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 verfügen über immer raffiniertere Methoden, um Unternehmen durch E-Mail-basierte Angriffe zu infiltrieren. Dies kann zu finanziellen, betrieblichen und Reputationsverlusten führen. Um diesen Entwicklungen entgegenzuwirken, müssen Unternehmen sowohl über Widerstandsfähigkeit als auch über Schutz nachdenken. Indem Sie Ihre Sicherheit optimieren und die Angriffsfläche minimieren, können Sie Ihr Unternehmen zu einem weniger attraktiven und sogar unerreichbaren Ziel für Angreifer machen. Und der beste Zeitpunkt für den Einsatz von entsprechenden Gegenmaßnahmen ist, noch bevor unerwünschte E-Mails mit Benutzern und deren Endpoints in Kontakt kommen.

Im Jahr 2019 haben wir **fast eine halbe Milliarde versuchte Phishing-Angriffe blockiert**

Securelist, Spam & Phishing 2019

Stärken Sie Ihre Abwehr am Eintrittspunkt Nummer Eins für Angriffe

Die Anwendungen 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 E-Mails auf Gateway-Ebene

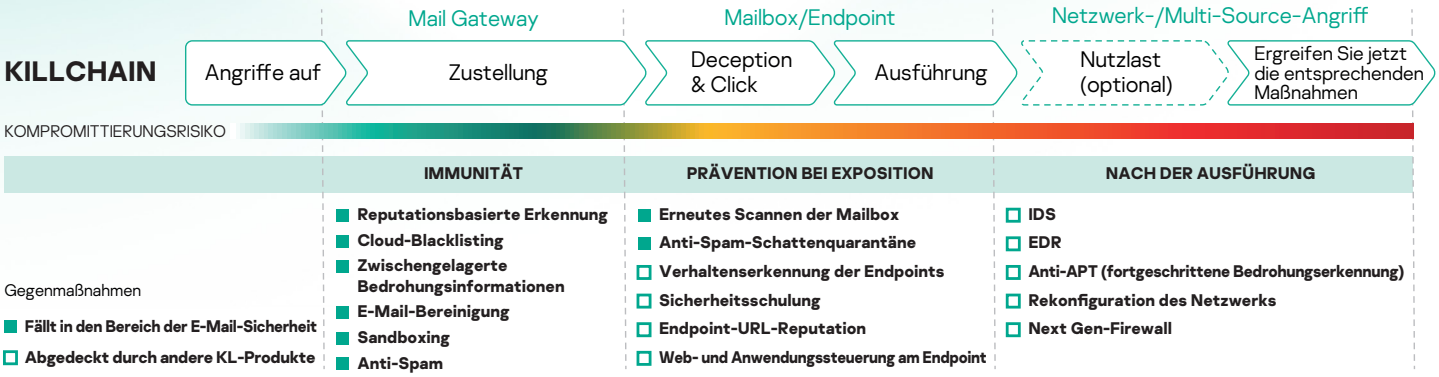
Die meisten Mail-Angriffe werden erst auf Endpoint-Ebene aktiviert – Kaspersky Security for Mail Server setzt alles daran, sie zu stoppen, lange bevor sie so weit kommen. Unser vielfach getesteter und ausgezeichneter Schutz stärkt Ihre Widerstandskraft, indem er Angriffe erkennt und abfängt, noch bevor sie Ihren Sicherheitsbereich durchbrechen und zu Ihren Endpoints und Benutzern vordringen können.

Schnelles und präzises Verarbeiten der Bedrohungen

Die zentrale Rolle, die E-Mails in der geschäftlichen Kommunikation spielen, bedeutet, dass die Sicherheitsverarbeitung schnell, agil und genau sein muss – ohne die legitime Kommunikation zu beeinträchtigen. Kaspersky Security for Mail Server bietet die effektivsten1 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.

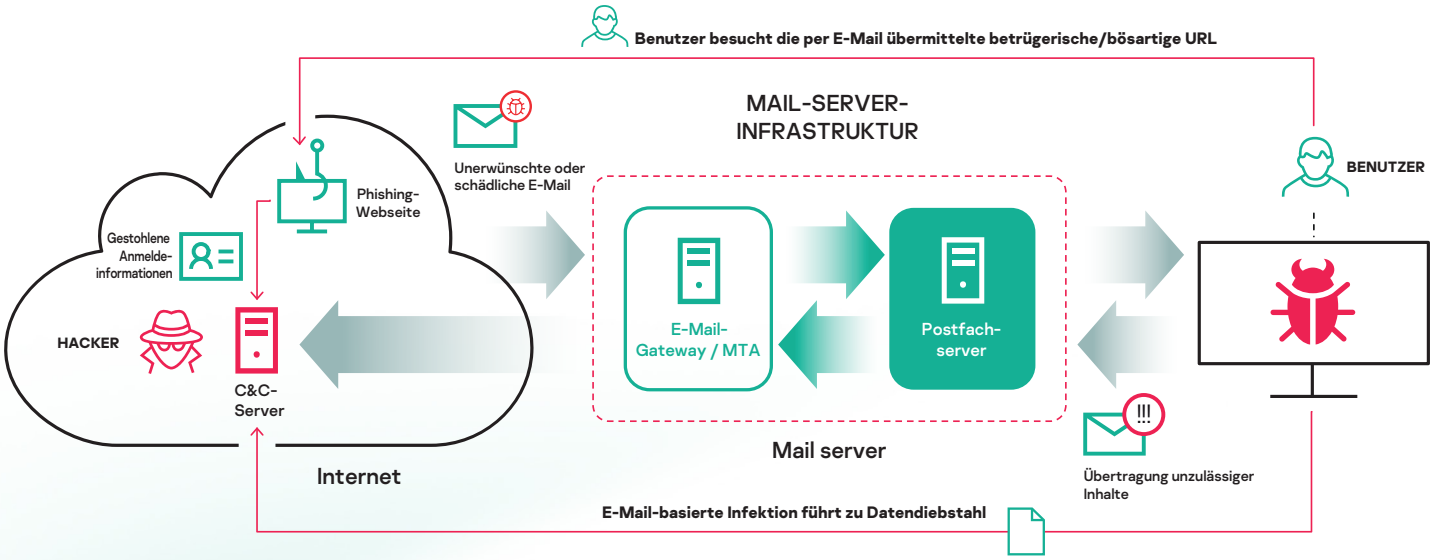
E-Mail-Schutz über den Gateway hinaus

Die Benutzer müssen geschützt werden, auch vor sich selbst – und das Unternehmen muss vor den Folgen von Unwissenheit oder Fehlern der Benutzer geschützt werden. Kaspersky Security for Mail Server erkennt bösartige oder unerwünschte Inhalte auf der Ebene des individuellen Posteingangs und Postausgangs auf Microsoft Exchange Servern – einschließlich Malware, Phishing-E-Mails und potenziell gefährlichen Anhängen, wie es die vom Administrator konfigurierten Richtlinien vorschreiben. Um Kontoübernahme- oder Insider-Bedrohungen einzudämmen, wird ein Schutz auf Posteingangs-Server-Ebene dringend empfohlen.



1 https://www.kaspersky.de/top3

Hauptfunktionen



Das E-Mail-basierte Bedrohungsmodell

Mehrschichtiger Malware-Schutz

Mehrere Sicherheitsebenen, die über tiefgreifende Lernnetzwerke implementiert werden, stoppen die komplexeste per E-Mail übertragene Malware – einschließlich Fällen von gezielter Ransomware, Wipern und Minern, die oft durch Spear-Phishing unterstützt werden. Verhaltensanalysen, Reputationsdaten aus der Cloud und auf Signaturen basierende Engines, Heuristik und Signaturdatenbanken werden mit menschlichem Fachwissen kombiniert, um mehrere Ebenen effektiver Erkennungs- und Präventionsstufen mit minimalen Fehlalarmen zu liefern.

Sandboxing

Um Systeme selbst vor fortschrittlicher und schwer erkennbarer Malware zu schützen, werden Anhänge in einer sicher emulierten Umgebungen ausgeführt. Dort werden sie analysiert, um sicherzustellen, dass gefährliche Proben nicht ins Unternehmenssystem eindringen. Anwender von Kaspersky Anti Targeted Attack profitieren von der vollständigen Integration, die eine physische Aktivierung in einer externen Sandbox-Umgebung unterstützt und somit eine viel detailliertere Bewertung und dynamische Analyse ermöglicht. Ein gezielter Angriff kann dann unterbrochen werden, indem die Übertragung seiner Komponenten blockiert wird.

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

Das Kaspersky Anti-Spam-System verwendet intelligente Engines, um die Möglichkeit von Fehlalarmen zu minimieren und sich an Veränderungen in der Bedrohungslage anzupassen. Zusätzlich erfolgt eine Überwachung durch Experten. Global gesammelte Reputationsdaten werden in der Cloud verarbeitet, um eine solide Grundlage für eine effiziente Spam-Erkennung zu schaffen.

Abwehr von Kompromittierungen von geschäftlichen E-Mails (BEC)

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 Business Email Compromise (BEC)-Szenarien standzuhalten.

Jenseits des Gateways – Ausfallsicherheit auf Mailbox-Ebene

Technologien auf Mailbox-Ebene umfassen:

Erneutes Scannen von E-Mails – Adressierung von Szenarien wie verzögerte Phishing-URL-Aktivierung

Anti-Spam-Schattenquarantäne – ideal für toleranzarme Umgebungen. 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.

Fortschrittlicher Phishing-Schutz

Das fortschrittliche Anti-Phishing-System von Kaspersky basiert auf der Analyse von neuronalen Netzwerken für effektive Erkennungsmodelle. Mit über 1000 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.

Die Übertragung unsicherer Inhalte verhindern

Das konfigurierbare Anhangsfiltersystem von Kaspersky kann Dateiverschleierungen erkennen, die häufig von Cyberkriminellen verwendet werden, um potenziell gefährliche Anhänge zu identifizieren. Die Inhaltsfilterfunktion ermöglicht es dem Administrator, spezielle Regeln zur Verhinderung von Datenlecks zu konfigurieren.

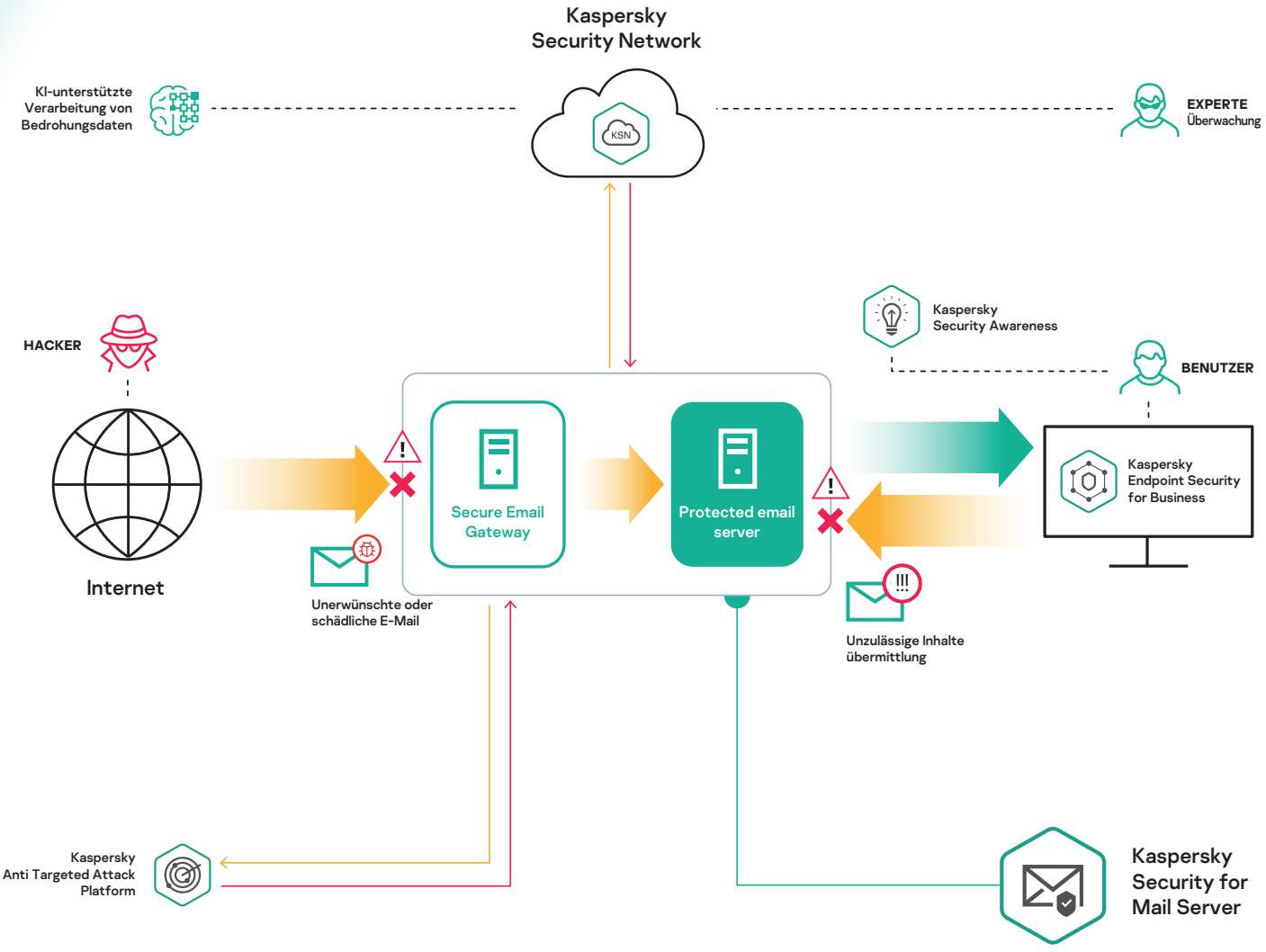
Integriertes Backup

Damit während einer Desinfektion oder Löschung keine wichtigen Daten verloren gehen, können Originalnachrichten auf einem Backup-Speicher gespeichert werden, die vom Administrator an einem passenderen Zeitpunkt bearbeitet werden. Es können bestimmte Regeln für eine bedingte Sicherung von Daten konfiguriert werden.

Verwaltbarkeit und Transparenz

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

- Flexible, aber einfache Regel- und Richtlinienkonfiguration
- Active-Directory-Integration
- Ereignisexport in SIEM-Systeme
- Systemdiagnose



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

Möglicherweise auch für Sie interessant:

Kaspersky Security for Microsoft Office 365: Diese Lösung ist speziell auf das Cloud-Angebot von Microsoft zugeschnitten, darunter Outlook 365.

Kaspersky Security for Internet Gateway — ergänzen Sie Ihren E-Mail-Perimeterschutz mit einer ebenso leistungsstarken Web-Gateway-Sicherheit — 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.

Holen Sie sich Kaspersky Security for Mail Server

Kaspersky Security for Mail Server ist nur eine von vielen Kaspersky-Lösungen, die wir intern mit unseren über 20 Jahren Erfahrung basierend auf einer einzigen Code-Basis entwickelt haben – und die nahtlos ineinandergreifen, um eine umfassende und zuverlässige Sicherheitsplattform zu schaffen.

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, indem Sie Kaspersky Security for Mail Server neben oder anstelle Ihres aktuellen E-Mail-Schutzes installieren.

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

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? Bei Rückfragen können Sie gerne eine telefonische Beratung anfordern.

Bei unseren Partnern kaufen

Sie möchten die Lösung erwerben? Suchen Sie einen Fachhändler in Ihrer Region, der Sie hierbei unterstützt.

Cyber Threat News: https://de.securelist.com/
IT Security News: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir sie, 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.