is een risico voor de sector, met name als het een veelgebruikt product of dienst betreft. Daarnaast kunnen kwetsbaarheden met een sectorbrede impact ook politieke en media-aandacht krijgen, wat mee kan gaan spelen in de besluitvorming.

Op 17 december 2019 werden kwetsbaarheden in de Citrix-producten Citrix ADC (voorheen Netscaler) en Citrix Gateway bekend gemaakt. Deze producten maken thuiswerken voor personeel van zorginstellingen mogelijk. In januari 2020 werd er software publiek gemaakt om de kwetsbaarheid te kunnen misbruiken. Cybercriminelen en statelijke actoren hadden nu een middel in handen om actief aan te vallen. Door veel internationale partijen werd actief misbruik waargenomen. Patchen kon pas meer dan een maand na de bekendmaking van de kwetsbaarheid. Tot die tijd konden alleen bepaalde maatregelen genomen worden om misbruik te voorkomen.

Op basis van dreigingsinformatie heeft Z-CERT, in overleg met het NCSC en het ministerie van VWS, op 17 januari 2020 dringend geadviseerd om Citrix-systemen uit te zetten. Dit had grote impact. Veel ziekenhuizen gaven gehoor aan deze oproep. Hierdoor was thuiswerken in veel gevallen niet meer mogelijk, en kon bijvoorbeeld (medisch) personeel niet meer vanuit huis het EPD raadplegen. Voor verschillende ziekenhuizen heeft dit ertoe geleid dat personeel op de campus moest verblijven. Ook bleken ziekenhuizen die geen gebruik maakten van Citrix toch last te hebben, omdat leveranciers of ketenpartners Citrix gebruikten. Aandachtspunt is om de hele keten in beeld te hebben en op verschillende scenario's voorbereid te zijn. Een soortgelijk advies wordt gegeven in het OVV-rapport 'Patiëntveiligheid bij ICT-uitval in ziekenhuizen'(Februari 2020) .

> **“Aandachtspunt is om de hele keten in beeld te hebben en op verschillende scenario's voorbereid te zijn.”**

Ziekenhuizen hebben een eigen risicoafweging gemaakt. Verschillende ziekenhuizen hebben Citrix niet uitgezet en hebben niet geëscaleerd, terwijl andere ziekenhuizen dat wel hebben gedaan. Vaak werd de media en politieke-aandacht als escalerende factor genoemd. Deze dynamiek veroorzaakte bestuurlijke druk binnen organisaties, waarbij een aantal organisaties heeft besloten om Citrix uit voorzorg uit te zetten.

Advies

Er zijn voorbeelden van zorginstellingen bekend die gehackt zijn omdat zij niet de best practices van Citrix wat betreft security toepasten (Citrix, 2020). Een organisatie doet er goed aan om voor Citrix niet alleen preventiemaatregelen toe te passen maar ook de monitoring goed in te regelen. In situaties met verhoogd risico is zichtbaarheid op wat er in uw IT-omgeving gebeurt belangrijk om het risico te kunnen inschatten en aanvallers op te kunnen merken. Ga ook hier uit van het “zero trust” principe. Voor meer informatie over een architectuur die uitgaat van het zero-trust principe, verwijzen we u naar het artikel van het NCSC UK (NCSC UK, 2019).

dreiging

Datalekken

De zorgsector heeft regelmatig te maken met datalekken. Deze datalekken komen voornamelijk door malware-infecties, menselijke fouten, phishing, en soms door kwetsbaarheden in webapplicaties. Persoonsgegevens zijn veelal bijvangst bij opportunistische aanvallen, echter sommige buitgemaakte data wordt door cybercriminelen verhandeld op het darkweb. Andere datalekken kwamen aan het licht door onderzoek van journalisten.

Credential phishing

Bij dit type aanval worden gebruikersnaam en wachtwoord gestolen van een slachtoffer door ze over te halen op een nepsite in te loggen. De cybercrimineel onderschept de logingegevens en gebruikt deze om in te loggen op de echte website (bijvoorbeeld de webmail van het slachtoffer) en steelt vervolgens alle mail en data die daar te vinden is. Dit soort incidenten zagen we in 2020 minder dan in 2019, mogelijk omdat veel zorginstellingen overgestapt zijn op multi-factor authenticatie. Een must vandaag de dag. Hierbij zie je dat een enkele maatregel sectorbreed tot direct meer veiligheid leidt. Een organisatie die dit nog niet geïmplementeerd heeft, introduceert een risico voor zijn relaties. Bij de meeste succesvolle phishingincidenten gebruikt de kwaadwillende namelijk de mailinfrastructuur van het slachtoffer om zijn malafide mailcampagne voort te zetten. Omdat de aanvaller mailt vanuit een vertrouwde zorginstelling, is de kans op 'succes' bij een andere zorginstelling, groter. De kwaadwillende maakt hier misbruik van de vertrouwensband binnen de sector.

Malware

In 2020 verspreiden cybercriminelen op grote schaal de malware Emotet. Deze malware kwam bij meerdere Nederlandse zorginstellingen binnen. Emotet kan door een aanvaller voor vele doeleinden gebruikt worden. Dit jaar zagen we dat Emotet direct tot datalekken leidde omdat mail van het slachtoffer gestolen werd. Diegene met wie het slachtoffer eerder een mailwisseling had, kreeg vervolgens ook een mail met de Emotet malware en met de vertrouwde inhoud uit eerdere mailconversaties. Dat maakte de kans van slagen van deze malware groot. Wie wantrouwt immers een mailtje van een bekende? We zagen daardoor in korte tijd meerdere malware-incidenten en datalekken bij verschillende zorginstellingen maar ook zorgsector gerelateerde instellingen.
Als zorginstellingen applicatiewhitelisting toepassen en macro's afkomstig van het internet uitschakelen, zal het aantal incidenten naar verwachting flink omlaag gaan. Binnen de zorg wordt nog met enige regelmaat gebruikgemaakt van officebestanden met macro's.

Domeinnamen

Een naamswijziging van een zorgorganisatie of fusie gaat vaak gepaard met een nieuwe website en bijbehorende domeinnaam. De nieuwe domeinnaam is geregistreerd, er komt mail op binnen en mensen weten je online te vinden. Maar wat doe je met die oude domeinnaam? Het afsluiten van de domeinnaam is een voetnoot bij een fusie maar

kan ernstige gevolgen hebben, zoals het lekken van gevoelige gegevens, als dit niet goed wordt afgehandeld. Dat blijkt uit onderzoek van RTL nieuws (RTLNieuws, 2020).

Een journalist van RTL bemachtigde in het najaar van 2020 een verouderde domeinnaam van Kenter Jeugdhulp. Hierop kwam nog altijd mail binnen. Via deze mail kreeg de journalist toegang tot gevoelige data en zelfs tot de database van VECOZO. VECOZO is een samenwerkingsverband van zorgverzekeraars en maakt veilige digitale communicatie mogelijk tussen de zorgverzekeraars, zorgkantoren en zorgverleners.

Een domeinnaam is het adres van je website; zoals bijvoorbeeld www.zorginstelling.nl. Iedereen kan deze naam, mits deze niet al door iemand anders is geregistreerd, registreren. Je betaalt hiervoor vaak een vast bedrag per jaar. Als je niet blijft betalen, zal het domein verlopen en ben je niet langer de eigenaar van het domein. De naam komt weer op de markt en is vrij beschikbaar voor wie het wil.
Een verlopen domeinnaam kan dus vervelende gevolgen hebben. En dit hoeft niet alleen een domeinnaam te zijn die uit het oog wordt verloren bij fusies. Er worden binnen organisaties domeinnamen voor allerlei zaken aangevraagd. Bv voor: informatieweken, interne afdelingen, feestjes, jaarverslagen etc. Op sommigen van deze domeinnamen kan gevoelige mail binnenkomen. Voor aanbevelingen verwijzen we naar het kader 'advies' op deze pagina.

Webapplicaties/websites
Digitalisering gaat gestaag door in de zorg, dit heeft geleid tot de ontwikkeling van een breed assortiment aan webapplicaties voor allerlei zorgprocessen. Dit brengt ook afhankelijkheden met zich mee. Als een webapplicatie niet beschikbaar is door een cyberincident dan kan dit impact hebben op zorgprocessen binnen een organisatie.

Advies
- Beheer en administreer domeinnamen centraal binnen de organisatie.
- Definieer een proces voor het verlengen van de domeinnamen. Maak de organisatie onafhankelijk van herinneringsmails van de registratiepartij.
- Laat domeinnamen waar (ooit) mail op binnen is gekomen nooit verlopen.
- Definieer een procedure voor het vrijgeven van domeinnamen, waarbij onderzocht wordt of dit kan leiden tot een datalek. Hanteer daarbij een afkoelingsperiode van tenminste 2 jaar.

Als het een webapplicatie van een dienstverlener betreft, dan kan het impact hebben op meerdere zorginstellingen.

Soms ontwikkelt een zorginstelling zelf een webapplicatie of laten ze dit doen door een derde partij. Dit brengt risico's met zich mee wanneer de maker van de applicatie niet of te weinig rekening houdt met digitale beveiliging. Hierdoor is de applicatie kwetsbaar voor soms zeer basale digitale aanvallen zoals SQL-injecties.

Z-CERT adviseert makers van zorggerelateerde webapplicaties om adequate en actuele beveiligingsrichtlijnen te hanteren. De NCSC factsheet "ICT-beveiligingsrichtlijnen voor webapplicaties (NCSC, 2019) somt de belangrijkste regels op. Daarnaast is het verstandig om webapplicaties een security audit te laten ondergaan voordat ze in productie worden genomen. Herhaal dit met enige regelmaat omdat updates en andere veranderingen kunnen leiden tot kwetsbaarheden in de webapplicatie zonder dat men het in de gaten heeft.

“ Het is een misverstand dat statelijke actoren alleen zeer geavanceerde technieken gebruiken, waar de zorg zich moeilijk tegen kan beschermen. ”

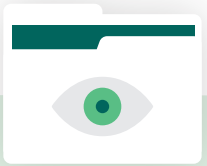
dreiging

Cyberspionage

Vanuit de hoek van statelijke actoren viel het volgende internationaal op:

- Statelijke actoren hadden veel interesse in onderzoeksinstituten en bedrijven die zich richten op de ontwikkeling van een vaccin tegen COVID-19 (NCSC UK, 2020)
- Bepaalde kwetsbaarheden (bijvoorbeeld in VPN-oplossingen en Citrix) werden regelmatig misbruikt door statelijke actoren (CISA & FBI, 2020)
- De FBI waarschuwde voor malware die via de leveranciersketen ziekenhuizen infecteert (FBI, 2020).

Er zijn statelijke actoren die de zorgsector als doelwit hebben. Daarbij hebben ze laten zien geïnteresseerd te zijn in kankeronderzoek (FireEye, 2020), COVID-19 onderzoek en kennis over 'disease control' (CERT-EU, 2019). Daarnaast is data gestolen die het hele reilen en zeilen in een farmaceutisch bedrijf blootlegt. Motieven voor de spionage zijn bijvoorbeeld het bevorderen van de volksgezondheid van het eigen land, maar kunnen ook economisch van aard zijn. Buitgemaakte kennis kan voordeel opleveren voor de eigen farmaceutische industrie of andere organisaties die aan research en development doen.



De interesse van statelijke actoren heeft echter niet geleid tot cyberspionage incidenten die bij Z-CERT gemeld zijn. Kanttekening hierbij is dat het vaak lastig is om een actor achter een aanval te duiden. Criminelen gebruiken namelijk vaak dezelfde technieken als statelijke actoren en vice versa. (ACSC, 2020). Ook staat onderzoeksdata van lopende klinische onderzoeken meestal niet bij ziekenhuizen zelf maar bij dienstverleners die gespecialiseerd zijn in diensten voor klinisch onderzoek. Deze partijen zijn mogelijk nog interessanter voor statelijke actoren als het gaat om diefstal van onderzoeksdata. Zorginstellingen moeten zich hier bewust van zijn. De verwachting bij Z-CERT is dat met het ZorgDetectieNetwerk, het zicht op de activiteit van statelijke actoren gaat toenemen.

> **“De verwachting bij Z-CERT is dat het zicht op de activiteit van statelijke actoren gaat toenemen.”**

Cyberweerbaarheid tegen statelijke actoren

Het is een misverstand dat statelijke actoren alleen zeer geavanceerde technieken gebruiken, waar de zorg zich moeilijk tegen kan beschermen. Statelijke actoren hebben wel meer in huis op dat gebied, maar kiezen regelmatig voor de makkelijke weg. Vaak misbruiken zij bekende kwetsbaarheden waar al updates voor bestaan (FireEye, 2020) of gebruiken basale phishing technieken en standaardmethoden om wachtwoorden te raden of te stelen (ACSC, 2020). Als de zorg de cyberweerbaarheid in zijn algemeenheid goed op orde brengt zal ook de weerbaarheid tegen statelijke actoren verbeteren.

Samenvatting

Covid-19

Cybercriminelen spelen slim in op de actualiteit. 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.

Financiële fraude

Zorginstellingen ontvangen pogingen tot financiële fraude, door bijvoorbeeld valse facturen, CEO-fraude en malafide pogingen om rekeningnummers van medewerkers en leveranciers te veranderen. Wij raden 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

DDoS-aanvallen op de zorgsector komen niet vaak voor. Echter de drempel om een aanval uit te voeren is 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 cyber-weerbaarheid tegen DDoS-aanvallen op orde moeten hebben.

Ransomware
De grootste dreiging op dit moment in de zorgsector is ransomware en dit zal voorlopig zo blijven. 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. Er zijn drie preventieve maatregelen die de kans om slachtoffer te worden van ransomware aanzienlijk verkleinen.

Datalekken
Er zijn verschillende manieren waarop datalekken tot stand komen: malware, 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 ook 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 werden door veel nationale cybersecurity autoriteiten gewaarschuwd dat er verhoogde interesse door statelijke actoren is in COVID-19 onderzoek. Bij Z-CERT zijn dit jaar 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.

Cybersecurity is een kwestie van goed managen. 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.

column

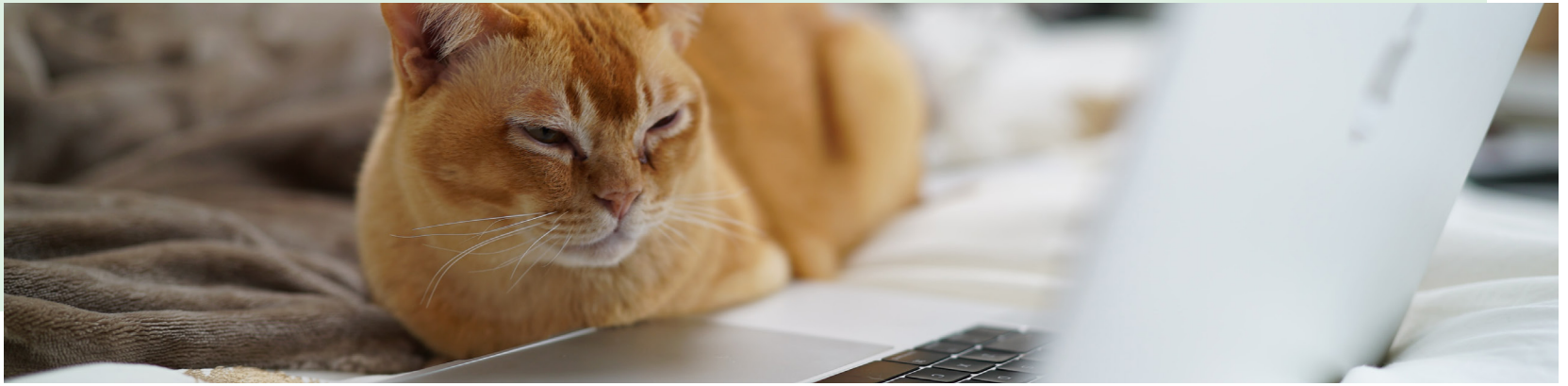
Ewald Beekman IT Security Officer, Amsterdam UMC

De zorg kan niet meer om cybersecurity heen; het 8-uur journaal opent er mee als het mis gaat. De bestuurders vragen zich vervolgens af hoe het dan "bij ons" zit, zijn wij veilig en beginnen te appen.

Begin van dit jaar was dat al dubbel het geval. Begonnen we met de ransomware aanval op de Universiteit Maastricht, daarna werd het nieuws ingehaald door kwetsbaarheden in Citrix Netscaler. Nederland maakte kennis met het begrip Citrix-file omdat de thuiswerkoplossing dicht was gezet. Die Citrix kwetsbaarheden hadden nog een trieste nabrander toen een Duits ziekenhuis in september(!) alsnog via dit lek met ransomware besmet raakte en de SEH moest sluiten. Een ambulance op weg naar dit ziekenhuis werd omgeleid waardoor de patiënt pas een uur later op de operatietafel lag. Voor de patiënt kwam dit te laat en zij is overleden. Dat doet beseffen waar het allemaal om draait en dat het zo ontzettend belangrijk is om het goed te doen.

Dat cyberincidenten vele vormen kan hebben bleek bijvoorbeeld toen wij een melding van een Amerikaanse vrouw kregen over een hulpvraag die zij via de mail ontvangen had. In die mail (via een nagebootst domein) vroeg een Nederlandse militair een bijdrage voor de kankerbehandeling van zijn zoon. De nep-factuur had ons briefhoofd en bevatte behalve de kosten van $52.000 ook

'Waren we eerst sprinters, nu moeten we omscholen naar marathon renners.'



röntgenfoto's van de zogenaamde patiënt. Gelukkig leidde juist dat aspect tot argwaan van de Amerikaanse en vroeg ze het toch maar even na bij ons.

Het blijkt wel dat er steeds frequenter hoog risico kwetsbaarheden voorbijkomen. Waren we eerst sprinters, nu moeten we omscholen naar marathon renners. Er gaat geen maand voorbij of er is wel een nieuw lek in het nieuws dat direct acteren vereist. Natuurlijk komt dat ook omdat NCSC en Z-CERT bovenop het cybersecurity nieuws zitten en iedereen voorzien van actuele informatie. Als instelling moet je ook maar met die stroom van risico's om kunnen gaan. Gelukkig begint de cybersecurity machinerie van speuren, melden, acteren en controleren steeds meer een vaste plaats te krijgen in de organisaties. Veel instellingen snappen al dat dit niet meer het werk van één "local hero" is, maar dat hier een team van een aantal fte voor nodig is.

Door corona is de digitalisering in een verdere stroomversnelling gekomen. De thuiscomputer lijkt voor een aantal van ons voorlopig de primaire werkplek te zijn en videoconferencing is al bijna net zo gewoon als bellen. Het gebruik van clouddiensten zet door en daarmee staat het oude (simplistische) model van "veilig binnen, onveilig buiten" onder spanning. Zoals we werken, anytime and anywhere, zo zal ook onze beveiliging anytime and anywhere moeten worden.

> **"Zoals we werken, anytime and anywhere, zo zal ook onze beveiliging anytime and anywhere moeten worden."**

Bij het lezen van deze tekst vraagt u zich misschien af wat uw bijdrage kan zijn op dit gebied.

Mijn advies, ga eens praten met uw CISO, vraag waar hij of zij wakker van ligt en hoe u hem of haar kan helpen om gerust te kunnen slapen.

Bibliografie

ACSC. (2020). Retrieved from Advanced Persistent Threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services: https://www.cyber.gov.au/acsc/view-all-content/alerts/advanced-persistent-threat-apt-actors-targeting-australian-health-sector-organisations-and-covid-19-essential-services

ACSC. (2020, Juni). *Microsoft Office Macro Security.* Retrieved from https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security

AP. (2019). Retrieved from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verwerkers#wat-moet-er-in-een-verwerkersovereenkomst-staan-7104

CERT-EU. (2017). *DDoS Overview and Response Guide.* Retrieved from https://cert.europa.eu/static/WhitePapers/CERT-EU_Security_Whitepaper_DDoS_17-003.pdf

CERT-EU. (2020, maart 23). *Attacks on Healthcare.* Retrieved from https://media.cert.europa.eu/static/MEMO/2020/TLP-WHITE-CERT-EU-MEMO-Attacks-on-Healthcare.pdf

CISA, & FBI. (2020). Retrieved from APT Actors Chaining Vulnerabilities Against SLTT, Critical Infrastructure, and Elections Organizations: https://us-cert.cisa.gov/ncas/alerts/aa20-283a

Citrix. (2020). Retrieved from https://www.citrix.com/about/legal/security-compliance/security-standards.html

ENISA. (2020). Retrieved from ENISA Threat Landscape 2020 - Distributed denial of service: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

Europol. (2020). I*NTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020.* Retrieved from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

FBI. (2020, maart 30). *Kwampirs Malware Employed in Ongoing Cyber Supply Chain Campaign Targeting Global Industries, including Healthcare Sector.* Retrieved from https://www.aha.org/system/files/media/file/2020/03/fbi-alert-tlp-white-kwampirs-malware-employed-in-ongoing-cyber-supply-chain-campaign-targeting-global-industries-healthcare-sector-3-30-2020.pdf

FireEye. (2019). *Beyond Compliance:Cyber Threats and Healthcare.* Retrieved from https://content.fireeye.com/cyber-security-for-healthcare/rpt-beyond-compliance-cyber-threats-and-healthcare

FireEye. (2020, maart 25). *This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits.*

Retrieved from https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

HMR. (2020). Retrieved from https://www.hmrlondon.com/hmr-targeted-by-cyber-criminals.

Krebs, B. (2019, november). *110 Nursing Homes Cut Off from Health Records in Ransomware Attack.* Retrieved from https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/

Krebs, B. (2019a). *Ransomware at Colorado IT Provider Affects 100+ Dental Offices.* Retrieved from https://krebsonsecurity.com/2019/12/ransomware-at-colorado-it-provider-affects-100-dental-offices/

Krebs, B. (2020, mei 6). *Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware.* Retrieved from https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/

Le Monde. (2019). *Frappé par une cyberattaque massive, le CHU de Rouen forcé de tourner sans ordinateurs.* Retrieved from https://www.lemonde.fr/pixels/article/2019/11/18/frappe-par-une-cyberattaque-massive-le-chu-de-rouen-force-de-tourner-sans-ordinateurs_6019650_4408996.html

Microsoft. (2020, September). https://www.microsoft.com/en-us/download/details.aspx?id=101738. Retrieved from Microsoft Digital Defense Report.

NCSC. (2019). Retrieved from https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties

NCSC NL. (2020). *Toename aan intensiteit en aantal DDoS-aanvallen.* Retrieved from https://www.ncsc.nl/actueel/nieuws/2020/september/4/toename-aan-intensiviteit-en-aantal-ddos-aanvallen

NCSC UK. (2019). *Zero trust architecture design principles.* Retrieved from https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-design-principles

NCSC UK. (2020, juli 16). Retrieved from https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

RTLNieuws. (2020, oktober 1). *Groot datalek bij Jeugdriagg: medische dossiers kwetsbare kinderen gelekt.* Retrieved from https://www.rtlnieuws.nl/nieuws/nederland/artikel/5187220/jeugdriagg-kenter-jeugdhulp-datalek-dossiers

Sophos. (2020). *THE STATE OF RANSOMWARE 2020.* Retrieved from https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf

University of Utah. (2020, August). https://attheu.utah.edu/facultystaff/university-of-utah-update-on-data-security-incident/. Retrieved from University of Utah update on data security incident

Verizon. (2020). *2020 Data Breach Investigations Report.* Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Wired. (2020, november 11). *The untold story of a cyberattack, a hospital and a dying woman.* Retrieved from https://www.wired.co.uk/article/ransomware-hospital-death-germany

Dankwoord

Dit document is een initiatief van Stichting Z-CERT en is mede tot stand gekomen dankzij de steun van onze deelnemers en het Ministerie van Volksgezondheid Welzijn en Sport.

Onze speciale dank aan columnisten **Ewald Beekman** en **Jonathan Bouman** voor hun bijdrage aan dit Cyberdreigingsbeeld. We danken ook **Hugo Leisink** van het Nationaal Cyber Security Center voor het tegenlezen van de ruwe versie van het document en zijn constructieve commentaar.

Dank ook aan alle specialisten van Z-CERT voor hun inhoudelijke bijdragen, advies, geduld en tegenlezen van de tekst. Tot slot, dank aan **Artiënne Buissant des Amorie** van Artgen voor de opmaak van dit allereerste Cyberdreigingsbeeld voor de Zorg.

Vragen of opmerkingen over dit rapport:
communicatie@z-cert.nl

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
033 737 06 09

info@z-cert.nl
www.z-cert.nl