Veilig mailen dankzij een e-mail wasstraat

14 april 2021

Met andere woorden, zij moeten een oplossing gebruiken die veilige communicatie garandeert. Fortinet is de eerste internationale security-leverancier die, dankzij de samenwerking met Pinewood, voldoet aan deze belangrijke norm op het gebied van e-mail.

Digitale transformatie staat al jaren hoog op de agenda in de zorgsector. De mogelijkheden om efficiënter met elkaar samen te werken en informatie uit te wisselen worden steeds vaker ingezet. De versnelling van deze digitalisering is niet meer te stoppen, ‘digitaal is het nieuwe normaal’. Maar daarmee ontstaat ook een toenemend risico op cybercriminaliteit. Het aantal doelgerichte ransomware-aanvallen in de zorgsector groeit elk jaar. Het gevaar hiervan is dat EPD’s niet meer beschikbaar zijn voor het raadplegen van patiëntengegevens. Daarmee vormen de aanvallen een directe bedreiging voor het leveren van zorg. Ook dreigen cybercriminelen steeds vaker met het openbaar maken van gevoelige informatie, als een organisatie niet wil betalen.

Adequate beveiliging e-mail cruciaal

Een veelgebruikte en effectieve methode die door cybercriminelen wordt ingezet is het verspreiden van zogenaamde phishing e-mails, in eerste instantie onschuldig berichten van een afzender die zich voordoet als een vertrouwde autoriteit die een nietsvermoedende gebruiker verleid tot het openen van een bijlage, het klikken op een link of het verschaffen van gevoelige informatie. Dit kan leiden tot datalekken en maakt aanvallen met ransomware mogelijk. Een adequate beveiliging voor e-mail is daarom cruciaal.

Fortinet’s FortiMail is een geavanceerde e-mailbeveiligingsoplossing die email de optimale bescherming biedt voor het berichtverkeer van organisaties. Niet alleen door het bieden van maatregelen zoals antispam, antivirus, IP/URI reputatie tegen bekende bedreigingen, maar ook tegen onbekende aanvallen, ook wel ‘zero-day’ genoemd.

Fortinet’s partner Pinewood heeft een configuratie-stappenplan opgesteld waardoor FortiMail voldoet aan de NTA 7516. Zorgorganisaties houden hierdoor controle over hun informatiebeveiliging, terwijl ze de eisen van wet- en regelgeving rond e-mailbeveiliging naleven.

Datalekken in de zorg

Paul Hoekstra, public sector sales manager bij Fortinet, vertelt: “De Autoriteit Persoonsgegevens kopt elk half jaar weer dat de meeste datalekken in de zorg voorkomen. Veel lekken ontstaan door e-mail. Medische gegevens die gemaild worden vereisen een goede bescherming, want je wilt niet dat de data in verkeerde handen terechtkomt.”

Om de zorg een veilige e-mail omgeving te bieden die voldoet aan wet en regelgeving, is Fortinet een samenwerking aangegaan met Pinewood. “Dit bedrijf is al jaar en dag een belangrijke partner van ons”, vervolgt Hoekstra, “die niet alleen veel kennis heeft van onze producten, maar ook heel goed weet welke problemen er spelen in de zorg, én hoe deze opgelost kunnen worden. Pinewood is een expert in informatiebeveiliging, en is dan ook gecertificeerd voor de NEN-norm 7510.”

Waar zijn de online gevaren?

“Fortinet is de eerste internationale security leverancier die in Nederland voldoet aan de norm”, zegt Arthur van Vliet, operations manager bij Pinewood. “Dat laat zien dat het bedrijf veel moeite doet om te voldoen aan wet- en regelgeving op landelijk niveau, en bovendien oog heeft voor de behoeftes van bepaalde marktsegmenten. De zorg is enorm gebaat bij een veilige mailomgeving die past binnen een bredere security-infrastructuur.”

De Security Fabric van Fortinet, waarin meerdere oplossingen van één leverancier threat-informatie met elkaar delen, zorgt voor minder beheerlast en lagere kosten doordat het taken versnelt en reacties automatiseert. De Security Fabric biedt organisaties tevens een beter inzicht in wat er speelt in het netwerk: waar komen de gevaren vandaan, waar gaat het mis? “Van Vliet: Met die kennis kan je het systeem zo inrichten dat bijvoorbeeld de kans op cyberaanvallen of het lekken van data geminimaliseerd wordt.”

De norm voor veilige communicatie is binnen de zorg aanleiding om goed naar de bestaande mailomgeving te kijken, en deze zo aan te passen dat het voldoet aan alle beveiligingseisen. Een belangrijk onderdeel van de NTA 7516 is de nadruk op interoperabiliteit tussen de verschillende oplossingen die onderdeel uit maken van de e-mailketen van een organisatie. Dit om ongestructureerde en ad-hoc berichtenverkeer te vermijden voor de uitwisseling van gevoelige informatie. “Het feit dat organisaties met FortiMail de regels van de NTA 7516 naleven, toont aan dat de integratie en samenwerking met andere systemen van een hoog niveau is”, aldus Hoekstra.

Norm e-mail ook voor andere markten

Ook ketenpartners, zoals lokale overheden, moeten voldoen aan de norm voor veilige communicatie, stelt Van Vliet. “Het veilig uitwisselen van gegevens is natuurlijk niet alleen in de zorg van belang, ook de overheid en bijvoorbeeld verzekeringsmaatschappijen en de juridische sector kijken met interesse naar ontwikkelingen op dit gebied. We verwachten dat deze, of een variant van deze norm de aankomende jaren voor veel meer sectoren verplicht wordt. Met de inzet van FortiMail zullen we nú de zorg, maar in de toekomst ook alle andere branches voorzien van een veilige mailoplossing die voldoet aan de eisen van beveiligingsrichtlijnen zoals de NTA 7516. Het is een groeimarkt, waar we samen met Fortinet enorm veel kunnen betekenen.”

Meer weten over Fortinet en veilig mailen? Schrijf je in voor het gratis online event op 28 april.

Dit artikel is tot stand gekomen in samenwerking met Fortinet.