kaspersky BRING ON THE FUTURE

Kaspersky Security for Mail Server

So schützen Sie sich vor dem Angriffsvektor Nummer Eins

E-Mails sind der Hauptangriffsvektor, der die IT-Sicherheit von Unternehmen bedroht. Angreifer wenden immer raffiniertere Methoden an, um Unternehmen durch E-Mail-basierte Angriffe zu infiltrieren. Dies kann zu finanziellen, betrieblichen und Reputationsverlusten führen. Nur eine leistungsstarke Sicherheitslösung kann dem entgegenwirken. Zeit, Ihre Resilienz zu optimieren und Ihre Angriffsfläche zu minimieren – so können Sie Ihr Unternehmen zu einem weniger attraktiven und sogar unerreichbaren Ziel für Angreifer machen – unabhängig davon, ob Ihr Unternehmen eine lokale, Cloud- oder hybride E-Mail-Infrastruktur betreibt.

Hauptvektor für Datenschutzverletzungen

- Laut Data Breach Investigation Report (DBIR) von Verizon ist Social Engineering die am häufigsten eingesetzte Methode für Datenverletzungen.
- In dem Bericht heißt es außerdem, dass „...Phishing nach wie vor die wichtigste „Aktionsvariante" bei Sicherheitsverletzungen darstellt, und das schon seit zwei Jahren".

Quelle: Verizon Data Breach Investigation Report

Stärken Sie Ihre Abwehr am Eintrittspunkt Nummer Eins für Angriffe

Die Anwendungen unter dem Dach von Kaspersky Security for Mail Server tragen dazu bei, die Widerstandsfähigkeit gegen E-Mail-basierte Angriffe zu erhöhen. Dies erfolgt durch:

Identifizieren und Herausfiltern verdächtiger oder unerwünschter Mails auf Gateway-Ebene

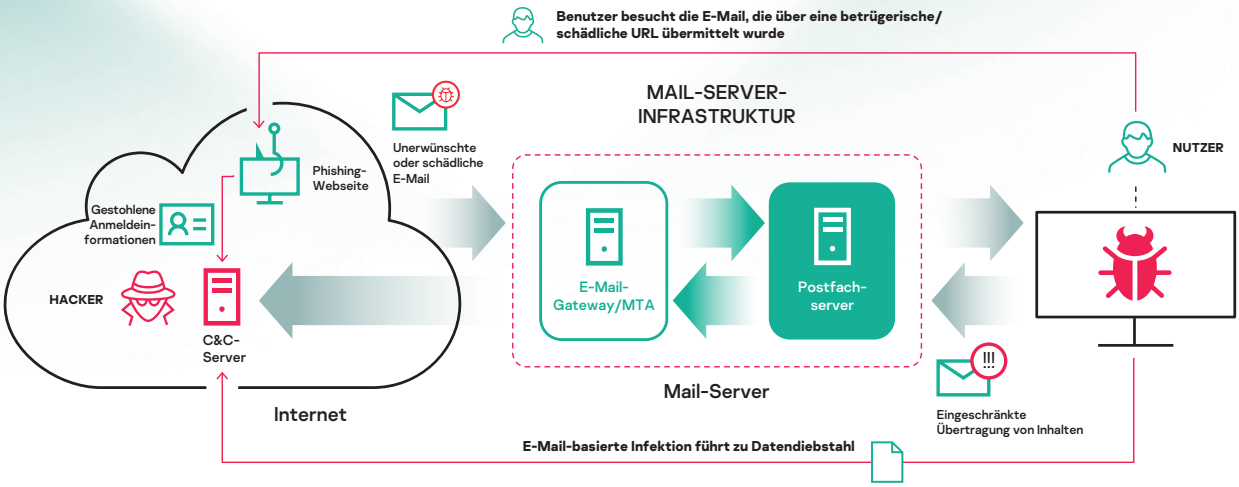
Die meisten Mail-Angriffe beginnen erst auf Endpoint-Ebene – Kaspersky Security for Mail Server stoppt diese, noch lange bevor sie so weit kommen. Unsere vielfach getestete und ausgezeichnete Schutzlösung stärkt die Resilienz Ihres Unternehmens, indem Angriffe gleich zu Beginn der Killchain erkannt und abgefangen werden – noch bevor sie Ihren Sicherheitsbereich durchbrechen und zu Ihren Endpoints und Benutzern vordringen können.

Schnelle und präzise Verarbeitung von seriösen E-Mails

Die zentrale Rolle, die E-Mails in der geschäftlichen Kommunikation spielen, bedeutet, dass die Sicherheitsverarbeitung schnell, agil und genau sein muss – und das ohne die legitime Kommunikation zu beeinträchtigen. Kaspersky Security for Mail Server bietet die effektivsten Schutztechnologien der Branche: Von Phishing-E-Mails und Spam bis hin zu BEC-Angriffen (Business Email Compromise) und Ransomware, mit nahezu null Fehlalarmen. Legitime E-Mails können dabei unterbrechungsfrei weitergeleitet werden.

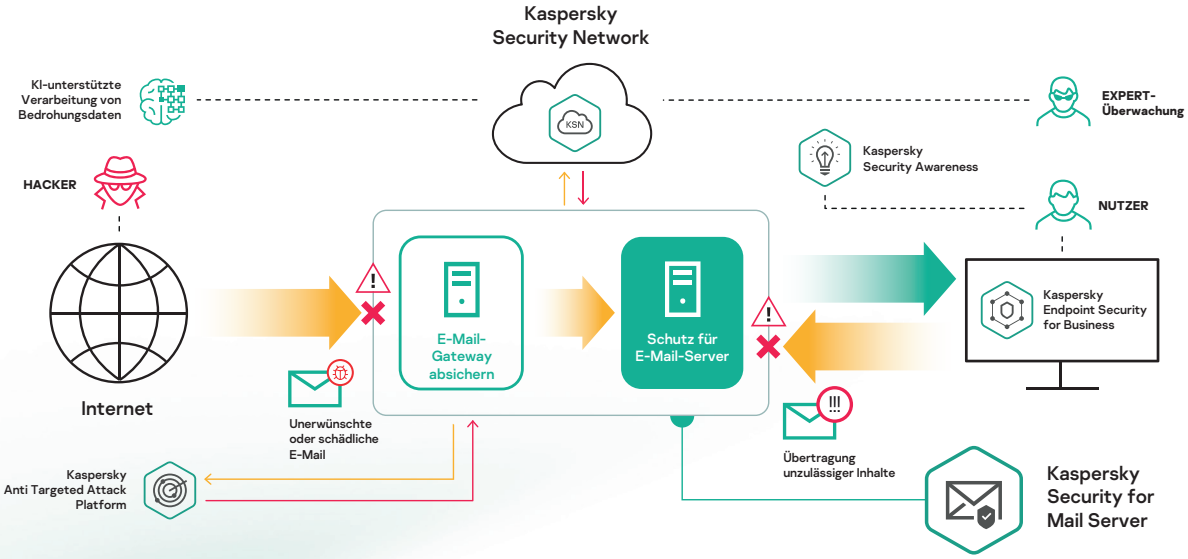
E-Mail-Schutz über das Gateway hinaus

Kaspersky Security for Mail Server erkennt schädliche oder unerwünschte Inhalte nicht nur am Gateway, sondern auch auf der Ebene einzelner Postfächer von Microsoft Exchange Server – oder/und Microsoft Exchange Online. Verzögerte Phishing-Angriffe, die darauf abzielen, Abwehrmaßnahmen auf Gateway-Ebene zu umgehen, BEC-Nachrichten, die nach der Übernahme von Konten generiert werden, und Insider-Bedrohungsszenarien, die gar nicht erst über das Gateway gehen – alle diese Bedrohungen können erkannt und ausgemerzt werden. Dies macht den Schutz von Server-Postfächern zu einem Muss.



Das E-Mail-basierte Bedrohungsmodell

Hauptfunktionen



So schützt Kaspersky Security for Mail Server vor Cyber-Bedrohungen durch E-Mails

Mehrschichtiger Malware-Schutz

Dank mehrerer Sicherheitsebenen kann selbst hochkomplexe, per E-Mail verbreitete Malware gestoppt werden – einschließlich Spyware, Wiper, Miner und Ransomware, die allesamt meist durch gezieltes Phishing verbreitet werden. Reputationsdaten aus der Cloud, präzise Erkennung, lokale und Cloud-basierte ML-Modelle (maschinelles Lernen), weltweit gesammelte Threat Intelligence sowie exklusive Forschungsergebnisse sorgen für eines der besten Verhältnisse zwischen erfolgreicher Erkennung und False Positive-Warnhinweisen in der Branche.

Breite Palette an Szenarien: eine Lizenz für alles

Eine Vielzahl von Szenarien lässt sich mit nur einer Produktlizenz abdecken – so profitieren Sie von höherer Sicherheit Ihrer bestehenden Infrastruktur oder können eine neue, noch sicherere Infrastruktur aufbauen. Zahlreiche E-Mail-Architekturen, darunter auch Linux und Windows, ob lokal, virtualisiert, in der Cloud oder eine Kombination davon – all das wird von einem einzigen Kaspersky-Produkt abgedeckt.

Automatisierte Spam-Abwehr (mit Inhalt und Reputation der Quelladresse)

Der Spam-Schutz von Kaspersky basiert auf intelligenten Engines, die sich kontinuierlich an die veränderten Techniken der Spammer anpassen. So wird die Zahl der Fehlalarme auf ein Minimum reduziert. Global erfasste Reputationsdaten werden in der Cloud verarbeitet und fließen in die KI-Analyse ein, um eine solide Grundlage für eine effiziente Spam-Erkennung zu schaffen.

Countering Business Email Compromise (BEC): Abwehr

Ein dediziertes, auf maschinellem Lernen basierendes Erkennungssystem, dessen algorithmische Modelle regelmäßig mit neuen Szenarien aktualisiert werden, verarbeitet eine Reihe indirekter Indikatoren, so dass das System selbst die überzeugendsten gefälschten E-Mails blockieren kann. Die Unterstützung von Absender-Authentifizierungsmechanismen wie SPF/DKIM/DMARC trägt zum Schutz vor Quellenfälschung bei und ist besonders hilfreich, um BEC-Szenarien standzuhalten.

Sandboxing

Um Systeme selbst vor fortschrittlicher und schwer erkennbarer Malware zu schützen, werden Anhänge in einer sicher emulierten Umgebungen ausgeführt, wo sie im Detail analysiert werden. So kann sichergestellt werden, dass gefährliche Proben nicht ins Unternehmenssystem eindringen. Anwender von Kaspersky Anti Targeted Attack profitieren von der Integration, die eine physische Aktivierung in einer realitätsnahen externen und fortschrittlichen Sandbox-Umgebung unterstützt und somit eine viel detailliertere Bewertung und dynamischere Analyse ermöglicht.

Fortschrittlicher Phishing-Schutz

Das fortschrittliche Anti-Phishing-System von Kaspersky nutzt Analysen von neuronalen Netzwerken für effektive Erkennungsmodelle. Mit über 1.000 verwendeten Kriterien – einschließlich Bildern, Sprachprüfungen und speziellen Skript-Sprachen – wird dieser Cloud-basierte Ansatz durch weltweit gesammelte Daten zu schädlichen und Phishing-URLs sowie IP-Adressen unterstützt. Damit wird umfassender Schutz vor sowohl bekannten als auch unbekannten/Zero-Hour-Phishing-E-Mails ermöglicht.

Blockieren der Übertragung unsicherer Inhalte

Das konfigurierbare Anhangsfiltersystem von Kaspersky kann Dateiverschleierungen erkennen, die häufig von Cyberkriminellen verwendet werden, um potenziell gefährliche Anhänge zu identifizieren. Mithilfe DLP-ähnlicher Funktionen kann der Administrator komplexe Regeln zur Verhinderung von Datenlecks konfigurieren. Ganz nebenbei profitiert er außerdem von einer Fülle von Best Practices aus der Community.

Jenseits des Gateways – Ausfallsicherheit auf Postfach-Ebene

Zu den Technologien auf Postfach-Ebene gehören:

Erneutes Scannen von E-Mails: für Szenarien wie die verzögerte Aktivierung von Phishing-URLs.

Anti-Spam-Schattenquarantäne: ideal für Umgebungen mit geringer Toleranz. Verdächtige E-Mails können in einer vorübergehenden Quarantäne gehalten werden, bis das Kaspersky Security Network genügend Beweise gesammelt hat, um beurteilen zu können, ob die Zustellung definitiv sicher ist.

Transparenz

Eine übersichtliche, benutzerfreundliche und webbasierte Schnittstelle ermöglicht es Ihrem Administrator, den Schutz Ihrer E-Mails zu überwachen, unter anderem mit folgenden Tools:

- Konfigurierbares Dashboard
- Bequeme Ereignisanzeige mit leistungsstarker boolescher Ereignissuche
- Ereignisexport in SIEM-Systeme
- Berichte in der Konsole oder per E-Mail
- Überwachung der Systemintegrität

Skalierung und Resilienz

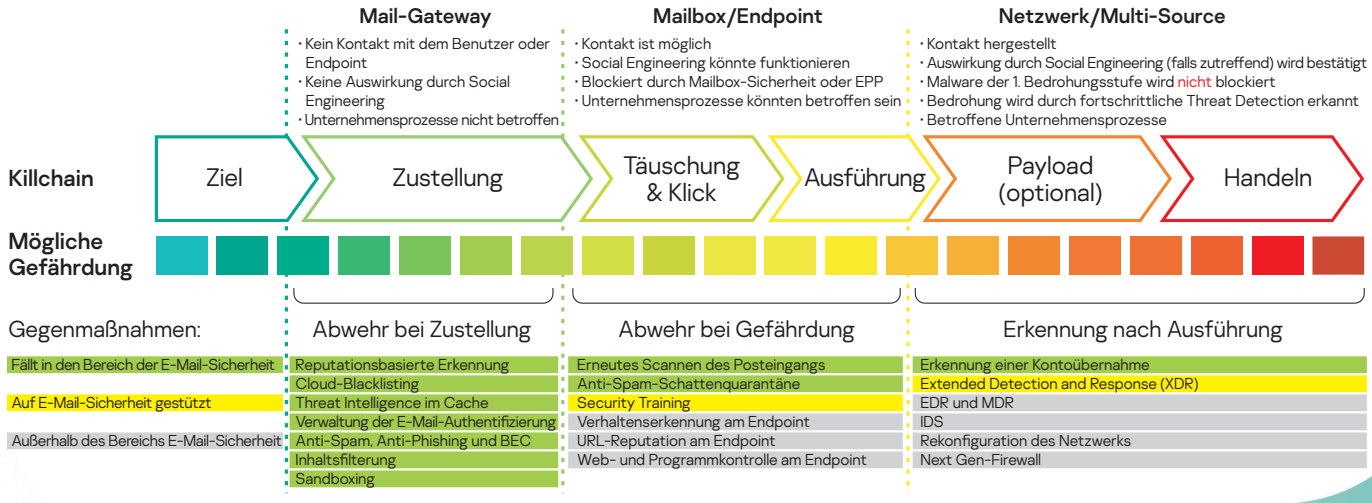
Die Lösung unterstützt Cluster-Architekturen, um dem wachsenden Datenverkehr Herr zu werden und die Resilienz der gesamten Mail-Sicherheit sicherzustellen. Damit kritischen Daten nicht durch Bereinigung, Löschung oder technische Pannen verloren gehen, können Originalnachrichten nach zuvor festgelegten Kriterien gesichert werden, was einen risikofreien Zugriff ermöglicht.

Verwaltung und Zugriffssteuerung

Mithilfe flexibler Regeln kann der Administrator Richtlinien mit unterschiedlich kombinierten Kriterien einrichten und alle Versuche von Verstößen verfolgen. Bei einer zentralen Secure Email Appliance werden spezielle Instrumente zur Konfiguration der nicht sicherheitsrelevanten Aspekte des Systems in derselben Verwaltungskonsole angeboten. Die rollenbasierte Zugriffssteuerung bedeutet, dass separate Administratoren unterschiedlichen Unternehmensbereichen oder Kunden zugewiesen werden können.

Extended Detection & Response

Durch die Integration in Kaspersky Anti Targeted Attack erhalten Sie Zugriff auf eine ganze Reihe von Erkennungstechnologien auf Expertenniveau, wie z. B. eine fortschrittliche Sandbox, eine Analysefunktion für mobile Bedrohungen, spezielle Datenfeeds mit C&C-Daten und vieles mehr. Nach erfolgter Erkennung kann ein gezielter Angriff abgewehrt werden, indem seine Komponenten mithilfe von produktübergreifenden XDR-Szenarien auf unterschiedlichen Infrastrukturebenen aufgespürt, isoliert und letztendlich blockiert werden.



Rolle der E-Mail-Sicherheit in den verschiedenen Phasen der Killchain

Sichern jetzt auch Sie sich mit Kaspersky Security for Mail Server umfassend ab

Kaspersky Security for Mail Server ist nur eine von vielen Kaspersky-Lösungen, die auf unserer mehr als 20-jährigen Erfahrung beruht, von uns selbst auf der Grundlage einer einzigen Codebasis entwickelt wurde und die nahtlos ineinandergreifen. So wird eine umfassende und zuverlässige Sicherheitsplattform geschaffen.

Wenn Sie bereits Kaspersky Endpoint Security for Business einsetzen, können Sie durch die Installation von Kaspersky Security for Mail Server sicherstellen, dass der Schutz Ihres Mail-Gateways die gleichen hohen Leistungsstandards bietet wie der Rest Ihrer Sicherheitsmaßnahmen.

Wenn dies noch nicht der Fall ist, könnte jetzt ein guter Zeitpunkt sein, Ihre Sicherheit zu optimieren: Installieren Sie Kaspersky Security for Mail Server neben oder anstelle Ihres aktuellen E-Mail-Schutzes.

Möglicherweise auch für Sie interessant...

Kaspersky Security for Internet Gateway: ergänzen Sie Ihren E-Mail-Perimeterschutz mit einer ebenso leistungsstarken Web-Gateway-Sicherheitslösung — ebenfalls in Kaspersky Total Security for Business enthalten.

Kaspersky Endpoint Security for Business: Unsere führende Lösung für Endpoint-Sicherheit, die Ihnen häufig getesteten und vielfach ausgezeichneten Endpoint-Schutz bietet.

Kaspersky EDR Optimum: Sorgt für noch mehr Transparenz am Endpoint sowie detaillierteren Informationen über Malware-Erkennungen, ergänzt durch Ursachenanalyse und automatische Abwehroptionen.

Hinweise zum Kauf

Kaspersky Security for Mail Server wird als eigenständige, zielgerichtete Lösung oder als Erweiterung verkauft, die nur für Kunden von Kaspersky Endpoint Security for Business erhältlich ist.

Enthaltene Programme

- Kaspersky Security for Linux Mail Server
- Kaspersky Secure Mail Gateway
- Kaspersky Security for Microsoft Exchange Server
- Kaspersky Security for Cloud Mail

Lizenzierung

Kaspersky Security for Mail Server wird wie folgt lizenziert:

- Jahreslizenz
- Monatliches Abonnement

Kostenlos testen

Kaspersky Security for Mail Server jetzt mit unserer kostenlosen 30-Tage-Testversion.

Kontakt

Sie benötigen weitere Informationen? Gerne kontaktieren wir Sie telefonisch!

Bei unseren Partnern kaufen

Sie möchten die Lösung kaufen? Sicher finden Sie auch einen Partner in Ihrer Region, der Sie hierbei unterstützt.

Cyber Threats News: www.securelist.com
IT Security News: www.kaspersky.de/blog/b2b/
Kaspersky-Technologien: kaspersky.com/technowiki
IT-Sicherheit für SMB: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sicherere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency

Proven. Transparent. Independent.