« Fraude au président », hameçonnage, ransomware – Une protection robuste contre les menaces complexes: Retarus Advanced Threat Protection

Le défi

De nos jours, les messages indésirables représentent la majeure partie des courriers électroniques : en plus du flux habituel d'e-mails contenant des spams et des virus, les entreprises et les employés sont de plus en plus exposés à des menaces complexes telles que l'ingénierie sociale et les tentatives de hameçonnage. Face à ces e-mails individuels, les mécanismes traditionnels de sécurité n'offrent pas de protection suffisamment efficace. En outre, les programmes malveillants sont également modifiés à des intervalles de plus en plus courts et de nouvelles variantes ne cessent de se développer.

Le contexte

Lorsqu'elles apparaissent pour la première fois, les nouvelles menaces qui pèsent sur les antivirus sont naturellement inconnues. Comme il n'existe toujours pas de signatures appropriées, les e-mails infectés se propagent en très peu de temps. En plus de cette dynamique, les cybercriminels utilisent des méthodes de plus en plus sophistiquées dans le but d'avoir accès à des informations sensibles. Les solutions de sécurité traditionnelles ont du mal à distinguer ce type d'e-mails des messages légitimes. Les attaques réussies entraînent non seulement de graves pertes de données et des défaillances massives du système, mais également d'énormes coûts et une atteinte à la réputation de la victime. Il est donc urgent pour les entreprises d'adapter leurs concepts de sécurité informatique à la situation actuelle.

La solution

Le paquet **Essential Protection** de **Retarus Email Security** accède déjà à des mécanismes de protection complets et jusqu'à quatre antivirus différents, filtrant la majorité des e-mails dangereux de manière fiable. Avec **Advanced Threat Protection** (ATP), les entreprises peuvent se protéger contre les menaces qui vont au-delà des virus traditionnels et des spams grâce à une foule de fonctionnalités supplémentaires.

Avantages pour le client

- Protection des communications commerciales sensibles
- Sécurité informatique à l'épreuve du temps
- Prévention des pertes financières dues à la fraude
- Sensibilisation des employés à l'hameçonnage et autres méthodes de fraude
- Protection contre les atteintes à la réputation dues à la perte de données

Les avantages en un coup d'œil

- Détection fiable de nouvelles variantes de virus et de programmes malveillants
- Protection avancée contre l'ingénierie sociale et autres menaces complexes
- Analyse via des sources de données spécialisées et leurs propres algorithmes
- Rapports et analyses détaillés
- Intégration transparente des autres services e-mail de la plate-forme Retarus

Cas pratique

Les attaquants recourent de plus en plus à l'ingénierie sociale pour réaliser des attaques qui comportent un risque de préjudice financier pour les entreprises. Par exemple, dans le cas de la « fraude au président », les cybercriminels se font passer pour le PDG d'une entreprise et font appel à leurs victimes dans de faux e-mails pour qu'ils transfèrent de grosses sommes d'argent. La **CxO Fraud Detection** de Retarus permet de reconnaître à temps les fausses adresses d'expéditeurs utilisées pour ces attaques ciblées et de prévenir les employés à propos des faux e-mails. En plus d'une analyse avancée de l'en-tête de l'e-mail, des algorithmes spécialisés sont également utilisés pour identifier de manière fiable ce qu'on appelle le « From-Spoofing » et le « Domain-Spoofing » (usurpation d'identité de domaine ou de provenance).

Retarus Time-of-Click Protection peut également être utilisé pour prévenir les attaques à l'hameçonnage et la perte de données sensibles qui en découle. Cette technologie contrôle tous les liens contenus dans les e-mails à la recherche d'adresses cibles suspectées d'hameçonnage. Tout d'abord, tous les liens dans les e-mails entrants sont automatiquement réécrits (« URL Rewriting »). À chaque fois que les destinataires cliquent sur un lien de ce type, une seconde vérification est effectuée. Si de nouvelles informations sur la page cible située derrière le lien sont rendues disponibles entre-temps, elles sont bloquées, et l'utilisateur reçoit un avertissement de sécurité.

Afin de mieux protéger les entreprises contre les programmes malveillants en constante évolution tels que les ransomwares, Retarus Advanced Threat Protection inclut également un **Deferred Delivery Scan** et une analyse approfondie de **Sandboxing**. Le Deferred Delivery Scan consiste en une ré-analyse différée des pièces jointes sélectionnées. Pour cela, la livraison de l'e-mail est retardée de quelques minutes : en effet, après un court instant, une nouvelle analyse peut déjà détecter des signatures de virus mises à jour qui n'étaient pas encore disponibles au moment de la première analyse. Le Sandboxing, également proposé dans le cadre de l'Advanced Threat Protection, permet d'exécuter les pièces jointes dans un environnement de test virtuel et sécurisé avant la livraison et de repérer un comportement inhabituel en utilisant des procédures de simulation complexes.

Le saviez-vous ?

Plus de 390 000 nouveaux programmes malveillants sont enregistrés chaque jour dans le monde. Cela représente une moyenne de 270 nouvelles variantes de virus par minute.

Autres scénarios

Postdelivery Protection

La technologie innovante de **Retarus Patient Zero Detection®** détecte les e-mails dangereux qui ont déjà été envoyés. En cas de suspicion, les destinataires et les administrateurs sont immédiatement informés afin d'éviter des dommages plus importants.

Chiffrement sécurisé

Les données sensibles ne doivent jamais tomber entre de mauvaises mains. Avec **Retarus Email Encryption** (prend en charge les chiffrements PGP, OpenPGP et S/MIME), les entreprises peuvent protéger la confidentialité de leurs communications et facilement mettre en œuvre les lois relatives à la protection des données en vigueur.

Email Live Search

Dans le cadre de Retarus Essential Protection, **Email Live Search** offre une analyse rapide de la livraison des emails. De cette manière, votre équipe d'assistance peut suivre en détail à quel moment quel e-mail a traversé quel point de l'infrastructure, et quels filtres de sécurité lui ont été appliqués.