pinewood

Whitepaper

Wapenen tegen ransomware in de zorg is simpeler dan u denkt!

We see risks
before they hurt

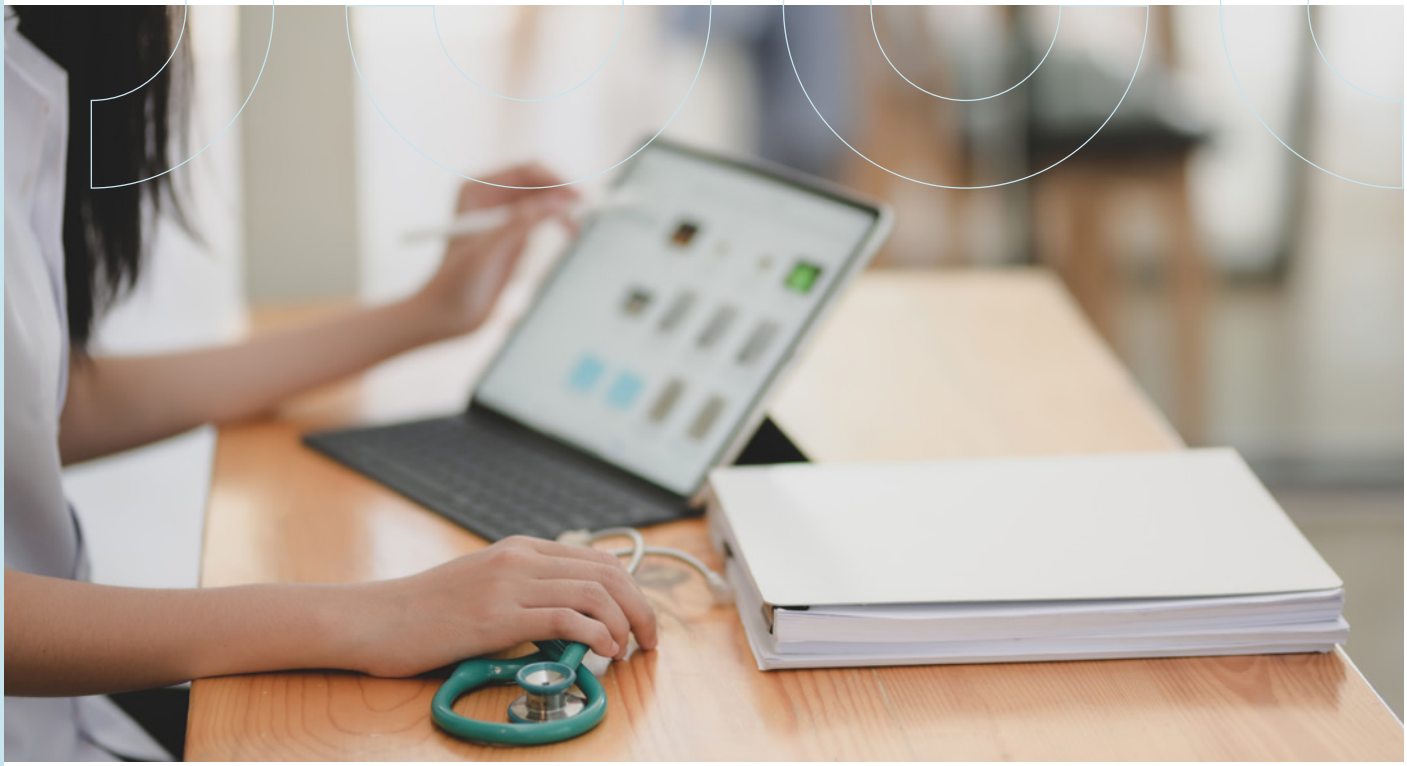
Wapenen tegen ransomware in de zorg is simpeler dan u denkt!

Een doelgerichte ransomware-aanval door cybercriminelen wordt door Z-CERT, het Computer Emergency Response Team voor de Nederlandse zorgsector, als de grootste dreiging gezien voor de zorg. Deze vorm van malware kan computersystemen en bestanden blokkeren, waarna cybercriminelen vaak losgeld (ransom) vragen om de gekaapte systemen en bestanden weer vrij te geven. Daarbij wordt er vaak gedreigd met het lekken of veilen van de gekaapte bestanden als de organisatie niet bereid blijkt te zijn het losgeld te betalen, maar het wapenen tegen ransomware is niet heel ingewikkeld. In deze whitepaper leest u waarom het misschien simpeler is dan u denkt.

Dreigingsbeeld ransomware

In februari 2021 bracht Z-CERT het eerste rapport 'Dreigingsbeeld voor de zorgsector' uit. Hierin geven zij aan dat de dreiging voor aanvallen met ransomware op de zorg hoog en permanent aanwezig is. Zo werden er in 2020 een bedrijf dat betrokken was bij een COVID-19 vaccin, een Duits ziekenhuis en een Tsjechisch ziekenhuis het slachtoffer van een grote ransomware-aanval. Dit waren geen Nederlandse zorginstellingen, maar dat betekent niet dat we in Nederland immuun zijn. Cybercriminelen zoeken namelijk op afstand naar zwakke plekken in de beveiliging van zorginstellingen. Waar deze geografisch staan, maakt in dit geval geen verschil.

Dit blijkt ook uit de rapporten van de deelnemende zorginstellingen aan Z-CERT. Hoewel zij geen doelwit zijn geweest van grote ransomware-aanvallen, geven zij wel aan te zijn gescand door kwaadwillenden en dat ze malware hebben ontvangen die bedoeld was om ransomware te downloaden. In een groot deel van de gevallen gaat het hier om de Emotet malware, dat via e-mail werd ontvangen.



Leveranciers

Leveranciers zijn vaak essentieel voor de zorgtaken van zorginstellingen. Dit maakt leveranciers een gewild doelwit voor aanvallers. Uit een onderzoek, uitgevoerd door Sophos in 2020, bleek dat 9% van de onderzochte ransomware-aanvallen werden veroorzaakt door gecompromitteerde leveranciers. Er zijn een aantal voorbeelden uit binnen- en buitenland waarbij leveranciers van EPD's werden geraakt, waardoor de aangesloten zorginstellingen een lange tijd geen toegang hadden tot hun patiëntdata. Om deze redenen is het belangrijk dat leveranciers niet blind worden vertrouwd door de zorg, maar dat er eisen aan hun informatiebeveiliging worden gesteld.

Zo zou de zorg van leveranciers kunnen eisen dat ze periodiek inzicht geven in hun informatiebeveiliging, dat ze voldoen aan de lokale wet- en regelgeving en dat ze over bepaalde certificeringen bezitten, zoals de NEN 7510. Ook zou er geëist kunnen worden om periodieke pentests en kwetsbaarheidscans te laten uitvoeren, zeker wanneer de leveranciers patiëntgegevens verwerken.

De bron van ransomware

Volgens onderzoeksbureau Gartner is 90% van de ransomware-aanvallen te voorkomen. Deze aanvallen komen meestal via de gebruiker binnen. Volgens het Center for Internet Security (CIS) komen de meeste ransomware-aanvallen op een systeem binnen:

- door phishing e-mails met een kwaadaardige bijlage;
- doordat een gebruiker op een kwaadaardige link klikt;
- door een advertentie te bekijken die malware bevat (malvertising).

Doordat ransomware veelal via de gebruiker binnenkomt, wordt er vaak gekeken naar het gedrag van de gebruiker en wordt dit direct gekoppeld aan awareness. Dit is zeker een onderdeel van security, maar zorgt niet voor een concrete oplossing. Naast preventieve maatregelen en awareness worden detectie en response veel belangrijker.

Security Monitoring

Door het inrichten van Security Monitoring beschermt u digitale systemen door een grote hoeveelheid aan databronnen te analyseren en hierin verdachte patronen en afwijkende gedragingen te detecteren. Met behulp van slimme algoritmes wordt de data optimaal geanalyseerd en kunnen cyberaanvallen worden gedetecteerd. Ook kan er direct op deze aanvallen worden gereageerd met passende maatregelen. Naast cyberaanvallen kan ook de werking van technische maatregelen gemonitord worden. Op die manier beheerst u de effectiviteit van uw maatregelen en kunt u risico's op tijd detecteren en nieuwe maatregelen treffen.

Endpoint Detection and Response (EDR)

Een van de beveiligingsoplossingen die wordt gebruikt binnen Security Monitoring is Endpoint Detection and Response. EDR is de opvolger van next-gen antivirus en biedt een geïntegreerde oplossing voor endpointbeveiliging. Door realtime continue bewaking en verzameling van endpointdata te combineren met geautomatiseerde respons- en analysemogelijkheden biedt EDR een concrete oplossing tegen ransomware. Zo kijkt EDR naast traditionele antivirus praktijken ook naar het gedrag van de gebruiker en dat van andere gebruikers wereldwijd. Door deze grote hoeveelheid data wordt er meer geanalyseerd en kunnen nieuwe dreigingen sneller gesignaleerd worden. Dit proces kunt u vergelijken met dat van een Security Operations Center (SOC).

EDR kan bijvoorbeeld detecteren dat een endpoint, zoals een laptop, regelmatig verbinding maakt met de buitenwereld of veel op het internet zit. Dit zou kunnen duiden op malware besmetting. De oorzaak hiervan is vaak onduidelijk, want het kan op allerlei manieren op het endpoint terecht zijn gekomen. Hierdoor is het bijna onmogelijk om dit met preventieve maatregelen te bestrijden. EDR kan vanwege de slimme algoritmes deze patronen snel detecteren en de gevolgen van een ransomware aanval voorkomen of minimaliseren.

Andere manieren om te wapenen tegen ransomware

Het opnemen van een EDR-oplossing is een geavanceerde manier om te wapenen tegen ransomware, maar er zijn ook simpelere manieren die u direct kunt implementeren. We noemen ze hieronder onderverdeeld in twee categorieën:

Security maatregelen die direct het risico van Ransomware beperken:

Patchen

Bijna alle ransomware maakt gebruik van kwetsbaarheden. Vaak zijn deze kwetsbaarheden reeds verholpen door middel van een patch, maar de kans op misbruik wordt alleen verkleind als deze patches daadwerkelijk geïnstalleerd zijn. Zorg ervoor dat u cybercriminelen geen kans geeft en onderhoudt uw software en applicaties met de laatste patches en updates.

Netwerksegmentatie

In een netwerk dat niet gesegmenteerd is, kunnen alle endpoints met elkaar 'praten'. Dit zorgt ervoor dat ransomware en andere dreigingen zich makkelijk kunnen verspreiden over de aangesloten endpoints in het netwerk. Door uw netwerk te segmenteren plaatst u endpoints in virtuele groepen binnen het netwerk en zorgt u ervoor dat een dreiging ingesloten kan worden in een deel van het netwerk. Hierdoor kan ransomware niet direct het gehele netwerk infecteren.

Offline back-ups

Wanneer ransomware eenmaal het netwerk is binnengedrongen, zal het lastig zijn om dit terug te draaien. Zeker als alle back-ups online, en vaak in hetzelfde netwerk, zijn opgeslagen. Daarom raden we aan om regelmatige back-ups offline te bewaren. Zo heeft u altijd nog een bron van data om op terug te vallen.

Security maatregelen die bijdragen aan de weerstand tegen ransomware:

Applicatiewhitelisting

Applicatiewhitelisting is het maken van een lijst met veilige applicaties, in plaats van een 'verboden lijst' te maken (blacklisting). Zo kunt u meer controle uitoefenen op welke applicaties verbinding kunnen maken met het netwerk en zorgt u ervoor dat applicaties die niet op de whitelist staan niet uitgevoerd kunnen worden. Wanneer u de tijd investeert in het implementeren en onderhouden van de applicatiewhitelist maakt u het ransomware afkomstig van het internet bijna onmogelijk om nog uitgevoerd te worden.

Remote Desktopprotocol (RDP)

Met het Remote Desktopprotocol (RDP) kan er op afstand gewerkt worden. Veel grote ransomware-aanvallen maken misbruik van RDP's die zijn aangesloten op het internet. Dit maakt het namelijk makkelijk voor cybercriminelen om een ingang te vinden. Zorg ervoor dat uw RDP niet direct is aangesloten op het internet, door bijvoorbeeld een VPN te implementeren, om de kans op misbruik van buitenaf aanzienlijk te verkleinen.

Microsoft Office macro's

De kleine programma's binnen Office-bestanden die vaak worden gebruikt om malware te downloaden en uit te voeren heten macro's. Om deze malware geen kans te geven zou de beste oplossing zijn om alle macro's afkomstig van het internet niet toe te staan en het gebruik van macro's uit te faseren. Zorginstellingen die toch bepaalde macro's nodig hebben, zouden het gebruik daarvan streng moeten reguleren.

Principle of Least Privilege (PoLP)

Het Principle of Least Privilege (PoLP) is gebaseerd op het idee dat een gebruiker alleen toegang heeft tot de cruciaal benodigde bestanden. Zo heeft iemand die alleen werkt met de database geen admin-rechten nodig en heeft een programmeur die alleen met code werkt geen toegang nodig tot de boekhouding. Wanneer gebruikers alleen de rechten hebben die nodig zijn voor het uitvoeren van hun taken, maakt u de kans dat malware zich kan verspreiden door uw netwerk kleiner. Dit zorgt ervoor dat kritische systemen en gevoelige data minder vatbaar zijn voor misbruik.

Hoe helpt Pinewood?

Pinewood doet meer dan detecteren en reageren. Wij ondersteunen zorginstellingen preventief en voeren gesprekken over de risico's van onder andere malware en hoe die opgevangen dienen te worden. Hiermee slaan we een brug tussen techniek en beleid.

- Wij helpen u met het uitvoeren van een gedetailleerde risicoanalyse.
- Endpointdetectie en EDR maken het mogelijk om aanvallen en bedreigingen in realtime te signaleren en aan te pakken.
- Met behulp van Continuous Vulnerability Scanning analyseren, interpreteren en prioriteren onze Pinewood-specialisten continu uw informatie.
- Met ons SOC kunnen we de effectiviteit van uw informatiebeveiligingsmaatregelen controleren en de controle op afwijkingen, in bijvoorbeeld de toegang tot patiëntgegevens, uit handen nemen. Onze beoordeling op veiligheidsincidenten is ingericht conform de norm NEN 7510-2, die zorginstellingen verplicht om de beschik-baarheid, integriteit en vertrouwelijkheid van medische gegevens te garanderen.

pinewood

Pinewood is al sinds 1994 een gevestigde naam in de dynamische wereld van de IT-beveiliging. Focus, kwaliteit en samenwerking zijn de kernelementen van onze filosofie. Pinewood focust zich niet exclusief op de technische kant van IT, maar legt altijd de link met uw business. Als zorgin-stelling betekent dit dat uw informatiebeveiliging in vakkundige en veilige handen is.

Benieuwd naar wat wij voor u kunnen betekenen? Bel ons dan gerust op **015 251 36 36** of stuur een mail naar **info@pinewood.nl**.

NEN
NEN 7510
INFORMATIEBEVEILIGING
IN DE ZORG

Pinewood BV.
Delftechpark 57
2628 XJ, Delft

015 251 36 36
info@pinewood.nl