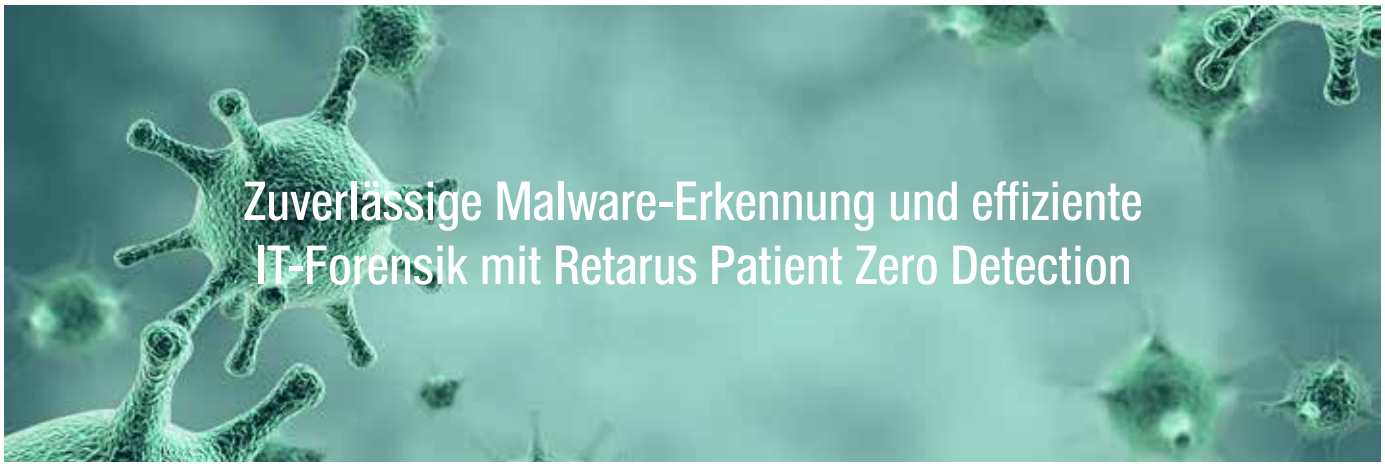
retarus



Zuverlässige Malware-Erkennung und effiziente IT-Forensik mit Retarus Patient Zero Detection

Die Herausforderung

Einfache Schutzmaßnahmen reichen längst nicht mehr aus. Zu groß ist die Anzahl neuer Viren, die täglich per E-Mail die Unternehmensinfrastruktur angreifen. Ist die Malware erst einmal im Netzwerk, gilt es, den Schaden so gering wie möglich zu halten. Nur durch die schnelle Identifizierung betroffener Empfänger, sogenannter Patient Zeros, lassen sich rechtzeitig Gegenmaßnahmen einleiten, um größere Störungen zu verhindern. Gleichzeitig sollten Systemeinstellungen kontinuierlich optimiert werden, um umfassenden Schutz vor zukünftigen Bedrohungen zu bieten.

Die Ausgangssituation

Leider besteht der Großteil der gesamten elektronischen Post aus Spam, Viren oder gezielten Phishing-Attacken. Weltweit werden täglich mehr als 390.000 neue Schadprogramme registriert. Das sind pro Minute im Durchschnitt rund 270 neue Virenvarianten. In der Regel filtern E-Mail-Security-Lösungen infizierte Nachrichten zuverlässig aus. Einen hundertprozentigen Schutz können jedoch auch die besten Virenfilter nicht bieten. Denn beim ersten Auftreten neuer Schadprogramme ist deren Signatur noch unbekannt. Viele Unternehmen setzen deshalb zusätzlich zu Cloud-Lösungen auch lokal installierte Virenscanner oder aufwendige Sandboxing-Lösungen ein. Doch auch in diesem Fall erfahren Administratoren und Empfänger neuartiger Viren häufig erst von deren Existenz, wenn es bereits zu spät ist und die Malware mitunter schon Schaden angerichtet hat. Zudem erschwert der meist noch unbekannte Ursprung des Angriffs die IT-Forensik enorm.

Die Lösung

Die Retarus E-Mail Security Services schützen dank mehrstufigem Virenschutz, intelligenten Spam- und Phishing-Filtern und dem Retarus Attachment Blocker zuverlässig vor Malware-Angriffen. So bietet beispielsweise der bewährte Retarus Vierfach-Scan bereits ein sehr hohes Schutzniveau, indem er rund 35 Prozent mehr Viren herausfiltert als herkömmliche Virenschutzlösungen, die auf nur zwei Scanner zurückgreifen. Durch die Kombination mit Retarus Patient Zero Detection können Unternehmen ihre Infrastruktur noch besser gegen Angriffe absichern und zusätzlich auch zunächst unbekannte Malware erkennen.

Kundennutzen

- Maximaler Schutz der IT-Infrastruktur
- Schnelle Reaktion auf Angriffe
- Erleichterte IT-Forensik
- Effiziente Business-Kommunikation
- Nachhaltige Systemoptimierung

Ihre Vorteile auf einen Blick

- Zuverlässige Erkennung der Empfänger von zunächst unerkannter Malware
- Sofortige Alarmierung
- E-Mail-Zustellung ohne zeitliche Verzögerung
- Detaillierte Reports und Analysen
- Nahtlose Integration mit Retarus Enterprise E-Mail Archive und Retarus E-Mail Encryption

Anwendungsfall

Die Retarus E-Mail Security Services greifen parallel auf mehrere Virenscanner zu, deren Filterregeln kontinuierlich aktualisiert werden, und wehren somit einen Großteil gefährlicher Schädlinge bereits zuverlässig ab. Die innovative Patient-Zero-Detection-Technologie von Retarus identifiziert zusätzlich auch gefährliche E-Mails, die bereits zugestellt wurden. Dazu wird schon beim E-Mail-Eingang ein digitaler Fingerabdruck aller Attachments erzeugt und in der Retarus-Infrastruktur in einer Datenbank hinterlegt. Zeitliche Verzögerungen bei der Zustellung ergeben sich dadurch nicht. Sobald ein Virenscanner zu einem späteren Zeitpunkt bei einem weiteren Empfänger Schadcode in einem gleichartigen Anhang entdeckt, gleicht Retarus diesen Fingerabdruck mit allen in der Datenbank hinterlegten Daten ab. Die infizierte E-Mail selbst wird unmittelbar gelöscht. Wenn die Signatur mit einer bereits abgespeicherten übereinstimmt, werden die jeweils zuständigen Administratoren sowie optional auch alle bisherigen Empfänger umgehend benachrichtigt.

Dank der schnellen Alarmierung sowie der Informationen zum Ursprung des Angriffs und zum Empfängerkreis können Unternehmen betroffene Systeme binnen kürzester Zeit identifizieren und entsprechende Gegenmaßnahmen einleiten, ehe sich die Viren im Unternehmensnetzwerk verbreiten. Der Administrator kann mühelos überprüfen, ob die E-Mail bereits weitergeleitet wurde. Die infizierte E-Mail lässt sich dadurch meist noch rechtzeitig vor dem Öffnen löschen.

Wurde ein betroffenes Attachment bereits ausgeführt, erleichtert Retarus Patient Zero Detection die IT-Forensik. Detaillierte Reports und Analysen liefern konkrete Anhaltspunkte, in welchen Dateien nach Viren gesucht werden muss. Um das System im Falle zukünftiger Angriffe besser zu schützen, lassen sich auf Basis der Patient-Zero-Detection-Informationen auch die Filtereinstellungen von Retarus E-Mail Security kontinuierlich optimieren.

Schon gewusst?

Laut Kaspersky betragen die durchschnittlichen Kosten in Folge eines Cyberangriffs für große Unternehmen rund 861.000 $.

Weitere Szenarien

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.

Intelligente E-Mail-Quarantäne
E-Mail-Digests geben Unternehmen schnell einen Überblick über abgefangene Viren- und Spam-Nachrichten. Als Spam klassifizierte E-Mails können Anwender schnell und ohne Portalzugang aus der Quarantäne anfordern. Für einen optimalen Schutz werden die Nachrichten bei Abruf erneut auf Viren überprüft.

Attachment Blocker
Mit dem Retarus Attachment Blocker können Unternehmen ihre Infrastruktur noch besser gegen Malware-Angriffe absichern. Die Funktion unterbindet den Empfang aller Attachment-Typen, die vom Administrator als nicht vertrauenswürdig eingestuft werden.