COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Bescherm uw zorgorganisatie tegen ransomware

Versie: 1.0

31 december 2019

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
the Netherlands
+31 (0)33 737 06 09

info@z-cert.nl
www.z-cert.nl
IBAN NL32 INGB 0007 4995 81
KvK 67374972
BTW 856955516B01

Inhoud

1 Inleiding

Er is een toegenomen dreiging van gerichte aanvallen met ransomware op de zorgsector door goed georganiseerde groepen cybercriminelen (Europol, 2019). Z-CERT presenteert in deze factsheet in grote lijnen de maatregelen die u kunt nemen om een ransomware-infectie te voorkomen en om de impact van een aanval te beperken. Aan het eind van dit artikel staat een samenvatting met alle maatregelen op een rijtje. De factsheet is bedoeld voor technische IT- en security specialisten. Voor een aantal maatregelen binnen deze lijst worden meer diepgaande technische kennisproducten ontwikkeld in samenwerking met onze deelnemers.

1.1 Wat is ransomware

Crypto-ransomware is een malwaretype dat de data van uw organisatie ontoegankelijk kan maken door deze te versleutelen. Uw data wordt daardoor onleesbaar en onbruikbaar. Dit kan directe consequenties hebben voor de patiëntveiligheid indien vitale data niet toegankelijk is voor zorgpersoneel. Echter zorginstellingen melden ook impact op fysieke security systemen, HVAC systemen en het functioneren van medische apparaten (Branch, 2018).

Om de data te ontsleutelen moet een gedupeerde instelling een specifieke digitale sleutel, voor een vaak hoog bedrag, kopen van een aanvaller. Er is geen garantie dat deze sleutel na betaling ook daadwerkelijk ontvangen wordt. In sommige gevallen zijn de sleutels publiek beschikbaar en kan de data ontsleuteld worden zonder te betalen (nomoreransom.org, 2019).

1.2 Dreigingsbeeld ransomware

Daar waar doelwitten in 2017 en 2018 vrij willekeurig gekozen werden, zien we in 2019 wereldwijd een flinke toename van gerichte ransomware-aanvallen op organisaties in zowel de private als de publieke sector (CERT-EU, 2019). Deze stijging is ook waar te nemen binnen de zorgsector (Kaspersky, 2019). Met het veranderen van het doelwit worden ook de bedragen die gevraagd worden steeds hoger. Inmiddels worden bedragen van boven een miljoen Euro gevraagd. Europol meldt in zijn “Internet Organised Crime Threat Assessment” (2019) dat ransomware de top cybercrime dreiging is van 2019 en dat dit waarschijnlijk voorlopig zo blijft.

We zien een professionalisering in de “ransomware sector”. Ransomware-aanvallen worden bijvoorbeeld aangeboden als een service zonder dat er technische kennis nodig is. De kwaadwillende kan gebruik maken van een helpdesk voor ondersteuning. Ook kunnen cybercriminelen soms logingegevens tot het netwerk van een zorginstelling op het internet of darkweb kopen. Hier zijn bij Z-CERT ook gevallen van bekend.

We zien dat deze doelgerichte aanvallen nauwkeurig gepland en gecoördineerd worden. Zo werden er in augustus 2019, 23 lokale overheden in Texas tegelijkertijd aangevallen. Dit was een aanval waarbij het doelwit nauwkeurig uitgekozen en de aanval zorgvuldig gecoördineerd en gepland was (CERT-EU, 2019). Er bestaan dus groepen cybercriminelen die zowel de organisatorische als de technische vaardigheden en ervaring hebben om grote groepen organisaties succesvol aan te vallen. Wij raden zorgorganisaties aan om te evalueren of hun organisatie opgewassen is tegen dit soort aanvallen.

1.3 Gevolgen van ransomware

Ondertussen richt ransomware veel schade aan in de zorgsector wereldwijd. Bij een recente aanval (oktober, 2019) moest bij een aantal Australische ziekenhuizen chirurgische ingrepen worden uitgesteld, werden financiële systemen getroffen en moesten systemen met patiëntengegevens worden uitgezet (Barwon Health, 2019).

Bij een andere aanval (oktober, 2019) kon een aantal regionale ziekenhuizen in de Verenigde Staten geen reguliere nieuwe patiënten aannemen en moesten ambulances naar andere ziekenhuizen uitwijken (DCH Health System, 2019).

In 2017 tijdens de grote uitbraak van de Wannacry Ransomware variant, werden 36 zorginstellingen in het Verenigd Koninkrijk geraakt en stonden in sommige gevallen levens op het spel (Chappell & Neuman, 2017).

Vooral zorginstellingen in de Verenigde Staten zijn doelwit maar ook steeds vaker worden zorginstellingen in Europa aangevallen. In de zomer van 2019 werden in Duitsland dertien ziekenhuizen (Süddeutsche Zeitung, 2019) getroffen door Ransomware, in Roemenië naar schatting 5 ziekenhuizen (Romania Journal , 2019) en in november een ziekenhuis in Frankrijk (CHU Rouen, 2019), verschillende ziekenhuizen in Spanje (Noticiascyl, 2019) en in december een ziekenhuis in Tsjechië (Kronen, 2019). Dit zijn alleen de ziekenhuizen waarbij publiek is gemaakt dat er een ransomware-incident was.

Wat opvalt uit de zaken in Duitsland en Roemenië is dat zorginstellingen soms IT-faciliteiten en -services met elkaar delen en dat een ransomware-aanval direct impact heeft op meerdere zorginstellingen. Dit soort IT-organisaties vormen steeds vaker een doelwit voor cybercriminelen (CERT-EU, 2019b).

Voor de zorgsector in Nederland zijn voor 2019 nog geen specifieke landelijke statistieken bekend, behalve dat bij Z-CERT wel in 2018 en 2019 ransomware incidenten gemeld zijn. Het algemene beeld in Nederland is dat ook hier dat het aantal zorgvuldig geplande ransomware aanvallen op organisaties toeneemt (Kronen, 2019).

2 Impact van een ransomware aanval beperken

2.1 Maak back-ups en test ze regelmatig

Wat vaak mis gaat is dat back-up procedures, waaronder het terugzetten van de data, zelden of niet getest worden. Het risico is dat problemen met deze procedures of de back-ups zelf pas aan het licht komen op het moment dat er een ransomware-incident speelt. Een vervelend scenario, waarbij in het verleden ziekenhuizen toch hoge bedragen betaalden omdat ze niet instaat waren hun data op korte termijn te herstellen (Connolly, 2019).

Houd er ook rekening mee dat moderne ransomware vaak probeert back-ups te versleutelen of te verwijderen. Het hebben van een offline back-up is daarom geen overbodige luxe. Belangrijk is dat de devices zelf geen toegang hebben tot de back-uplocatie. We raden aan de "3-2-1-1" regel te hanteren. Dit wil zeggen: heb minstens 3 kopieën van de data, gebruik 2 verschillende media, heb 1 offsite back-up (back-up op een ander netwerk, bv de cloud) en 1 offline back-up (Veeam, 2016).

Wij raden aan om de "kroonjuwelen" binnen uw netwerk te identificeren en extra middelen te wijden aan het beveiligen en back-uppen van deze data. Voor een zorginstelling zal dit o.a. alle persoonlijke gezondheidsinformatie zijn. Betrek met name ook deze data in uw incident response plan en crisissimulatietrainingen. De zekersheidsaspecten beschikbaarheid, integriteit en vertrouwelijkheid (BIV) uit de NEN7512 kunnen u helpen de bedrijfsmiddelen binnen uw netwerk te classificeren (NEN, 2015) en de kroonjuwelen te identificeren.

Voor een implementatierichtlijn en een checklist voor back-up maatregelen verwijzen we u naar de NEN7510 (NEN, 2017).

2.2 Pas "privilege access management" principes toe

2.2.1 Least privilege

Het is belangrijk dat wanneer ransomware toeslaat, zo min mogelijk data versleuteld wordt. Bij het "least privilege" model geeft u aan uw gebruikers alleen die toegang tot data die strikt noodzakelijk is voor hun werk en evalueert u periodiek of de rechten nog steeds noodzakelijk zijn.

Bij een eventuele ransomware-incident wordt de hoeveelheid data die versleuteld wordt op deze manier zoveel mogelijk beperkt. Microsoft heeft uitgebreide documentatie hoe u "least privilege" in een Windowsomgeving zou kunnen inrichten (Microsoft, 2019a), maar ook in Office365 (Microsoft, 2019c) en Azure (Microsoft, 2019d).

Least privilege kan ook al op een heel basaal "access management" niveau worden toegepast. Een voorbeeld hiervan was een zorginstelling die na een ransomware-aanval evalueerde wie er voor hun dagelijkse taken toegang nodig hadden tot het netwerk. Op basis hiervan trokken ze vele accounts in (Branch, 2018).

2.2.2 Fileshares

Het is belangrijk om na te denken over het gebruik van fileshares binnen uw organisatie. Ransomware scant het netwerk actief naar netwerkshares (Vectra, 2019) en beperkt zich niet tot de automatisch toegevoegde netwerkschijven. Daar waar veel mensen schrijfrechten hebben op bepaalde data is de kans dat dit versleuteld wordt door ransomware ook groter.

Least privilege houdt ook in dat mensen zo min mogelijk schrijfrechten hebben op fileshares. U kunt ook er voor kiezen dat mensen zichzelf tijdelijk schrijfrechten kunnen geven of deze kunnen aanvragen door gebruik te maken van een JIT-admin oplossing. Hierbij wordt de kans kleiner dat een gebruiker op het moment van ransomware-infectie schrijfrechten heeft tot een bepaalde share.

Microsoft heeft een JIT-admin oplossing meegeleverd met Windows Server (Microsoft, 2019a), maar ook met het makkelijker te implementeren JEA kan vergelijkbare functionaliteit gecreëerd worden (Microsoft, 2019g). Binnen een Active Directory omgeving kan sinds Windows Server 2016 tijdelijke lidmaatschappen tot groepen gedefinieerd worden (Smirnov, 2018). Hiermee zou bijvoorbeeld voor de duur van een project schrijfrechten gegeven kunnen worden tot een bepaalde map.

Back-ups, gevoelige data en archief data hoeven niet toegankelijk te zijn op fileshares waar mensen schrijfrechten hebben met hun standaard loginaccounts. Er bestaan voor dit soort data goede alternatieven, zoals SFTP.

2.2.3 Hoge rechten gaan niet samen met risicovolle activiteiten

Waar het mis kan gaan is als beheerders of medewerkers met toegang tot gevoelige data hun accounts gebruiken om op het internet te browsen of om bijlages te openen vanuit hun mailprogramma. Voor normaal internetgebruik is het aan te bevelen om nooit accounts te gebruiken met meer rechten dan reguliere gebruikers. Er zitten regelmatig kwetsbaarheden in browsers die gebruikt zouden kunnen worden om ransomware te installeren (Kaspersky, 2019). Ook is het aan te raden voor beheerders of medewerkers met veel rechten in de IT-omgeving om workstations te gebruiken die speciaal ingericht zijn voor het uitvoeren van beheertaken met directe toegang tot gevoelige gegevens. Microsoft heeft informatie beschikbaar over hoe je deze “Privilege Access Workstations” in uw organisatie kan implementeren (Microsoft, 2019b). De functionaliteit die daarvoor nodig is, is reeds aanwezig in Windows. Wat betreft patiëntendata is het goed te definiëren op welke servers patiëntendata mag staan en vanaf welke computers toegang verkregen mag worden tot deze data.

2.2.4 Beperk de lokale administrator

Het kan mis gaan als er accounts worden gebruikt die lokale administrator rechten geven op alle workstations in de omgeving. Dit is niet ongebruikelijk bij accounts voor bijvoorbeeld servicedeskmedewerkers. Op deze manier is 1 gecompromitteerd servicedesk-account een toegangskaartje tot vele computers. Indien de omgeving gebaseerd is op Active Directory kan een lokale administrator alle rechten overnemen van iedereen die op hetzelfde device gaat inloggen. Ook kunnen bestaande sessies worden overgenomen.

Microsoft heeft een gratis tool beschikbaar die ervoor zorgt dat iedere computer een unieke administrator heeft (Microsoft, 2018).

2.2.5 Laat hackers niet oversteken van workstation naar server

Zorg dat accounts met hoge rechten in het netwerk niet mogen inloggen op workstations die gebruikt worden voor risicovolle activiteiten als mailen en browsen op het web. Ditzelfde principe kan worden toegepast worden op meerdere lagen in de ICT-infrastructuur. Dit wordt het "Administrative Tier Model" genoemd. Op deze manier zorg je dat hackers veel moeilijker vanuit workstations kunnen "oversteken" naar servers en back-up-servers. Dit is een bekende tactiek bij ransomware-aanvallen (Sophos, 2019). Microsoft heeft een uitgebreid document over hoe je dit "Administrative Tier Model" zou kunnen inrichten binnen een omgeving (Microsoft, 2019e).

2.2.6 Beperk leverancierstoegang

Maak afspraken met leveranciers wanneer zij mogen inloggen. Houd daar het principe van "least privilege" aan. Zorg dat de leveranciers alleen mogen inloggen wanneer is afgesproken. Audit wat de leverancier gedaan heeft. Bij leveranciers bent u afhankelijk van de security die deze partij intern heeft. Als zij hun security niet op orde hebben, dan is dit voor uw organisatie een risico. Het is daarom geen overbodige luxe en uw goed recht om hier strikt mee om te gaan. Neem hardening op als eis bij de aanschaf van nieuwe apparatuur.

2.3 Incident response plan voor ransomware

Het reguliere "incident response plan" is bij een ransomware-aanval vaak niet afdoende. Ook is het hebben van een herstelplan niet genoeg, de haken en ogen worden pas echt zichtbaar bij een simulatietraining.

De impact van een ransomware-aanval is in potentie zo groot dat hier organisatie breed over nagedacht moet worden. Alles wat gebruik maakt van het netwerk en computers kan in principe geraakt worden tijdens een ransomware-aanval. Als het niet door de ransomware zelf is, dan kan het zijn doordat bepaalde gedeelten van het netwerk of systemen moeten worden uitgeschakeld om verspreiding van de ransomware te voorkomen.

Zorginstellingen rapporteerden naast impact op de reguliere IT-infrastructuur ook impact op bijvoorbeeld medische apparaten, HVAC systemen, fysieke security systemen en het functioneren van vele applicaties (Branch, 2018). Om "gevoel" te krijgen voor de impact die zoiets kan hebben op de organisatie, volgen enkele voorbeelden.

2.3.1 IT-infrastructuur

De impact op de IT-infrastructuur kan groot zijn. Soms is slechts een aantal workstations in een bepaald netwerksegment geïnfecteerd, maar andere keren weten hackers diep door te dringen in het

netwerk en weten ze verhoogde rechten te krijgen. Er zijn situaties bekend waarbij dit het geval was en bijna alle systemen in het ziekenhuis moesten worden uitgeschakeld en elke PC en netwerkapparaat vervangen werd of opnieuw geïnstalleerd en geconfigureerd moest worden. Het duurde bijna zes maanden totdat het ziekenhuis weer volledig operationeel was (Branch, 2018).

2.3.2 Medische apparaten

Soms zijn medische apparaten afhankelijk van de beschikbaarheid van het netwerk of de bereikbaarheid van het elektronische patiëntendossier. Een ziekenhuis rapporteerde dat ze de glucosewaarden in het bloed niet meer konden meten, omdat deze meetapparaten zo geconfigureerd waren dat ze alleen konden meten als het patiëntennummer gescand was. Omdat dit niet functioneerde (het EPD was niet bereikbaar) konden glucosebloedwaarden niet gemeten worden (Branch, 2018).

2.3.3 HVAC en toegangssystemen

Ziekenhuizen rapporteerden ook problemen met hun fysieke security systemen en HVAC systemen. Zo was er een ziekenhuis waar de badgereaders korte tijd niet werkten. En bij een ander ziekenhuis werkte de security camera's een tijd niet. Bij een ziekenhuis waren er problemen bij het monitoren van de temperatuur en ventilatie en moest de monitoring en ook de aanpassingen handmatig worden uitgevoerd (Branch, 2018).

2.3.4 Applicaties

Wat ziekenhuizen die getroffen worden door een ransomware-aanval soms melden is dat er geen goed overzicht was van de applicaties die gebruikt werden binnen het ziekenhuis. Van sommige applicaties had de IT-afdeling geen idee dat ze gebruikt werden. Als niet duidelijk is welke applicaties er draaien welke rollen zij vervullen binnen een organisatie, dan is dat bij het herstelproces na een incident een probleem, zeker omdat de risico's van deze applicaties ook niet bekend zijn.

3 Voorkomen van ransomware-infectie

3.1 Blokkeer malafide mail

De meeste ransomware komt nog binnen via mailcampagnes. Dit zijn steeds meer hele gerichte phishingcampagnes op bijvoorbeeld belangrijke medische professionals (Proofpoint, 2019).

Er is een aantal technische maatregelen die u kunt nemen om phishing en andere malafide mail zoveel mogelijk te stoppen.

De meest gebruikelijk zijn de implementatie van een spamfilter en multifactor authenticatie (Z-CERT, 2019). Voorkom daarbij dat via "legacy authenticatie" alsnog de multifactor barrière omzeild kan worden (Microsoft, 2018b).

Wat niet altijd vanzelfsprekend is, is de implementatie van SPF, DKIM en DMARC . Bij een succesvolle implementatie van deze technologieën wordt het minder makkelijk voor aanvallers om te mailen uit naam van uw organisatie. In de praktijk wordt dit gebruikt door bijvoorbeeld te mailen met het e-mailadres van uw collega, waardoor u eerder geneigd bent een malafide bijlage te openen. Voor de technische details voor deze implementaties raden wij het paper van NCSC over phishing aan (NCSC, 2015).

3.2 Patchmanagement

Het updaten en patchen van software is zeer belangrijk. Er zitten regelmatig kwetsbaarheden in RDP, VPN-oplossingen, routers en firewalls. Deze kwetsbaarheden worden veel misbruikt (NCSC UK, 2019) om in te breken op netwerken en er is gratis software beschikbaar om te scannen op dit soort kwetsbaarheden en de kwetsbaarheid actief te misbruiken.

Naast malafide mail komt veel ransomware de organisatie binnen via het remote desktop protocol (RDP). Kwetsbaarheden in RDP zoals Bluekeep (CISA, 2019)kunnen gebruikt worden om servers binnen te dringen en van daaruit is het vaak makkelijk voor een aanvaller om uw netwerk verder binnen te dringen. Ook zijn er verschillende kwetsbaarheden in SMB die door Ransomware misbruikt kan worden (RiskSense, 2019). Sommige van deze RDP en SMB kwetsbaarheden zijn "wormable" wat betekent dat de malware zich zonder gebruikersinteractie kan verspreiden naar andere computers in het netwerk, die ook dezelfde kwetsbaarheden bezitten.

Er zijn legio andere kwetsbaarheden in serversoftware waarop ransomware binnen komt. Voorbeelden van software waar kwetsbaarheden actief misbruikt worden door ransomware zijn: Oracle JRE, WebLogic Server, RedHat's JBOSS application servers, Apache Struts, Tomcat, Spring Data ,Atlassian's Confluence en Elasticsearch (RiskSense, 2019).

In een studie waar onderzoek gedaan werd naar kwetsbaarheden die in toenemende mate gebruikt worden door ransomware, bleek dat meer dan de helft van de kwetsbaarheden een lagere CVSS v2 score had als 8 (RiskSense, 2019). Dit laat zien dat je als organisatie niet alleen oog moet hebben voor kwetsbaarheden die hoog zijn ingeschaald.

Daarnaast maakt ransomware ook vaak gebruik van kwetsbaarheden op uw lokale workstation. Kwetsbaarheden in Windows 10 of Windows 7 worden bijvoorbeeld gebruikt om administratorrechten te verkrijgen (Vectra, 2019).

Ook worden actief kwetsbaarheden in desktopapplicaties gebruikt om malware te installeren. Voorbeelden zijn: Office, Edge, Internet Explorer, Adobe Flashplayer maar ook desktopapplicaties als WinRar.

Het illustreert dat zowel aan de server en de client kant, patchen zeer belangrijk is en dat geen applicaties moeten worden uitgesloten van dit patchproces.

3.3 Scan op openstaande services binnen de infrastructuur

Wij raden aan RDP zoveel mogelijk dicht te zetten naar het internet toe. Als het echt niet anders kan, zorg er dan voor dat RDP alleen benaderbaar is via een VPN-oplossing en inclusief multifactor authenticatie. Dit geldt ook voor andere remote-access oplossingen zoals VNC. Daarnaast is het belangrijk dat SMB naar het internet toe dichtstaat. Het is aan te bevelen uw infrastructuur te scannen op het openstaan van services naar het internet. Soms staan services aan zonder dat dit de bedoeling is. Zeker als er veel administrators zijn, die niet voor de IT-afdeling werken, kan het gebeuren dat zij een service openzetten zonder dat ze de securityimpact hiervan overzien. Er is bij Z-CERT een geval bekend bij een buitenlandse zorginstelling waarbij RDP open stond naar het internet toe alhoewel dat niet de bedoeling was en alleen intern toegankelijk had moeten zijn. Dit had verstrekkende gevolgen.

3.4 Dwing af welke software mag worden uitgevoerd en welke niet

Een zeer krachtig middel om het uitvoeren van malware te voorkomen is applicatiewhitelisting. Hierbij wordt afgedwongen dat alleen bepaalde, goedgekeurde software uitgevoerd mag worden op een device. Op deze manier kan ransomware (en andere malware) die niet door de antivirusoplossing gedetecteerd wordt, tegengehouden worden. Microsoft heeft twee oplossingen voor het implementeren van applicatiewhitelisting die voor de meeste organisaties direct beschikbaar zijn omdat deze meegeleverd wordt met Windows (Microsoft, 2019f). U hoeft dus geen software aan te schaffen. Applicatiewhitelisting wordt ook aangeraden in de NEN7510 (NEN, 2017).

Applicatiewhitelisting kan veel malware tegen houden. Echter sommige code wordt niet uitgevoerd door Windows zelf, maar door een applicatie. Dit is het geval bij bijvoorbeeld macro's binnen Microsoft Office. De code die uitgevoerd wordt binnen macro's, wordt dus niet opgepikt door de applicatiewhitelisting software, tenzij de macro zelf malware gaat downloaden en deze op de reguliere manier probeert uit te voeren.

Macro's zijn nog steeds een veelgebruikte aanvalsvector binnen de zorgsector. Verizon onderzocht in 2019 duizenden security incidenten en bij 67.1% van de malware incidenten in de zorgsector werd een officedocument gebruikt als aanvalsvector (Verizon, 2019). Z-CERT adviseert het gebruik van macro's uit te schakelen. Mocht er echter toch noodzaak zijn dan zijn er mogelijkheden om het gebruik van Macro's extra te beveiligen. Meer informatie hierover kunt u lezen in een artikel van het Australische nationale CERT (ACSC, 2019). Wij adviseren u het gebruik van macro's uit te faseren. Voor enkele tips voor vervangende technologieën verwijzen wij u naar het artikel van het NCSC UK (NCSC UK, 2019b).

3.5 Gebruik een antivirusoplossing en zorg dat deze up-to-date blijft

Voor veel organisaties is dit vanzelfsprekend. Toch kan het zijn dat dit op oudere systemen ontbreekt of dat de virusscanner niet up-to-date is. Het vermoeden is dat de ransomware-aanval in een Roemeens ziekenhuis voorkomen had kunnen worden met een up-to-date antivirusscanner (ACTMedia, 2019). Ook is bekend dat op sommige medische apparaten de virusscanner standaard is uitgeschakeld (Frost & Sullivan, 2019).

3.6 Management van verwijderbare media

Het gebruik van verwijderbare media (zoals USB-sticks) brengt risico's met zich mee voor uw organisatie. Wij raden aan om beleid te ontwikkelen en implementeren voor het gebruik van verwijderbare media.

Het is zeer makkelijk een USB-stick met malware in een workstation te steken waardoor deze malware automatisch opgestart wordt. Of om iemand een USB-stick te geven, en te vragen om bijvoorbeeld een malafide Word document of PDF document te openen. Een kwaadwillende kan zich bijvoorbeeld voordoen als een sollicitant en vragen aan een medewerker om zijn CV uit te printen die zich op een malafide USB-stick bevindt. Overweeg of dit voor uw organisatie een waarschijnlijk risico is. Voor meer informatie over het managen van verwijderbare media, raden wij het artikel van NCSC UK aan (NCSC UK, 2018).

3.7 Netwerksegmentatie

Netwerksegmentatie is een bekende "best practice" binnen de security waar voor zorginstellingen nog winst is te behalen (Forescout, 2019). Het is aan te bevelen systemen met belangrijke en gevoelige data een eigen netwerksegment te geven, waarbij eventuele noodzakelijke routering strikt geregeld is. Als een pc van een eindgebruiker besmet raakt met ransomware, blijft het probleem beperkt tot dat segment, waardoor de kans dat het andere segment met de gevoelige data besmet wordt, drastisch wordt verlaagd.

3.7.1 Medische apparaten

Veel medische apparaten maken gebruik van oude software en oude versies van Windows. Deze apparaten hebben daarom security issues en kunnen soms zelfs niet meer gepatcht worden (Frost & Sullivan, 2019). Soms worden medische apparaten niet meer ondersteund door leveranciers omdat ze zijn uitgefaseerd. Ze worden daarom niet meer gepatcht (Frost & Sullivan, 2019). Ook zijn leveranciers vaak verantwoordelijk voor het patchen en configureren van medische apparaten. In sommige gevallen blijkt security niet een topprioriteit te zijn (Rahman, 2019).

Indien een apparaat waar deze issues spelen niet vervangen kan worden, is het zeer aan te bevelen het te isoleren op een segment waar het reguliere internetverkeer niet over heen gaat.

Forescout (2019) laat zien dat binnen 75 onderzochte zorginstellingen de medische apparaten verspreid waren over maar weinig netwerksegmenten. Dit doet vermoeden dat er nog niet systematisch over netwerksegmentatie was nagedacht en hier nog winst te halen valt. Zeker met de verwachte toekomstige groei van de hoeveelheid medische apparaten, is het nu een goed moment om na te denken over netwerksegmentatie.

3.8 Isoleer risicovolle websites en URL's en bijlages

3.8.1 Browserisolatie

Bij browserisolatie wordt een website niet zomaar in de browser geopend maar draait de browser in een geïsoleerde omgeving. Indien een malafide website wordt geopend, heeft de malware geen toegang tot de PC omdat hij als het ware gevangen zit in deze geïsoleerde omgeving. Microsoft heeft hiervoor een oplossing genaamd "Application Guard", wat standaard meegeleverd wordt met Windows 10 en dus geen extra kosten met zich meebrengt.

3.8.2 URLfiltering

Filter het uitgaande webbrowserverkeer en blokkeer malafide URL's. Er zijn hier zowel open source als commerciële oplossingen voor. Het is een heel makkelijke manier om bekende malware URL's te blokkeren.

Ook lokaal kan een filter draaien die verdacht verkeer opmerkt en ingrijpt. Windows heeft bijvoorbeeld "Windows Defender SmartScreen" en kan zonder extra kosten geactiveerd worden. Gebruikers zien een waarschuwing als zij klikken op een verdachte link. Windows Defender Smartscreen is geen vervanging voor geavanceerdere URL filtering proxy's, echter kan een extra toevoeging vormen voor de totaaloplossing.

3.9 Verhoog security awareness

De meeste ransomware komt nog altijd binnen via mailcampagnes (Europol, 2019). Net zoals elke cel in uw lichaam een essentiële rol vervult in het afweersysteem van het lichaam, zo zou dat ook moeten gelden voor elke medewerker in uw organisatie. Het is 1 van de belangrijkste pijlers in uw cybersecurity strategie.

Gebruikers trainen in het herkennen van malafide mail kan de hoeveelheid incidenten verlagen (Gordon, 2019). U kunt klassieke trainingsmodellen gebruiken als PowerPointpresentaties en quizzen. Er zijn ook andere werkvormen beschikbaar die de training kunnen verrijken, zoals rol-playing-games en computergames (Silic, 2019). Doordat gebruikers daar zelf verbanden moeten liggen, is dit vaak een effectief trainingsmiddel.

Naast dat u mensen kunt trainen kunt u ook een cultuur creëren binnen uw organisatie waarbij securitybesef intrinsiek aanwezig is en mensen zelf functioneren als onderdeel van uw digitale afweer. Training is daarbij een aanvulling. Er is een aantal zaken die u kunt doen om een securitybewuste organisatie te bouwen. Hiervoor verwijzen wij u graag door naar het rapport van SANS (SANS, 2019). Hier wordt u een spiegel voorgehouden in welke fase u, op weg naar een "security bewuste cultuur", zich bevindt en wat u kunt doen om dit te verbeteren.

Er zijn ook mensen binnen de organisatie die meer worden aangevallen dan anderen. Het is belangrijk deze mensen te identificeren. Het zijn mensen waarvan vermoed wordt dat ze veel toegang hebben tot gevoelige data of systemen. In de zorgsector zijn dit vaak artsen, leidinggevenden, onderzoekers of leidinggevend administratief personeel (Proofpoint, 2019). Ook worden vaak publieke mailadressen gebruikt die bijvoorbeeld op de website gepubliceerd worden. Mailadressen van onderzoekers zijn vaak makkelijk te vinden via de artikelen die zij publiceren.

In sommige mailoplossingen kunt u zien wie de meeste phishing mailtjes krijgt. U kunt aan deze mensen extra aandacht besteden wat betreft security awareness.

3.10 Uitschakelen niet-gebruikte services op medische apparaten

Het gebeurt regelmatig dat er bepaalde services openstaan op medische apparaten waar IT niet van op de hoogte is. Sommige van die services staan soms "per default" open, zonder dat het functioneel is. Services die soms ongemerkt openstaan zijn bijvoorbeeld: SMB, RDP, FTP, SSH, telnet maar ook DICOM (Digital Imaging and Communication In Medicine imaging protocol). Vooral kwetsbaarheden in SMB zijn in het verleden vaak gebruikt door Ransomware om zich te verspreiden. Onderzoeken laten zien dat bij meer dan 80% van de medische apparaten die Windows gebruiken op de onderzochte netwerken, SMB open stond (Forescout, 2019).

Daarnaast zijn protocollen als FTP en Telnet niet gewenst omdat ze geen encryptie gebruiken. Ze kunnen daarom het best uitgeschakeld worden. Bij deze protocollen kunnen met simpele algemeen beschikbare programma's de wachtwoorden van het netwerk bekeken of verzameld worden, zonder dat dit kan worden gedetecteerd.

Z-CERT beveelt aan om segmenten met medische apparaten op het netwerk regelmatig te scannen op de aanwezigheid van openstaande services. Daarbij kan ook opgemerkt worden dat er soms medische apparaten aangesloten worden op het netwerk buiten de IT-afdeling om (Forescout, 2019). Ook deze apparaten kunnen door te scannen gevonden worden en opgenomen worden in het reguliere changemanagementproces.

Deze problemen kunnen deels voorkomen worden door goede afspraken te maken met uw leverancier over de beveiliging van het apparaat, de services die aan mogen staan en het gebruik van protocollen.

4 Shortlist: bescherm uw organisatie tegen ransomware

Voorkomen van ransomware infecties

- Beveilig uw organisatie tegen phishing en malafide mail
    - Implementeer best practices voor mail security:
        - Antispam filter
        - Multifactor authenticatie
        - Implementeer SPF, DKIM en DMARC
- Zet RDP en SMB niet open naar het internet toe
    - Indien dit niet mogelijk is:
        - Zorg dat RDP alleen bereikbaar is via een VPN-connectie en vanaf bepaalde IP-adressen, met multifactor authenticatie
- Scan uw infrastructuur regelmatig op services die open staan naar het internet toe
- Patchmanagement
    - Patch uw servers, netwerkapparaten en workstations. Moderne ransomware gebruikt steeds vaker kwetsbaarheden.
    - Patch ook lager ingeschaalde kwetsbaarheden en sluit geen applicaties uit van het patchproces
- Applicatiecontrole
    - Implementeer applicatiewhitelisting
    - Schakel macro's uit of vervang macro's door veiligere alternatieven.
- Gebruik een antivirusoplossing en zorg dat het product up-to-date blijft
- USB device management
    - Definieer en implementeer beleid voor USB-sticks die op uw devices mogen worden aangesloten
- Isoleer risicovolle websites en URL's
    - Pas browserisolatie toe waar mogelijk
    - Detecteer malafide URL's en blokkeer deze
- Geef security awareness training en creëer een cybersecurity bewuste cultuur
- Segmenteer uw netwerk
    - Belangrijke data op eigen netwerksegment
    - Medische apparaten geïsoleerd op netwerksegment die niet gebruikt wordt voor normaal internetgebruik (mail, browsen).
- Schakel niet-gebruikte services zoals RDP en SMB uit op uw (medische) apparaten op uw interne netwerk.
- Vermijd het gebruik van protocollen die geen encryptie gebruiken
- Scan uw interne netwerk op services die niet gedocumenteerd/bekend zijn bij uw IT-afdeling

Impact van een ransomware aanval beperken

- Maak back-ups van uw data
    - Test back-upprocedures
    - Controleer de back-ups zelf
    - Geen toegang clients tot back-uplocatie
    - Maak een offline back-up
- Pas "privilege access management" principes toe
    - Geef mensen alleen de rechten die zij nodig hebben
    - Evalueer de rechten die mensen hebben regelmatig
    - Gebruik een JIT-admin oplossing voor fileshares waar mogelijk
    - Gebruik alternatieven voor fileshares waar mogelijk
    - Gebruik speciaal beveiligde workstations voor werkzaamheden die toegang geven tot gevoelige data of die hoge rechten nodig hebben
    - Laat hackers binnen een Active Directory omgeving niet oversteken van gebruikerscomputers naar servers door te voorkomen dat mensen met beheeraccounts inloggen op computers van gebruikers
    - Zorg dat leveranciers alleen mogen inloggen wanneer afgesproken en audit hun activiteiten, geef ze alleen de rechten die ze nodig hebben. Maak afspraken over hardening van het apparaat.
    - Vermijd het bestaan van lokale administrator accounts die met ditzelfde account op grote aantallen devices lokale administrator zijn. Gebruik geen lokale administrators of gebruik de gratis tool van Microsoft: LAPS.
    - In een Active Directory omgeving kunnen lokale administrators sessies en rechten overnemen van iemand die inlogt op de machine waar zij lokale administrator zijn. Houd hier rekening mee in uw privilege access management.

- Maak een incidentresponse en disaster recovery plan specifiek voor een aanval met ransomware en oefen dit plan.

5. Bibliografie

ACSC. (2019). Retrieved from Microsoft Office Macro Security: https://www.cyber.gov.au/publications/microsoft-office-macro-security

ACTMedia. (2019). Retrieved from https://actmedia.eu/daily/kaspersky-cyber-attack-on-hospitals-in-romania-is-part-of-alarming-tendency-at-world-level/81471

Barwon Health. (2019). *Cyber security incident*. Retrieved from https://www.barwonhealth.org.au/news/item/cyber-security-incident-2

Branch, L. E. (2018). *Cyber Threats and Healthcare Organizations: A Public Health Preparedness Perspective.* West Virginia University.

CERT-EU. (2019). *Big Game Hunting in the public sector.* Retrieved from https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-190916-1.pdf

CERT-EU. (2019). *EU-CERT.* Retrieved from Major web hosting providers become victims of ransomware: https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-191114-1.pdf

CERT-EU. (2019b). *Major web hosting providers become victims of ransomware Reference.* Retrieved from https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-191114-1.pdf

Chappell, B., & Neuman, S. (2017, December 19). *U.S. says North Korea 'directly responsible' for wannacry ransomware attack*. Retrieved from https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack?t=1575466997308

CHU Rouen. (2019, 11 19). *Le point sur l'attaque informatique du 15 novembre 2019*. Retrieved from https://www.chu-rouen.fr/le-point-sur-lattaque-informatique-du-15-novembre-2019/

CISA. (2019, 6 17). *Microsoft Operating Systems BlueKeep Vulnerability*. Retrieved from https://www.us-cert.gov/ncas/alerts/AA19-168A

Connolly, L. Y. (2019). Retrieved from The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures: https://www.sciencedirect.com/science/article/pii/S0167404819301336

DCH Health System. (2019). *News*. Retrieved from https://www.dchsystem.com/Articles/all_3_dch_health_system_hospitals_closed_to_new_patients_due_to_ransomware_attack.aspx

Europol. (2019). *Internet organized crime threat assessment (IOCTA).* Retrieved from https://www.europol.europa.eu/sites/default/files/documents/iocta_2019.pdf

Forescout. (2019). Retrieved from Putting Healthcare Security Under the Microscope: https://www.forescout.com/industries/healthcare/research-report-putting-healthcare-security-under-the-microscope/

Fox-IT. (2019, 10 28). Retrieved from https://twitter.com/foxit/status/1188753857037373440

Frost & Sullivan. (2019). Retrieved from Medical Device and Network Security.

Gordon, W. (2019, 3 8). Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions. *Health Informatics*. Retrieved from Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions: https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270

Kaspersky. (2019). Retrieved from IT threat evolution Q3 2019. Statistics: https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

Kronen. (2019). Retrieved from Krypto-Trojaner legt Spital in Tschechien lahm: https://www.krone.at/2060401

Microsoft. (2018). Retrieved from Remote Use of Local Accounts: LAPS Changes Everything. : https://blogs.technet.microsoft.com/secguide/2018/12/10/remote-use-of-local-accounts-laps-changes-everything/

Microsoft. (2018b). Retrieved from Email Phishing Protection Guide – Part 16: Disable Office 365 Legacy Email Authentication Protocols: https://blogs.technet.microsoft.com/cloudready/2018/11/21/part-16-disable-office-365-legacy-email-authentication-protocols/

Microsoft. (2019a). Retrieved from Securing privileged access: https://docs.microsoft.com/nl-nl/windows-server/identity/securing-privileged-access/securing-privileged-access

Microsoft. (2019b). Retrieved from Privileged Access Workstations: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

Microsoft. (2019c). Retrieved from Privileged access management in Office 365: https://docs.microsoft.com/en-us/microsoft-365/compliance/privileged-access-management-overview

Microsoft. (2019d). Retrieved from Wat is Azure AD Privileged Identity Management?

Microsoft. (2019e). Retrieved from Active Directory administrative tier model: https://docs.microsoft.com/nl-nl/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

Microsoft. (2019f, 01 08). *Application Control*. Retrieved from https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/windows-defender-application-control

Microsoft. (2019g). Retrieved from https://docs.microsoft.com/nl-nl/powershell/scripting/learn/remoting/jea/overview?view=powershell-6

NCSC. (2015, 10 28). Retrieved from Factsheet Bescherm domeinnamen tegen phishing: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing

NCSC UK. (2018). *10 steps to cyber security .* Retrieved from NCSC UK: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security?curPage=/collection/10-steps-to-cyber-security/the-10-steps/removable-media-controls

NCSC UK. (2019, 10 2). Retrieved from Vulnerabilities exploited in VPN products used worldwide: https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

NCSC UK. (2019b). Retrieved from https://www.ncsc.gov.uk/guidance/macro-security-for-microsoft-office

NEN. (2015). Retrieved from https://www.nen.nl/NEN-Shop/Nieuwsberichten-Zorg-Welzijn/NEN-7512-Informatiebeveiliging-in-de-zorg-Vertrouwensbasis-voor-gegevensuitwisseling-ter-commentaar-gepubliceerd.htm

NEN. (2017). Retrieved from https://www.werkenmetnen7510.nl/publicaties/nen-7510-2-2017/sec_12/sec_12.3.1

nomoreransom.org. (2019). Retrieved from nomoreransom.org: https://www.nomoreransom.org/

Noticiascyl. (2019). Retrieved from Los hospitales de León y El Bierzo superan un peligroso ciberataque: https://www.noticiascyl.com/leon/sucesos-leon/2019/12/05/los-hospitales-de-leon-y-el-bierzo-superan-un-peligroso-ciberataque/

Proofpoint. (2019). *Protecting Patients, Providers and Players.* Proofpoint. Retrieved from Protecting Patients, Providers and Players.

Rahman, A. (2019). Retrieved from How weak cybersecurity for medical devices is putting patient lives at risks: https://www.nsmedicaldevices.com/news/enforcing-cybersecurity-risks-patient/

RiskSense. (2019). Retrieved from Enterprise Ransomware: https://info.risksense.com/ransomware_report

Romania Journal . (2019). Retrieved from Cyber-attacks against 5 hospitals in Romania. CCR's website, also hacked: https://www.romaniajournal.ro/society-people/cyber-attacks-five-hospitals-romania-ccr-website-hacked/

SANS. (2019). Retrieved from 2019 Security Awareness Report: The Rising Era of Awareness Training: https://www.sans.org/security-awareness-training/reports/2019-security-awareness-report

Silic, M. (2019). Using Design-Science Based Gamification to Improve Organizational Security Training and Compliance. *Journal of Management Information Systems*.

Smirnov, E. (2018). Retrieved from Just-in-time administration in Active Directory: http://www.admin-magazine.com/Archive/2018/47/Just-in-time-administration-in-Active-Directory

Sophos. (2019). Retrieved from A SophosLabs white paper November 2019: https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/sophoslabs-ransomware-behavior-report.pdf

Süddeutsche Zeitung. (2019, july 17). Retrieved from https://www.sueddeutsche.de/digital/krankenhaeuser-schadsoftware-ransomware-virus-drk-1.4529406: https://www.sueddeutsche.de/digital/krankenhaeuser-schadsoftware-ransomware-virus-drk-1.4529406

Vectra. (2019). Retrieved from https://content.vectra.ai/rs/748-MCE-447/images/IndustryResearch_2019_Vectra_Ransomware_Spotlight_Report_072519.pdf

Veeam. (2016). Retrieved from 7 Practical tips to prevent ransomware attacks on backup storage: https://www.veeam.com/blog/tips-to-prevent-ransomware-protect-backup-storage.html

Verizon. (2019). Retrieved from 2019 Data Breach Investigations Report: https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf

Z-CERT. (2019). *Pak phishing aan.* Retrieved from https://www.z-cert.nl/mededelingen/articles/whitepaper-phishing