proofpoint.

TÉMOIGNAGE CLIENT

AGRAVIS confie la protection des réseaux critiques de ses solutions agricoles à Proofpoint

Le défi

- Renforcer la sécurité de la messagerie et réduire les faux positifs
- Protéger les collaborateurs et les données des menaces internes
- Actualiser constamment les bonnes pratiques de sécurité pour s'adapter à l'évolution du paysage des menaces

La solution

- Proofpoint Enterprise Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Email Fraud Defense (EFD)
- Proofpoint Security Awareness Training (PSAT)
- Proofpoint Insider Threat Management (ITM)

Les résultats

- Augmentation de la productivité de la petite équipe informatique grâce à la réduction des faux positifs
- Technologie étayée par de bonnes pratiques améliorées à l'aide de formations de sensibilisation à la sécurité informatique

L'entreprise

Le commerce agricole fait partie d'un secteur bien particulier. AGRAVIS Raiffeisen AG occupe une place de leader sur ce marché. Basée en Allemagne, l'entreprise fournit un large éventail de produits à ses partenaires de distribution coopérative, aux agriculteurs et aux habitants des zones rurales. En parallèle, elle propose des services de conseil et met à profit ses connaissances étendues et sa vaste expérience. Mais pour protéger ses données et répondre aux besoins du marché en constante évolution, l'entreprise avait besoin d'une solution de cybersécurité de pointe.

Le défi

Sécuriser une plate-forme de messagerie d'entreprise mise à jour

AGRAVIS propose des produits dédiés à la culture de plantes, des aliments pour le bétail, des technologies et machines agricoles, et bien plus encore. Face à la croissance de ses activités, il était essentiel pour l'entreprise de préserver la sécurité et l'intégrité de son infrastructure réseau et de ses données. Pour assurer la sécurité de son personnel, de ses clients et de ses données, AGRAVIS a chargé cinq professionnels de l'informatique de la protection de ses 6 300 collaborateurs. Comme la plupart des entreprises, AGRAVIS n'a eu de cesse de faire évoluer et de mettre à niveau son infrastructure afin de répondre aux besoins émergents du marché. Mais lorsque l'entreprise a commencé à rencontrer des problèmes avec sa passerelle de sécurité de la messagerie, elle y a vu l'opportunité de mettre à jour ses communications et de renforcer son niveau de sécurité.

« Notre nouvelle stratégie informatique impliquait le passage à Microsoft 365 et Microsoft Exchange Online pour la messagerie d'entreprise », explique David Wydrinna, ingénieur en sécurité chez AGRAVIS. « Toutefois, nous rencontrions des problèmes avec notre passerelle de sécurité de la messagerie sur site à Münster, notamment des performances médiocres, des perturbations et des temps d'arrêt sans raison apparente. Nous avons donc procédé à une validation de concept (PoC) avec les principaux fournisseurs afin d'identifier la solution de protection de la messagerie la plus à même de répondre à nos besoins. »

La solution

Proofpoint offre une protection complète et évolutive de la messagerie
Après avoir évalué plusieurs options dans le cadre de sa PoC, AGRAVIS a opté pour une solution de protection de la messagerie complète et intégrée signée Proofpoint. Proofpoint Email Protection protège le personnel des dernières menaces véhiculées par la messagerie, y compris le phishing d'identifiants de connexion, les ransomwares et la fraude par email. La solution tire parti de l'apprentissage automatique et d'une protection multicouche pour identifier et neutraliser les emails malveillants. Par ailleurs, Proofpoint Threat Response Auto-Pull (TRAP) permet à l'équipe de sécurité informatique d'analyser les emails et de mettre les messages malveillants en quarantaine après leur remise.

« L'un des principaux avantages de la solution réside dans la capacité du serveur TRAP à identifier les emails qui sont passés entre les mailles du filet, puis à les supprimer automatiquement des données de boîte aux lettres », explique Patrick Hemsing, ingénieur en sécurité chez AGRAVIS.

« La solution Proofpoint est un atout majeur. Grâce à elle, nous identifions les attaques de phishing et de spam bien plus efficacement qu'avec notre ancienne solution. Elle nous a permis de réduire le nombre de menaces qui atteignent nos endpoints réseau d'environ 95 %. »

David Wydrinna, ingénieur en sécurité, AGRAVIS

Pour renforcer la protection de l'environnement de messagerie cloud de l'entreprise, Proofpoint Targeted Attack Protection (TAP) utilise des techniques statiques et dynamiques afin de procéder à un sandboxing et à des analyses en vue de détecter les menaces dès les premières étapes de la chaîne d'attaque.

« La fonctionnalité de sandboxing a été l'un des principaux facteurs de différenciation lorsque nous avons comparé différentes solutions dans le cadre de notre PoC », affirme l'ingénieur en sécurité. « Proofpoint offrait également un niveau de stabilité supérieur et une facilité d'utilisation accrue par rapport aux autres solutions. »

Bon nombre de menaces de sécurité sont d'origine interne, qu'elles soient dues à la malveillance, à la négligence ou au manque de connaissances des collaborateurs. Pour garantir la protection de l'entreprise, l'équipe informatique d'AGRAVIS a déployé Proofpoint Insider Threat Management (ITM). Cette solution met en corrélation les activités des utilisateurs et les mouvements de données. Elle permet à l'équipe d'évaluer avec précision les risques posés par les utilisateurs, de détecter les compromissions d'origine interne et d'intervenir rapidement en cas d'incident.

Les résultats

Meilleure visibilité sur le niveau de sécurité et réaffectation du personnel aux tâches prioritaires
Proofpoint offre à AGRAVIS la protection contre les menaces dont l'entreprise a besoin pour préserver la sécurité de ses processus métier stratégiques. En parallèle, il automatise les processus et réduit les faux positifs dont le traitement demandait beaucoup de temps au personnel.

« Avec notre ancienne solution, nous rencontrions des problèmes au quotidien », explique Patrick Hemsing. « Chaque jour, 50 emails étaient placés en quarantaine, et un membre du personnel devait passer plusieurs heures à les analyser manuellement afin de déterminer s'il s'agissait de spam, d'une attaque de spear phishing ou d'une erreur d'appliance. Avec Proofpoint, nous n'avons plus à le faire. Nous disposons donc de plus de temps pour nous consacrer à d'autres tâches. »

Grâce à son partenariat avec Proofpoint, AGRAVIS bénéficie également de l'assistance d'un conseiller de confiance qui peut lui fournir des renseignements supplémentaires sur les menaces, ce qui permet d'orienter les priorités et les décisions de l'entreprise en matière d'informatique.

« Nous avons reçu un appel de notre responsable de la réussite client Proofpoint, qui nous a indiqué le nombre d'emails de phishing que la solution avait interceptés et, pour la première fois, nous avons pu en informer notre DSI », se réjouit l'ingénieur en sécurité. « Le responsable nous a transmis un document reprenant toutes nos configurations, des statistiques sur les attaques dont nous n'avions pas connaissance, ainsi que des conseils sur les points à améliorer à l'avenir. »

Les solutions Proofpoint sont conçues pour évoluer, et AGRAVIS est déjà en passe d'étendre sa solution. L'entreprise a décidé de déployer Proofpoint Email Fraud Defense (EFD), qui simplifie l'authentification DMARC (Domain-based Message Authentication, Reporting & Conformance), en vue d'empêcher la fraude et de protéger son domaine de confiance. En outre, Proofpoint EFD surveille et analyse les rapports d'investigation numérique DMARC, ce qui fournit des informations à AGRAVIS sur la façon de bloquer les emails malveillants qui usurpent des domaines.

AGRAVIS a également décidé de proposer des formations PSAT (Proofpoint Security Awareness Training) à ses collaborateurs afin de les tenir informés du paysage des menaces en constante évolution. Face à l'évolution des attaques, l'entreprise souhaite s'assurer que ses collaborateurs restent toujours au fait des bonnes pratiques les plus récentes. Son niveau de sécurité devrait ainsi s'en trouver renforcé.

« Auparavant, la configuration manuelle d'une telle campagne pouvait nous prendre quatre semaines », explique David Wydrinna. « Désormais, avec PSAT, nous pouvons le faire en quelques minutes seulement. »

Grâce aux solutions et services Proofpoint qu'elle a déployés, l'entreprise est convaincue qu'elle conservera une longueur d'avance sur les menaces de sécurité émergentes.

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.