



Advanced Threat Protection: Une entreprise de technologie étend son partenariat avec Retarus

Le leader du marché des technologies dont le siège social se trouve en Allemagne développe, produit et vend une large gamme de technologies de l'information, de la communication et de la sécurité pour les secteurs privé et public. Employant environ 11 000 personnes dans plus de 70 pays, cette entreprise enregistre un chiffre d'affaires de 2 milliard d'euros.

LE CONTEXTE **Une relation de confiance bâtie au fil des années**

Cette entreprise de technologie fait partie des principaux fournisseurs mondiaux de technologies de mesure, technologies de la télévision et de l'audio, technologies radio et cybersécurité. Elle compte parmi ses clients des entreprises privées, par exemple dans l'industrie automobile, mais aussi des fournisseurs d'infrastructures critiques, des services de recherche, des établissements d'enseignement, des organismes d'état et des forces armées. Depuis dix ans, cette société protège efficacement son infrastructure contre les virus, les spams et autres programmes malveillants à l'aide de quatre scanners antivirus déployés parallèlement par Essential Protection, une solution éprouvée de Retarus Email Security. Face à la prolifération croissante des menaces avancées, le service informatique de la société a décidé d'étendre la sécurité des 16 000 boîtes de messagerie de ses employés ainsi que de ses boîtes de messagerie fonctionnelles. Pour ce faire, elle a ajouté à Essential Protection la solution Advanced Threat Protection (ATP) ainsi que la technologie brevetée de Retarus Patient Zero Detection (PZD)®.

L'OBJECTIF **Protection contre les menaces avancées**

EN plus du flux incessant des spams et e-mails porteurs de virus, que Retarus Essential Protection combat efficacement, le service informatique enregistre de plus en plus de menaces complexes, telles que les attaques de hameçonnage et d'ingénierie sociale. Son objectif était donc de prévenir efficacement ces menaces avancées en augmentant le niveau de protection, tout en évitant autant que possible de surcharger le service informatique en lui imposant de nouvelles tâches, car celui-ci était déjà en train de migrer de Lotus Notes/ Domino vers Microsoft Exchange. Ainsi, la condition préalable était que toute

solution de sécurité de messagerie déployée, notamment Advanced Threat Protection, puisse fonctionner de manière fiable en combinaison avec les deux systèmes de messagerie. En outre, il fallait que la solution de sécurité soit évolutive et flexible afin que les succursales et nouvelles sociétés acquises puissent être rattachées depuis n'importe quel endroit du monde. Enfin, la sécurité après défaillance et la protection des données jouent un rôle crucial dans l'entreprise qui compte des clients pour lesquels la sécurité est un enjeu capital.

” *En Retarus, la société technologique a un partenaire fiable et de longue date dans le domaine de la sécurité du courrier électronique. Grâce à nos services fiables et innovants, l'entreprise dispose également d'une protection optimale contre les menaces avancées et les attaques d'ingénierie sociale sur son personnel. Lors de la validation du concept, nous avons travaillé en étroite collaboration avec le client pour adapter les services à ses besoins, et continuer à optimiser le service en permanence dans le cadre de la gestion des services de Retarus.*

Miriam-Carena Schmitt, Vice President Expert Sales D-A-CH, retarus GmbH

LE DÉFI **Ajustement continu des systèmes**

Retarus Advanced Threat Protection (ATP), qui inclut la fonction CxO Fraud Detection ainsi qu'un système de sandboxing fourni par notre partenaire Palo Alto, a fait l'objet d'un essai de preuve de concept (PoC) initial de quatre semaines. L'entreprise a également choisi la technologie brevetée de Retarus Patient Zero Detection® pour se protéger. Ce service permet l'identification rapide des programmes malveillants les plus insidieux (patient zéro) lorsqu'ils sont parvenus à pénétrer dans l'infrastructure de l'entreprise malgré les mécanismes sophistiqués d'ATP, puis alerte immédiatement les administrateurs et les utilisateurs. Le processus de PoC a été suivi de près par les experts de sécurité de Retarus qui ont procédé à une coordination et à un ajustement continu du système. Les résultats intermédiaires ont été analysés avec les différents contacts de l'entreprise de technologie et des ajustements ont été effectués toutes les semaines. Suite à un debriefing positif, l'entreprise a choisi de continuer à utiliser les services de Retarus, en conservant les optimisations et ajustements apportés lors du PoC.

UTILITÉ ET AVANTAGES **Optimisation renforcée grâce à Retarus Service Management**

L'entreprise de technologie a opté pour une solution de sécurité comprenant les composants Essential Protection, Advanced Threat Protection et Patient Zero Detection® de Retarus Email Security. Elle dispose ainsi d'une protection complète partout dans le monde et son service informatique se voit soulagé de tout fardeau supplémentaire. Des connexions redondantes avec le centre de données propre de Retarus à Munich et un centre de données exploité par Retarus à

Francfort-sur-le-Main permettent de garantir la conformité du service avec les niveaux de sécurité après défaillance prévus dans le SLA ainsi que toutes les exigences de l'entreprise en matière de sécurité et de protection des données. Lors du PoC, les services de Retarus ont été étroitement alignés et adaptés aux besoins de l'entreprise. Grâce à Retarus Service Management, que l'entreprise a également retenu, le département informatique bénéficie d'une optimisation continue du service. Un interlocuteur dédié de Retarus coordonne les demandes de service et assistance et se charge de la gestion des escalades, le cas échéant. Lors d'appels et de rapports de service mensuels, des mesures et recommandations d'optimisation supplémentaires sont décidées et les tickets d'assistance sont examinés et documentés.

CONCLUSION ET PERSPECTIVES

Continuité des services à l'échelle mondiale

MAvec Retarus Email Security, l'entreprise de technologie dispose à présent d'un service cloud s'intégrant en toute transparence dans l'infrastructure de communication en pleine évolution et fonctionnant conformément aux réglementations européennes strictes en matière de protection des données. Le service, qui inclut désormais le composant Advanced Threat Protection avec le système de sandboxing et la fonction CxO Fraud Detection, ainsi que la technologie brevetée de Retarus Patient Zeo Detection®, remplit les exigences essentielles de conformité et de continuité des opérations, tout en proposant une structure de coûts transparente. Les services de Retarus peuvent aisément être étendus de manière à couvrir sans difficulté les boîtes de messagerie de succursales et de nouvelles sociétés acquises à travers le monde. Grâce à la preuve de concept mise en place en amont et à l'acquisition de l'option Service Management, les services de Retarus répondent précisément et constamment aux besoins de l'entreprise.

ÉLÉMENTS CLÉS

-  **Détection fiable des nouvelles variantes de virus et de malwares**
-  **Protection améliorée contre l'ingénierie sociale**
-  **Identification efficace des destinataires de patients zéros**
-  **Alertes instantanées**
-  **Rapports et analyses détaillés**
-  **Personnel informatique interne soulagé**