Cyberaanval bij Attent

In februari werd Attent, als eerste VVT-organisatie in Nederland, slachtoffer van een cyberaanval door een ransomeware-groep. Dit maakte dat we tegen lastige praktische situaties aanliepen. Zo waren we slecht bereikbaar en konden we geen gebruik maken van onze computersystemen. Gelukkig zijn onze financiële-, personele- en clientsystemen daarbij niet getroffen en hebben we de zorg kunnen leveren zoals onze cliënten dat van ons gewend waren.

Toen duidelijk was dat het ging om een ransomeware-aanval hebben we direct een melding gedaan bij de politie, de Autoriteit Persoonsgegevens (AP) en de Inspectie voor Gezondheid en Jeugd. Op dat moment konden we namelijk niet overzien of de veiligheid van onze cliënten in gevaar zou komen. Het expertisecentrum voor cybersecurity in de zorg Z-CERT adviseerde ons om een specialist op het gebied van cybercriminaliteit in te schakelen.
We vormden een kernteam met een vertegenwoordiging van de zorg, de techniek, communicatie en bestuurlijk. In onze interne en externe communicatie hebben we direct openheid van zaken gegeven zodat er geen misinformatie zou ontstaan en hebben gewerkt met Q&A's die we steeds actualiseerden.

Met behulp van de cyberexpert hadden we vrij snel zicht op de door de hackers aangerichte schade. De applicaties in de cloud waren niet geraakt en we konden binnen een paar dagen gefaseerd weer gebruik maken van deze applicaties.
De expert onderhield contact met de hackers en dat leverde ons meer inzicht op in de beperkte hoeveelheid gestolen gegevens. Hackers letten bij het stelen van gegevens op kopieën van identiteitsgegevens en op documenten met een vertrouwelijk karakter.
Zodra we wisten welke identiteitsgegevens gestolen waren, hebben we de betrokkenen via een aangetekende brief geïnformeerd en de geste gedaan om een nieuw paspoort te kopen.
We konden een expert inschakelen die in staat was om onze back-ups bijna volledig beschikbaar te maken. Ook is het ons, met ondersteuning van andere professionals, gelukt om onze mailserver bijna volledig te herstellen, inclusief alle mailhistorie. Dit maakte dat het onderhandelen met de hackers steeds minder van waarde werd en we hebben dan ook niet betaald.

Reacties

Over het algemeen hebben we veel support ontvangen, onder andere vanuit de regio waarin Attent actief is. Daarnaast toonden veel organisaties belangstelling omdat wij de eerste VVT-organisatie in Nederland waren die werd getroffen door een cyberaanval. Ook wij hebben steeds gezegd dat het niet de vraag is óf maar meer wanneer je door een dergelijke aanval wordt getroffen. Wij hebben kunnen vaststellen dat de aanval is gedaan via een gestolen account met een sterk wachtwoord. De oorzaak hiervan kan zijn dat er gereageerd is op phishing of fishing mails. Dit laat zien dat de kwetsbaarheid in een klein hoekje zit.

Cyberaanval bij Attent
vervolg

Het laatste kwartaal van 2023 hebben we onder de medewerkers een awareness campagne gehouden over informatieveilig werken. Wij hebben van de AP complimenten ontvangen over onze transparante, goede en doelgroepgerichte communicatie.
De melding is door de AP gesloten, omdat ze vertrouwen hadden in de opvolging.

"Moed en vertrouwen is nodig om samen over de angst heen te stappen als er iets misgaat." – Cliëntadviseur Attent

"De gevolgen van een cyberaanval zoals wij hebben ervaren raakt mensen emotioneel. Pas nu realiseer ik mij echt heel goed wat deze heftige vorm van criminaliteit teweeg kan brengen voor de persoonlijke levenssfeer van mensen." – Functionaris gegevensbescherming

"Gelukkig zijn we de periode van cyberaanval meer dan goed doorgekomen. Attent bleef zorgen. De 'techniekers' van Attent hebben ons er doorheen geleid. Onzichtbaar achter hun schermen, bijna klokje rond wekenlang ervoor zorgend dat er uiteindelijk weer gezorgd kon worden zoals we het gewend waren." – Directeur Zorg

Impact

Deze crisissituatie heeft veel impact gehad, zowel op medewerkers als de organisatie. Niet kunnen werken zoals je gewend bent, en de onzekerheid over de mate waarin het netwerk kan worden hersteld, creëert onzekerheid. Dat was op veel plekken in de organisatie voelbaar. Door steeds via updates te communiceren en door het samenstellen van een routekaart hebben we een poging gedaan om de organisatie mee te nemen in de weg die we af wilden leggen.

Er zijn ook positieve punten. Een crisis van deze omvang voedt de samenhorigheid. Doordat we al jaren investeren in onze cultuur, met als belangrijke waarde 'Ik zie, ik hoor je', konden we elkaar steeds een hart onder de riem steken en bij elkaar stil staan. Het appèl op ons vakmanschap hebben we omarmd.
Cliënten hebben weinig last ondervonden van de cyberaanval. De sfeer op de locaties was rustig en we hadden snel afspraken gemaakt over hoe we de continuïteit van zorg konden waarborgen. Uit de locaties kwamen zelfs signalen dat – nu er minder mogelijkheid was om de verantwoordingen achter de computer te doen – er meer tijd overbleef voor activiteiten met cliënten en familie.
We hebben een aantal medewerkersbijeenkomsten georganiseerd. Daarin was enerzijds ruimte voor emoties en anderzijds konden we de feiten delen. Deze bijeenkomsten werden goed bezocht. De aanpak en saamhorigheid zorgden voor rust in de organisatie.