



Cas client

Le SOC d'Orange Cyberdefense est la cyberassurance pour le Groupe P&V



Défis liés à la sécurité dans un monde des assurances en pleine digitalisation

Le Groupe P&V est un groupe d'assurance coopératif, actif sur le marché belge depuis plus de 100 ans. Les solutions d'assurance sont distribuées via un réseau d'agents et de courtiers sous différentes marques: Vivium, Actel, Arces et P&V Assurances. Au total, le groupe emploie quelque 1.700 collaborateurs. Il nourrit l'ambition de fournir des produits d'assurance adaptés aux différents besoins des clients particuliers et indépendants ainsi que des entreprises et des institutions.

La digitalisation offre au secteur des assurances l'opportunité de répondre à ces ambitions avec de nouveaux services et de nouvelles expériences utilisateurs. L'envoi de photos via une app pour compléter un dossier de sinistre ou l'ouverture de portails où le client peut suivre son dossier en sont de bons exemples. Le secteur n'échappe toutefois pas aux défis. Les compagnies d'assurance disposent de nombreuses informations confidentielles sur leurs clients (jusqu'à leurs antécédents médicaux), ce

qui en fait une cible intéressante pour les cybercriminels. « Nous travaillons avec des données sensibles et nous sommes actifs dans le secteur financier : cela fait de nous une cible privilégiée pour les attaques de phishing, les fraudes au CEO ou les attaques de ransomware », explique **Krist Cappelle, Information Security Program Manager pour le Groupe P&V**. La sécurité est donc essentielle. Tant le personnel interne qui travaille au siège que les divers agents doivent traiter ces données de la manière la plus sûre possible. Mais dans notre secteur, la communication se déroule encore largement de manière traditionnelle sur papier ou par e-mail. Un portail en ligne, auquel nous travaillons actuellement, est plus intéressant, car une partie de la communication se fait alors dans un environnement propre et sécurisé. »

De plus, le cloud pose au Groupe P&V de nouveaux défis de sécurité liés à l'authentification et à la gestion des droits. Sans oublier la sécurité informatique qui gagne en importance dans les audits. « Nous recevons plusieurs contrôles et audits par an de diverses institutions : la FSMA, la Banque nationale et notre propre service d'audit », précise Krist Cappelle.



- Meilleure vue sur les risques
- Charge de travail allégée pour l'équipe informatique interne
- Tickets de bien meilleure qualité
- Tranquillité d'esprit grâce à une expertise éprouvée
- Soulagement des ingénieurs systèmes



« La cybersécurité est comme une assurance incendie. On la paie pendant des années en pensant qu'il s'agit d'argent jeté par les fenêtres, jusqu'à ce qu'on en ait besoin. Là, on est heureux d'être assuré. »

**Krist Capelle |
Information Security
Program Manager
pour le Groupe P&V**

Solution via le SOC

La digitalisation, le cloud, les règles strictes en matière d'authentification et de contrôles... Autant d'éléments donnant lieu à de nombreux registres journaux de sécurité. P&V s'est mis en quête d'une solution pour mieux les gérer et les traiter. Les solutions existantes créaient surtout de nombreux registres journaux de sécurité, mais il n'y avait pas assez de personnel pour en assurer le suivi au moment opportun. « C'est la raison pour laquelle nous nous sommes mis à la recherche d'un partenaire capable de nous aider avec un Security Operations Center ou SOC », explique Krist Cappelle.

Le Groupe P&V a fixé plusieurs critères. La solution devait tout d'abord pouvoir englober Windows, Linux et le mainframe. Une deuxième exigence était que les informations devaient être utilisables par les ingénieurs systèmes en charge de trouver des solutions aux messages d'erreur et aux anomalies de sécurité signalés par les registres journaux. Mais les informations du SOC devaient également être accessibles à la direction afin de développer une vision stratégique et de soutenir les initiatives informatiques nécessaires. Krist Cappelle : Grâce à des rapports clairs, la direction doit pouvoir constater le degré de maturité du Groupe P&V en matière de sécurité informatique et le nombre de tentatives d'attaques, sans trop entrer dans les détails techniques.

P&V a lancé un appel d'offres en 2020, à l'issue duquel Orange Cyberdefense s'est révélé être le partenaire le plus intéressant. Le prix et la connaissance approfondie des différentes technologies ont joué un rôle non négligeable. « Orange Cyberdefense s'est surtout démarqué de ses concurrents en proposant une espèce de SOC de deuxième génération. Purement automatisé, mais aussi avec une batterie de spécialistes en sécurité qui font directement des propositions et suggèrent des solutions », se souvient Krist Cappelle.

Collaboration et avantages

Actif depuis 2021, le SOC est externe à Orange Cyberdefense. Les principaux systèmes sont reliés en interne au SOC. Un lac de données est alimenté avec beaucoup de données non structurées, tous telles que les journaux des commutateurs, les registres des répartiteurs de charge, des pare-feux... Le tout est examiné par les spécialistes d'Orange Cyberdefense. « Concrètement, Orange Cyberdefense examine en détail et filtre tous les registres journaux de sécurité », explique Krist Cap. « Le SOC nous envoie ensuite uniquement les éléments que nous devons examiner. Si un utilisateur connu se connecte, le SOC ne nous en fait pas part, sauf si la connexion se fait depuis un endroit inhabituel. Mais si, par exemple, un utilisateur inconnu essaie de se connecter 17 fois en 10 minutes, le SOC donne l'alerte. »

La collaboration se passe bien, avec des réunions à différents niveaux, adaptées aux divers délais et objectifs. Krist Cappelle : « Les experts d'Orange Cyberdefense savent à qui s'adresser pour quelles questions. Ils sont aussi très dynamiques dans leur approche. Pendant le projet, le planning et l'agenda ont dû être régulièrement ajustés, notamment en raison d'un changement fondamental de cap dans notre centre de données. Orange Cyberdefense a réagi avec beaucoup de souplesse. De plus, Orange Cyberdefense a déjà une connaissance approfondie du secteur des assurances, ce qui représente un atout de taille. Comme ils font partie d'un plus grand groupe, ils disposent de beaucoup de connaissances en interne, ce qui permet d'obtenir une réponse à chaque question. »

Sur le plan technologique, la plus-value d'Orange Cyberdefense et du SOC réside surtout dans une **meilleure vision des risques**. Comme les tickets qui arrivent sont de meilleure qualité – avant il y avait beaucoup de 'déchets', mais ce qui arrive aujourd'hui est important – **la charge de travail est réduite**. Cela soulage les ingénieurs systèmes qui peuvent désormais



se concentrer sur d'autres aspects axés sur le développement des activités. « Grâce à la taille du groupe, Orange Cyberdefense est en mesure de garantir des connaissances quelque part dans le monde pour résoudre chaque problème. Nous pouvons donc nous adresser à eux pour toutes nos technologies installées. Le fait de pouvoir s'appuyer sur le savoir-faire et l'expertise d'Orange Cyberdefense nous permet également d'avoir l'esprit tranquille », se réjouit Krist Cappelle.

Résultat

Au final, les ingénieurs systèmes savent que les registres des journaux de sécurité qu'ils reçoivent maintenant doivent être examinés immédiatement. « En plus d'avoir une meilleure vue sur les activités relatives à notre environnement informatique, nous disposons d'un environnement plus sûr grâce à la proactivité et à une première analyse réalisée par le SOC. Cela nous permet en outre de gagner du temps, notamment parce que les faux positifs sont filtrés. »

La sécurité est un sujet examiné au plus haut niveau au sein de l'organisation. Le budget est considérable, ce qui requiert également des résultats concrets. Pour la direction, la plus-value n'est apparue clairement qu'après les premiers rapports. « En tant que groupe d'assurance, nous faisons en permanence l'objet d'attaques, mais jusqu'à présent, personne n'est encore parvenu à s'infiltrer dans nos systèmes. Les rapports du SOC permettent de 'visualiser'

cela. Car dans le domaine de la sécurité informatique, le travail n'est bien fait que lorsqu'on est 'invisible'. Grâce au SOC, nous sommes en mesure de le prouver et de le signaler. Nous pouvons indiquer si nous sommes toujours au courant des développements et si nous sommes toujours protégés contre les attaques pointées par les médias. Le SOC nous offre surtout l'assurance de limiter les risques, et d'éviter les désastres informatiques. Et de ne pas faire les choux gras des médias, tout en préservant notre réputation de partenaire robuste. Cet aspect est crucial, surtout dans le monde des assurances. Egalement, vis-à-vis des clients », ajoute Krist Cappelle.

A cet égard, la cybersécurité est comme une assurance incendie. On la paie pendant des années en pensant qu'il s'agit d'argent jeté par les fenêtres. Jusqu'au jour où la maison brûle et qu'on est heureux d'être assuré.

L'avenir

Il y a deux ans, l'équipe informatique du Groupe P&V a élaboré une roadmap de la sécurité jusqu'en 2024. Cela a contribué à convaincre la direction de la nécessité de la sécurité et du besoin d'investir en permanence dans ce domaine. « La roadmap couvre différents domaines : aspects techniques, analyse des risques et cadre de sécurité. La prochaine étape de ce plan consiste à sensibiliser davantage les collaborateurs et les courtiers à la sécurité », conclut Krist Cappelle.

Orange Cyberdefense

Orange Cyberdefense est l'entité du groupe Orange spécialisée en cybersécurité. En tant que prestataire de sécurité de référence en Europe, nous mettons tout en oeuvre pour bâtir une société numérique plus sûre. Nous sommes un prestataire de services de sécurité pilotée par les données et d'analyse de la menace, procurant une vision inégalée des menaces existantes ou émergentes. Orange Cyberdefense jouit d'une expérience de plus de 25 ans dans le domaine de la sécurité de l'information, emploie plus de 250 chercheurs et analystes dans 16 SOC, 10 CyberSOC et 4 centres CERT répartis dans le monde entier ainsi que des équipes commerciales et de support dans 160 pays. Nous sommes fiers de pouvoir affirmer que nous proposons une protection globale avec une expertise locale et que nous assurons le support de nos clients tout au long du cycle de vie des menaces.