



Succesvolle samenwerking versterkt security en compliance bij Pluryn

Samenvatting

Zorgorganisatie Pluryn wenste de compliance en security van de organisatie te verhogen.

Wat begon als een vraag over licenties, groeide uit tot een uitgebreid project met een focus op beveiligingstechnologieën. Dankzij de samenwerking met Insight en Microsoft zijn beide aspecten nu succesvol verbeterd, middels:

- Diverse workshops en assessments ter bevordering van de beveiliging en compliance
- Microsoft 365 E5 Security met Microsoft Sentinel



Cybersecurity

Achtergrond

Pluryn biedt ondersteuning aan jongeren en volwassenen met complexe problematiek, zoals verstandelijke beperkingen en gedragsproblemen. Met meer dan 6.400 professionals en 650 vrijwilligers ontvangen cliënten passende hulp bij wonen, werken, leren en vrije tijd, bij voorkeur thuis of in de wijk. IT is een belangrijk ondersteunend middel voor de organisatie. Ingegeven door de Europese NIS2-richtlijn, die essentiële organisaties verplicht tot goede cybersecurity, wilde Pluryn de security en compliance optimaliseren.

Uitdaging

De zorginstelling schakelde mede op aanraden van Microsoft hun licentiepartner Insight in om weloverwogen keuzes te kunnen maken en voor de nodige ondersteuning.

Rob Leijssen, IT-beheerder bij Pluryn: "Onze zorginstelling levert 24/7 zorg en loopt daardoor continu risico. Beveiliging was altijd al belangrijk, maar NIS2 verplicht ons straks om ernstige incidenten binnen 24 uur te melden, wat de druk op onze IT-afdeling vergroot. Het Insight NIS2-evenement toonde ons hun kennis van cybercriminaliteit, met focus op de zorgsector, de AVG en NIS2. De grootste uitdaging daarbij is de balans vinden tussen beveiliging en werkbaarheid. Samen met Insight onderzochten we wat noodzakelijk is en hoe dit in te richten."

"Hoe streng kan de beveiliging zijn zonder de werkzaamheden van medewerkers te hinderen? Bij de invoering van multifactor-authenticatie stuitte we al eens eerder op bezwaren, omdat medewerkers de app niet op hun privétoestel wilden of konden gebruiken. Hoe gaan we hier nu mee om? Insight helpt hierbij om allereerst de basis optimaal te krijgen."

Rob Leijssen, IT-beheerder bij Pluryn

“De druk op onze IT-afdeling is groot en beveiliging is een belangrijk onderdeel. Als zorgorganisatie hebben we 24/7 zorgverantwoordelijkheid en daardoor ook 24/7 risico’s. Met NIS2 komt daar nu ook de meldingsplicht binnen 24 uur bij.”

Rob Leijssen, IT-beheerder bij Pluryn



Oplossing & Resultaat

Om de IT-afdeling van Pluryn te kunnen ondersteunen, werden een aantal stappen gezet. Samen met Microsoft werd er een nulpunt bepaald.

“De invoering van NIS2 zet bij veel organisaties alles op scherp. Het is hierbij belangrijk om te zorgen dat de basis eerst goed op orde is. Samen met Microsoft werd er een Threat Protection Assessment bij Pluryn gedaan, om het nulpunt te bepalen, om van daaruit adviezen te kunnen doen en te gaan bouwen. Via diverse workshops en een POC met zowel Microsoft 365 E5 Security en Microsoft Sentinel zijn we samen met hen tot vervolgstappen gekomen,” zegt Joon Bronsgeest, Executive Account Manager Healthcare bij Insight.

“Pluryn is een grote zorgorganisatie, met ruim 45 werknemers op IT. Beveiliging is echter zo specifiek, daar zijn specialisten voor nodig en we zien steeds meer organisaties daarvoor een beroep doen op Insight. Voor de basis werd gekozen om het bestaande Microsoft 365-pakket te upgraden naar E5. Met dit pakket zijn ze verzekerd van optimale databeveiliging, endpoint security en identiteits- en toegangsbeheer,” vult Dirk de Goede, Security Solution Specialist bij Insight, aan. “Daar bovenop is gekozen voor Microsoft Sentinel en dat gaat de IT-afdeling vooral helpen incidenten snel te signaleren, waardoor ze er ook snel melding van kunnen maken.”

Waarom Insight?

In Insight heeft Pluryn de waardevolle securitykennispartner gevonden die ze nodig hadden. Samen met hen hebben ze een duidelijke keuze kunnen maken voor extra security, mede dankzij de nodige workshops en assessments.

Het project was uniek door Insight’s diepgaande kennis, open communicatie en proactieve houding. Ze reageerden snel, zetten extra stappen, waardoor we ze echt die betrouwbare partner zijn. Ze geven ons de veiligheid en ondersteuning die we nodig hebben en waardoor wij ons kunnen focussen op het optimaal uitrollen van E5 en de adoptie onder medewerkers,” besluit Rob Leijssen.

KEY RESULTS

Optimale beveiliging

Optimale compliance

Kennispartner

Sparringspartner