Aanvallen in de zorg: epidemieën & datalekken

9 april 2018

In 2017 vond maar liefst één derde van alle datalekken plaats in de zorg. Dit komt mede door de gevoeligheid van de data binnen de gezondheidszorg, zoals medische dossiers, verzekeringsinformatie en financiële informatie. Laten we eens kijken naar de twee meest populaire vormen van cyberaanvallen in de zorg.

Afpersingsaanvallen

Afpersing is zoals gezegd zeer populair in de zorg. Afgelopen oktober kwam de bekende hacker thedarkoverlord weer in actie. Een Amerikaanse kliniek werd doelwit van een poging tot afpersing na een gegevensinbreuk met persoonsgegevens en gezondheidsgerelateerde informatie. Thedarkoverlord noemde de aanval op Twitter maar er is geen indicatie dat de gegevens daadwerkelijk openbaar gemaakt zijn. Rond dezelfde tijd was er nog een rapport van een Britse kliniek die te maken had met een datalek en die een afpersingsverzoek van thedarkoverlord ontving. Een niet-gespecificeerde hoeveelheid gegevens werd naar verluidt gestolen, zoals persoonsgegevens en pre- en postoperatieve foto's. Net als in het eerste geval waren er geen aanwijzingen dat de gegevens openbaar gemaakt zijn.

Dit zijn slechts twee voorbeelden van de vele aanvallen van thedarkoverlord gericht op de gezondheidszorg. Hoewel er geen details bekend zijn over de hoeveelheid data die jaarlijks gestolen wordt, is het wel duidelijk dat ze doelen op het gebruik van zero-day exploits in RDP-servers (Remote Desktop Protocol).

Datalekken

Datalekken kunnen langdurige gevolgen hebben voor organisaties en individuen. Denk bijvoorbeeld aan het enorme datalek dat plaatsvond bij Yahoo in 2016. Deze enorme lekken zien we ook in de gezondheidszorg. Eind vorig jaar heeft de website ‘Have I Been Pwned’ ongeveer vier miljoen records van Maleisische websites toegevoegd aan de databank. Deze gegevens zijn waarschijnlijk in 2012 verkregen van diverse bedrijven, waaronder bedrijven in de gezondheidszorg. Deze data omvat persoonsgegevens zoals fysieke adressen, Burgerservicenummers en inloggegevens. De gegevens zijn te downloaden op via een verborgen dienst en zijn zeer waarschijnlijk gebruikt door verschillende cybercriminelen voor kwaadaardige doeleinden. Denk bijvoorbeeld aan social engineering en identiteitsdiefstal.

De vier principes

Bovenstaande voorbeelden laten zien dat juist de zorgsector kampt met cybercriminaliteit. Gelukkig is er inmiddels een vaccin voor de griep, maar wat kan de sector doen om zich ook te wapenen tegen cyberdreigingen? Het begint met een diepgaande strategie, geleid door vier principes:

- Gebruik host-based firewalls en neem IP-whitelist maatregelen
- Segmenteer het netwerken en beperk onderlinge communicatie tussen werkstations
- Voer patches direct uit en schakel onnodige verouderde functies uit
- Beperk de toegang tot belangrijke gegevens tot alleen diegenen die deze écht nodig hebben

Maar er is meer nodig om een organisatie te beschermen. Digitale risico’s omvatten namelijk niet alleen cyberdreigingen en gegevenslekken (merkinformatie, informatie over infrastructuur), maar ook risico’s van derden, fysieke dreigingen en nog veel meer. Deze bedreigingen en risico’s kunnen vaak niet worden gedetecteerd met een enkele oplossing, soms zelfs niet door meerdere oplossingen.

In de gegeven voorbeelden van afpersingsaanvallen en inbreuken was het monitoren van sociale media een mogelijk preventiemiddel. Op basis van vermeldingen van uw bedrijf en IP-adressen kan worden bepaald of uw bedrijf een doelwit is (geweest). Zo ja, dan kunt u proactief uw security opschroeven en op gerichte plekken versterken. Daarnaast biedt het monitoren van het dark web mogelijk interessante informatie over profielen van afpersers en de acties die ze mogelijk gaan ondernemen.

Kortom: een aanpak van monitoring in combinatie met een diepgaande securitystrategie, geeft een compleet beeld van de actuele dreiging. Het helpt u op weg om het afweersysteem een boost te geven. Zo bent u voorbereid op het volgende griepseizoen.