Orange
Cyberdefense

Customer stories

SOC van Orange Cyberdefense is cyberverzekering voor P&V Groep



- Beter inzicht in de risco's
- Ontzorging van system engineers
- Lagere werklast voor intern IT-team
- Geruststelling door bewezen expertise

Security-uitdaging in sterk digitaliserende verzekeringssector

De P&V Groep is een coöperatieve verzekeringsgroep die al meer dan 100 jaar actief is op de Belgische markt. De verzekeringsoplossingen worden via een netwerk van agenten en makelaars verdeeld onder verschillende merken: Vivium, Actel, Arces en P&V Verzekeringen. In totaal telt de groep zo'n 1.700 medewerkers. De ambitie van de groep is om verzekeringsproducten te leveren die afgestemd zijn op de verschillende noden van zowel de particuliere en zelfstandige klant als bedrijven en instellingen.

De digitalisering biedt de verzekeringssector vandaag opportuniteiten om aan die noden te voldoen met nieuwe diensten en nieuwe gebruikservaringen. Denk maar aan het doorsturen van foto's via een app om een schadedossier aan te vullen of het openstellen van portals waar de klant zijn eigen dossier kan opvolgen. Maar de sector ontsnapt daarbij niet aan de uitdagingen. Zo beschikken verzekeringsmaatschappijen over heel veel vertrouwelijke informatie van de klanten – tot hun medische achtergrond – wat hen een interessant doelwit maakt voor cybercriminelen. "We werken met gevoelige data én we zitten in de financiële sector: dat maakt ons een geliefd doelwit voor phishing attacks, CEO-fraude of ransomware-aanvallen", verduidelijkt Krist Cappelle, Information Security Program Manager voor P&V Groep. Security is daarom heel belangrijk. Niet alleen de interne mensen op de hoofdzetel, maar ook de diverse agenten moeten op een zo veilig mogelijke manier met die data om springen. "Maar veel communicatie in onze sector verloopt nog via de klassieke manier op papier of via e-mail. Een online portal is interessanter, omdat je daar een stuk communicatie binnen de eigen beveiligde omgeving doet."

Daarnaast brengt het cloudverhaal voor P&V Groep nieuwe security-uitdagingen met zich mee die betrekking hebben op authenticatie en rechtenbeheer. Ook het belang van IT-security in audits wordt steeds belangrijker. "We krijgen meerdere controles en audits per jaar van diverse instellingen: het FSMA, de Nationale Bank, en een eigen auditafdeling."



> “Cybersecurity is als een brandverzekering. Je betaalt die jarenlang en vindt het weggegooid geld, totdat je ze nodig hebt. Dan ben je blij dat je een verzekering hebt.”

Krist Capelle | Information Security Program Manager voor P&V Groep

Oplossing via SOC

De digitalisering, het cloudverhaal, de strenge regels in verband met authenticatie en controles, … brengen veel security logs met zich mee. Een oplossing vinden om die vele logs beter te beheren en af te handelen was de directe aanleiding voor P&V Groep om een oplossing te zoeken. De vorige oplossingen creëerden wel veel logs, maar er waren niet genoeg mensen om die allemaal op de juiste momenten op te volgen. “Daarom keken we uit naar een partner die ons hierbij kon helpen via een Security Operations Center of kortweg SOC”, aldus Krist Cappelle.

Als criteria stelde P&V Groep een aantal voorwaarden. Zo moest het in eerste instantie één complete oplossing zijn die zowel Windows, Linux als mainframe kon behelzen. Een tweede vereiste was dat de informatie bruikbaar moest zijn voor de system engineers die de oplossingen moesten vinden voor de foutmeldingen en anomalieën in de beveiliging die de logs melden. Maar ook voor het management moest de informatie van het SOC inzichtelijk zijn om een strategische visie te kunnen ontwikkelen en de nodige IT-initiatieven te ondersteunen. “Via duidelijke rapporten moet het management kunnen zien hoe matuur de P&V Groep is op vlak van IT-security, hoeveel aanvalspogingen er zijn geweest, zonder daarbij te veel in technische details te vervallen.”

P&V zette toen een RFP in de markt in 2020 en nadat het proces doorlopen was, kwam Orange Cyberdefense als meest interessante partij uit de bus. De kostprijs en de uitgebreide kennis van de verschillende technologieën speelden zeker in het voordeel van Orange Cyberdefense. Krist Cappelle: “Het belangrijkste punt waarop Orange Cyberdefense echter een verschil maakte, was dat zij een soort SOC van de tweede generatie voorstelden. Niet allen puur geautomatiseerd maar ook een batterij securityspecialisten die direct met voorstellen als oplossing komen.”

Samenwerking en voordelen

Het SOC is sinds 2021 actief en zit extern bij Orange Cyberdefense. De belangrijkste systemen zijn intern gelinkt met de SOC van Orange Cyberdefense. Een data lake met een hoop ongestructureerde data, alle logs van load balancer, firewalls, … Die worden bekeken door de specialisten Orange Cyberdefense. “Concreet bekijkt Orange Cyberdefense alle logs in detail en filtert ze. Ze sturen vervolgens enkel de zaken door die we moeten bekijken. Als een bekende gebruiker inlogt, sturen ze dit niet door (tenzij dit vanop een vreemde locatie is), maar als bijvoorbeeld een onbekende gebruiker 17 maal tracht in te loggen op 10 minuten tijd, dan geven ze wel alarm”, zegt Krist Cappelle.

De samenwerking verloopt goed met meetings op diverse niveau en daaraan aangepast op verschillende termijnen en doelen. Krist Cappelle “Ze weten wie ze voor wat moeten aanspreken en zijn zeer dynamisch in hun aanpak. Zo zijn er tijdens project regelmatig momenten geweest waarop planning en agenda moest worden bijgestuurd onder meer door een fundamentele koerswijziging op vlak van ons datacenter. Orange Cyberdefense heeft daar heel flexibel op gereageerd. Het voordeel van Orange Cyberdefense is dat ze al diepgaande kennis hebben van de verzekeringssector. Doordat ze opgenomen zijn in een groter geheel is er intern ook veel meer kennis aanwezig en krijg je op elke vraag een antwoord.”

Op technologisch vlak zit de meerwaarde van Orange Cyberdefense en het SOC voornamelijk in een beter zicht hebben op de risico’s. Tickets die binnenkomen zijn van betere kwaliteit – waar vroeger veel ‘afval’ was, is nu wat binnenkomt belangrijk – dus is er minder werklast. Het ontzorgt de system engineers die zich nu kunnen focussen op andere business development gerelateerde zaken. “Kunnen terugvallen op de knowhow en expertise van Orange Cyberdefense geeft ons ook geruststelling”, aldus nog Krist Cappelle.



Resultaat

Het resultaat is dat de system engineers weten dat de logs die ze nu krijgen, direct moeten bekeken worden. “Naast een beter zicht op de activiteiten op en rond onze IT-omgeving hebben we ook een veiligere omgeving door de proactiviteit en eerste analyse door het SOC. Bovendien levert dit tijdswinst op onder meer omdat false positives gefilterd worden.”

Security is een topic dat op het hoogste niveau in de organisatie wordt bekeken. Er is veel budget, wat ook vraagt om concrete resultaten. Voor het management was de meerwaarde pas na de eerste rapporten duidelijk. “Als verzekeringsgroep krijgen we continu aanvallen, maar tot nu toe zijn ze er nog niet in geslaagd om binnen te dringen. De rapporten van het SOC maken dat ‘zichtbaar’. Want in onze sector (IT-security) is je werk maar goed gedaan als je ‘onzichtbaar’ bent. Dankzij het SOC kunnen we dat bewijzen en rapporteren. We kunnen aangeven of we nog mee zijn met de ontwikkelingen en nog beveiligd zijn tegen aanvallen zoals in de media verschijnen.

Het SOC biedt vooral zekerheid dat we de risico’s beperken en IT-rampen voorkomen. Doordat het SOC je dit helpt te verhinderen, blijf je uit de media en blijft je reputatie als solide partner overeind. Zeker in de verzekeringswereld is dat cruciaal. Ook naar klanten toe”, zegt Krist Cappelle over de businessvoordelen. “

In dat opzicht is cybersecurity als een brandverzekering. Je betaalt ze jaarlijks en vindt het misschien weggegooid geld. Tot je huis afbrandt. Dan ben je blij dat je over zo’n verzekering beschikt.

De toekomst

Twee jaar geleden tekende het IT-team van P&V Groep een security roadmap tot 2024 uit. Dit heeft geholpen om het management ervan te overtuigen dat security nodig is en er altijd zal in geïnvesteerd moeten worden. “Die roadmap omvatte verschillende domeinen: technische aspecten, een risicoanalyse en security framework, De volgende stap in het plan is security awareness verhogen bij de medewerkers en de makelaars”, besluit Krist.

Over Orange Cyberdefense

Orange Cyberdefense is de deskundige cybersecurity business unit van de Orange Group. Als Europa’s go-to security provider streven zij naar een veiligere digitale samenleving. Zij zijn een threat research en intelligence-driven security provider die ongeëvenaarde toegang biedt tot huidige en nieuwe dreigingen.

Orange Cyberdefense heeft meer dan 25 jaar ervaring op het gebied van informatiebeveiliging, 250+ onderzoekers en analisten, 16 SOC’s, 10 CyberSOC’s en 4 CERT’s verspreid over de hele wereld en verkoop- en dienstenondersteuning in 160 landen. Zij zijn er trots op dat ze met lokale expertise wereldwijde bescherming kunnen bieden en hun klanten gedurende de hele levenscyclus van een bedreiging kunnen ondersteunen.