retarus

CxO Fraud, Phishing, Ransomware: Stärkerer Schutz mit Advanced Threat Protection

Die Herausforderung

Ein Großteil der elektronischen Post besteht bereits heute aus unerwünschten Nachrichten: Neben der Flut aus gewöhnlichen Spam- und Viren-Mails sehen sich Unternehmen und Mitarbeiter zunehmend aber auch komplexen Bedrohungen wie Social-Engineering- und Phishing-Angriffen ausgesetzt. Traditionelle Sicherheitsmechanismen bieten vor diesen individualisierten E-Mails oft keinen ausreichenden Schutz mehr. Zudem wird auch Malware in immer kürzeren Zeitabständen abgewandelt und kursiert in stets neuen Varianten.

Die Ausgangssituation

Bei ihrem ersten Auftreten sind neue Bedrohungen für Virenscanner naturgemäß unbekannt. Da noch keine passenden Signaturen vorliegen, breiten sich infizierte E-Mails innerhalb kürzester Zeit aus. Zusätzlich zu dieser Dynamik setzen Cyberkriminelle auf immer raffiniertere Angriffsmethoden, mit denen Betrüger versuchen, an sensible Informationen zu gelangen. Herkömmliche Sicherheitslösungen können solche E-Mails nur schwer von legitimen Nachrichten unterscheiden. Erfolgreiche Attacken führen nicht nur zu folgenschwerem Datenverlust sowie massiven Systemausfällen, sondern auch zu enormen Kosten und Reputationsschäden. Unternehmen müssen ihre IT-Sicherheitskonzepte daher dringend den aktuellen Gegebenheiten anpassen.

Die Lösung

Bereits die Essential Protection der Retarus E-Mail Security greift auf umfassende Schutzmechanismen sowie auf bis zu vier verschiedene Virenscanner zu und filtert somit einen Großteil gefährlicher E-Mails zuverlässig aus. Mit dem erweiterten Schutz der Advanced Threat Protection sichern sich Unternehmen durch zahlreiche zusätzliche Funktionalitäten auch gegen jene Bedrohungen ab, die über klassische Viren und Spam-Mails hinausgehen.

Kundennutzen

- Schutz sensibler Geschäftskommunikation
- Zukunftssichere IT-Security
- Vermeidung finanzieller Schäden durch Betrug
- Sensibilisierung der Mitarbeiter für Phishing & Co.
- Absicherung gegen Reputationsschäden durch Datenverlust

Ihre Vorteile auf einen Blick

- Zuverlässige Erkennung neuer Viren- und Malware-Varianten
- Erweiterter Schutz vor Social Engineering
- Analyse über spezialisierte Datenquellen und eigene Algorithmen
- Detaillierte Reports und Analysen
- Nahtlose Integration anderer E-Mail-Services der Retarus-Plattform

Anwendungsfall

Angreifer nehmen über Social Engineering vermehrt Attacken vor, die für Unternehmen das Risiko finanzieller Schäden bergen. So geben sich Cyberkriminelle bei der Betrugsmasche des CxO Fraud als Geschäftsführer eines Unternehmens aus und fordern ihre Opfer in fingierten E-Mails auf, hohe Geldsummen zu überweisen. CxO Fraud Detection von Retarus ermöglicht es, die für diese zielgerichteten Angriffe verwendeten gefälschten Absenderadressen rechtzeitig zu erkennen und Mitarbeiter vor fingierten E-Mails zu warnen. Dafür kommen neben einer fortschrittlichen Analyse des E-Mail-Headers auch spezialisierte Algorithmen zum Einsatz, die sogenanntes From- oder Domain-Spoofing zuverlässig identifizieren.

Zusätzlich lassen sich mit Retarus Time-of-Click Protection auch Phishing-Angriffe und der damit einhergehende Verlust sensibler Daten verhindern. Die Technologie überprüft alle in E-Mails enthaltenen Links auf Phishing-verdächtige Zieladressen. Dafür werden zunächst alle Links in eingehenden E-Mails automatisiert umgeschrieben („URL Rewriting“). Immer wenn Empfänger einen solchen Link anklicken, wird dieser erneut auf mögliche Schädlichkeit überprüft. Falls zwischenzeitlich neue Erkenntnisse über die dahinterliegende Zielseite vorliegen, wird diese blockiert und dem Nutzer stattdessen eine Sicherheitswarnung angezeigt.

Um Unternehmen vor sich ständig weiterentwickelnder Malware, zum Beispiel Ransomware, besser zu schützen, beinhaltet die Retarus Advanced Threat Protection auch einen so genannten Deferred Delivery Scan sowie eine tiefgehende Sandboxing-Analyse. Beim Deferred Delivery Scan handelt es sich um einen zeitlich verzögerten Re-scan ausgewählter Dateianhänge. Hierfür wird die Zustellung der E-Mail wenige Minuten verzögert: Denn bei einem erneuten Scan können schon nach kurzer Zeit aktualisierte Virensignaturen vorliegen, die bei der ersten Überprüfung noch nicht verfügbar waren. Durch die ebenfalls im Rahmen der Advanced Threat Protection angebotene Sandbox werden Anhänge vor der Zustellung zunächst in einer virtuellen, sicheren Testumgebung ausgeführt und mittels komplexer Simulationsverfahren auf ein ungewöhnliches Verhalten überprüft.

Schon gewusst?

Weltweit werden täglich mehr als 390.000 neue Schadprogramme registriert. Das sind im Durchschnitt rund 270 neue Virenvarianten pro Minute.

Weitere Szenarien

Postdelivery Protection
Die innovative Retarus-Technologie „Patient Zero Detection“ identifiziert gefährliche E-Mails, die bereits zugestellt wurden. Im Verdachtsfall werden Administratoren umgehend informiert, so dass größerer Schaden verhindert werden kann.

Sichere Verschlüsselung
Sensible Daten dürfen keinesfalls in falsche Hände gelangen. Mit Retarus E-Mail Encryption können Unternehmen die Vertraulichkeit ihrer Kommunikation wahren und geltendes Datenschutzrecht problemlos umsetzen.

E-Mail Live Search
Mit E-Mail Live Search liefert Retarus einen Service für die schnelle Analyse der E-Mail-Zustellung. Für jede Nachricht können Ihre Support-Mitarbeiter detailliert nachvollziehen, welche Security-Filter angewendet wurden und wann diese welchen Punkt in der Infrastruktur durchlaufen hat.

© 2018 Retarus Group. All rights reserved.