Détection fiable des programmes malveillants et informatique légale efficace avec Retarus Patient Zero Detection®

Le défi

Les mesures de protection simples ne suffisent plus. Les nouveaux virus qui attaquent quotidiennement l'infrastructure des entreprises par e-mail sont trop nombreux. Une fois que le programme malveillant est entré dans le réseau, il est important de limiter au maximum les dégâts. Ce n'est que par l'identification rapide des destinataires affectés (appelés « patients zéro ») à l'aide de l'informatique légale que des contre-mesures peuvent être prises en temps utile pour éviter des perturbations majeures. En même temps, les paramètres du système doivent être optimisés en permanence afin d'offrir une protection complète contre les menaces futures.

Le contexte

Malheureusement, les spams, virus ou attaques de hameçonnage ciblées constituent la majorité des e-mails. 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. Les solutions Email Security filtrent généralement les messages infectés de manière fiable. Cependant, même les meilleurs filtres antivirus ne peuvent offrir une protection efficace à 100 %. En effet, lorsque de nouveaux logiciels malveillants apparaissent pour la première fois, leur signature est encore inconnue. C'est pourquoi de nombreuses entreprises utilisent des antivirus installés localement ou des solutions de Sandboxing complexes en plus des solutions cloud. Mais même dans ce cas, les administrateurs et les destinataires de nouveaux virus n'apprennent souvent leur existence que lorsqu'il est déjà trop tard et que le programme malveillant a déjà causé du tort. En outre, l'origine généralement inconnue de l'attaque rend l'informatique légale extrêmement difficile.

La solution

Les services **Retarus Email Security** vous protègent contre les attaques de logiciels malveillants grâce à une protection antivirus multicouche, des filtres anti-spam et anti-hameçonnage intelligents et un bloqueur de pièces jointes unique. L'analyseur à quatre couches de Retarus, par exemple, offre déjà un très haut niveau de protection en filtrant environ 35 % de virus de plus que les solutions de protection antivirus classiques qui n'utilisent que deux scans. En combinaison avec la technologie brevetée **Retarus Patient Zero Detection®**, les entreprises peuvent protéger encore mieux leur infrastructure contre les attaques et détecter les programmes malveillants inconnus.

Avantages client

- Protection maximale de l'infrastructure informatique
- Réponse rapide aux attaques
- Simplification de l'informatique légale
- Communication d'entreprise efficace
- Optimisation durable du système

Détail de vos avantages

- Détection fiable des destinataires de programmes malveillants initialement non détectés
- Alerte immédiate
- Livraison par e-mail sans délai
- Rapports et analyses détaillés
- Intégration transparente avec **Retarus Enterprise Email Encryption**

Cas pratique

Les services **Retarus Email Security** accèdent en parallèle à plusieurs antivirus, dont les règles de filtrage sont continuellement mises à jour, ce qui permet à Retarus de repousser de manière fiable la majorité des programmes malveillants. La technologie innovante **Patient Zero Detection®** de Retarus identifie également les e-mails dangereux qui ont déjà été envoyés, facilitant ainsi l'informatique légale. À cette fin, dès que l'e-mail est reçu, une empreinte digitale numérique de toutes les pièces jointes est générée et stockée dans une base de données de l'infrastructure Retarus. Cela n'entraîne donc aucun retard de livraison. Dès qu'un antivirus détecte un code malveillant dans une pièce jointe similaire chez un autre destinataire à une date ultérieure, Retarus compare cette empreinte digitale avec toutes les données stockées dans la base de données. L'e-mail infecté, lui, est immédiatement supprimé. Si la signature correspond à une signature déjà sauvegardée, les administrateurs concernés et éventuellement tous les destinataires précédents en sont immédiatement informés. **Patient Zero Detection® Real-Time Response** permet un traitement des résultats basé sur des règles pour identifier les e-mails potentiellement dangereux dans la boîte aux lettres d'un utilisateur et les déplacer ou les supprimer automatiquement.

Les entreprises peuvent identifier très rapidement les systèmes affectés et prendre les contre-mesures appropriées avant que les virus ne se propagent pas dans le réseau de l'entreprise. L'e-mail infecté peut alors généralement être supprimé avant d'être ouvert. Si une pièce jointe affectée a déjà été exécutée, **Retarus Patient Zero Detection®** facilite l'informatique légale. Des rapports et des analyses détaillés fournissent des indices concrets sur les fichiers qui doivent être analysés pour détecter les virus. Pour mieux protéger le système en cas d'attaques futures, les paramètres de filtrage de **Retarus Email Security** peuvent également être optimisés en permanence sur la base des informations de **Patient Zero Detection®**.

Le saviez-vous ?

Selon Kaspersky, le coût moyen d'une cyberattaque pour les grandes entreprises est d'environ 861 000 $.

Autres scénarios

Chiffrement sécurisé

Les données sensibles ne doivent jamais tomber entre de mauvaises mains. Avec **Retarus Email Encryption**, les entreprises peuvent préserver la confidentialité de leurs communications et facilement mettre en œuvre les lois relatives à la protection des données en vigueur.

Mise en quarantaine intelligente des e-mails

Les digests d'e-mails fournissent rapidement aux entreprises une vue d'ensemble des virus et des spams interceptés. Les e-mails classés comme spam peuvent être mis en quarantaine par des utilisateurs qui n'ont pas accès au portail.

Bloqueur de pièces jointes

Grâce à l'**Attachment Blocker** de Retarus, les entreprises peuvent protéger encore mieux leur infrastructure contre les attaques de programmes malveillants. Cette fonction empêche la réception de tous les types de pièces jointes classés comme non fiables par l'administrateur.