KASPERSKY lab

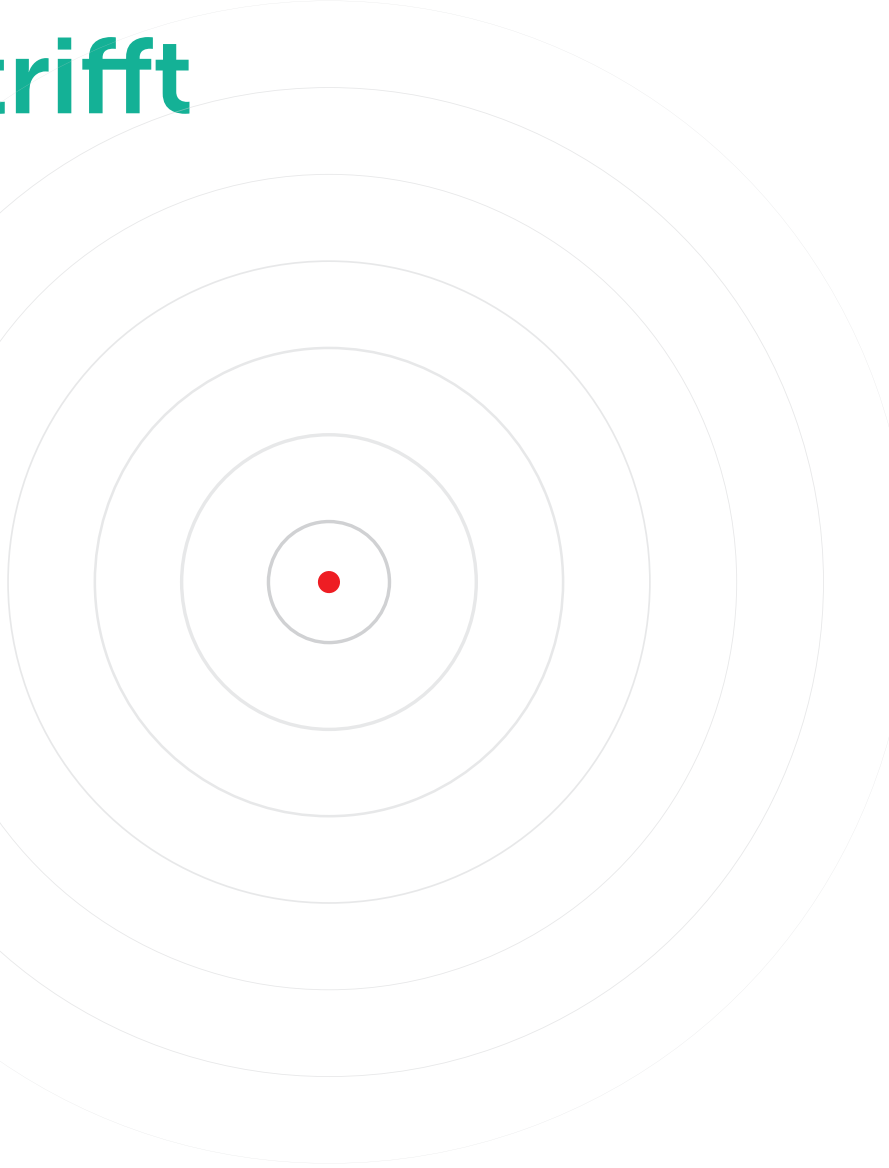
NEXT-GENERATION-SCHUTZ FÜR E-MAILS

E-Mails werden pro Sekunde versendet.

Eine einzige davon kann ausreichen, um Ihr Unternehmen lahmzulegen.

Wenn Office 365 rund um die Uhr auf Cyberbedrohungen trifft

Die meisten Unternehmen investieren sehr viel Zeit in Schulungen für ihre Mitarbeiter über verdächtige und gefährliche E-Mails. Aber was können Sie tun, wenn Cyberkriminelle und Spammer ständig ihre Taktiken ändern?



Angesichts der Tatsache, dass E-Mails der Malware-Vektor Nummer eins für Unternehmen sind[1], wäre es riskant, sich auf Standard- oder integrierte Sicherheitseinstellungen zu verlassen.

Kaspersky Security for Microsoft Office 365 hilft Ihrem Unternehmen, Spam und schädliche E-Mails zu erkennen und zu blockieren, bevor sie zum Problem werden – ohne Beeinträchtigung der Produktivität oder versehentliches Löschen von legitimem Datenverkehr.

Genau wie Microsoft Office 365 wird es in der Cloud gehostet. Es beruht wie alle Kaspersky-Lösungen auf umfassend getesteter und weltweit mit vielen Preisen ausgezeichneter Sicherheitssoftware.

1: Verizon Data Breach Investigation Report 2017

Spam: Mehr als nur ein Ärgernis

Von Bandbreite bis hin zu Produktivitätseinbußen: Spam ist mehr als nur ein Ärgernis. Der durchschnittliche Arbeitnehmer verbringt jährlich 13 Stunden mit dem Durchsuchen und Löschen solcher E-Mails.[2]

Ganz zu schweigen von der Zeit, die Mitarbeiter mit der Verfolgung legitimer geschäftlicher E-Mails verbringen, die versehentlich in den Spam-Ordner gewandert sind. Blockierte E-Mails sind eine Sache, aber noch schlimmer ist es, wenn E-Mails automatisch gelöscht werden – ein häufiges Problem bei integrierten Sicherheitseinstellungen für Cloud-E-Mails.

Obendrein führt viel Spam auch Malware mit sich. 58 % des gesamten E-Mail-Verkehrs sind Spam. Warum also Zeit, Ressourcen und Geld, das Sie durch die Umstellung auf die Cloud eingespart haben, für Junk-Nachrichten verlieren die niemand will?

2: Atlassian: Time Wasting At Work

Anti-Spam-Technologien

Kaspersky Security for Microsoft Office 365 verwendet Next-Generation-Spam-Erkennung und -Analyse, basierend auf lernfähigen Systemen und Cloud-basierter Threat Intelligence. Das Kaspersky Security Network unterstützt in Echtzeit die Erkennung und Blockierung von Spam-Techniken, die sich ständig weiterentwickeln.

Automatisiertes Anti-Spam (mit Inhaltsreputation)

Das Anti-Spam-System von Kaspersky Lab nutzt Erkennungsmodelle, die auf lernfähigen Systemen basieren. Die automatisierte Spam-Verarbeitung wird durch Experten von Kaspersky Lab betreut, sodass eine effektive Erkennung selbst von hochentwickeltem, unbekanntem Spam möglich ist. Und das bei minimalem Verlust wichtiger Nachrichten aufgrund von Fehlalarmen.

Unterstützung authentifizierter E-Mails

Das Senden von Spoof-E-Mails ist eines der wichtigsten Werkzeuge von betrügerischem und böswilligem Spam im Kontext von Social Engineering. Das Sender Policy Framework (SPF) stellt sicher, dass eingehende E-Mails, die scheinbar von vertrauenswürdigen Quellen stammen, echt sind. Dies verringert das Risiko von Spoofing erheblich.

Kaspersky Security Network

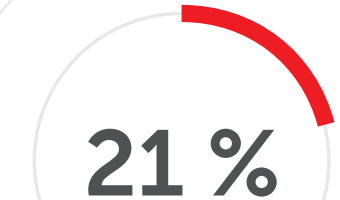
Das Kaspersky Security Network sammelt nahezu in Echtzeit Informationen über neuen Spam aus der ganzen Welt und ermöglicht damit sofortige Reaktionen auf unbekannten Spam, einschließlich Zero-Hour und neuen Epidemien. Dies geschieht automatisch, ohne Eingriff des IT-Personals, und trägt dazu bei, E-Mail-Überschwemmungen und Infektionen zu verhindern.

Massen-E-Mails

Nachrichten aus einer vertrauenswürdigen Quelle können einige Spam-Attribute enthalten, ohne wirklich Spam zu sein. Manche solcher Nachrichten können auch für die Arbeit verwendet werden. Um die Produktivität der Mitarbeiter sicherzustellen, können diese Nachrichten als Massen-E-Mails getaggt oder in einen speziellen Ordner verschoben werden, statt umgehend gelöscht zu werden.

Phishing: Die Bedrohung sitzt im Posteingang

Cyberkriminelle verwenden E-Mails für ihre Angriffe, weil es der schnellste und direkteste Weg in das Herz eines jeden Unternehmens ist.



der gemeldeten Cybervorfälle entstehen durch irgendeine Form des Phishing[3]

Sie wissen auch, dass trotz größter Bemühungen, die Benutzer zu erziehen, eine gut getarnte E-Mail meist ausreicht, um selbst vorsichtige Benutzer auf einen schädlichen Anhang oder Link klicken zu lassen. Phishing-Angriffe bestehen in der Regel aus E-Mails, die als legitime Kommunikation getarnt sind und die Benutzer auffordern, auf einen schädlichen Link oder Anhang zu klicken. Das haben wir alle schon gesehen: SONDERANGEBOT! ZAHLUNGSVERZUG! IHRE LIEFERUNG VERZÖGERT SICH! - Diese Mails zielen nicht einfach darauf ab, die Benutzer ohne Nachdenken zum Klicken zu veranlassen, sondern verwenden absichtlich manipulative Sprache und Techniken, was sie so überzeugend macht.

Beim Spear-Phishing geht dies noch einen Schritt weiter. Es funktioniert viel gezielter und richtet sich in der Regel an sorgfältig ausgewählte Personen, die in einem Unternehmen arbeiten, mit zugeschnittenen E-Mails und Anhängen, die fast genauso aussehen wie legitime Kommunikation: eine „Bewerbung" an den namentlich genannten Personalmanager, eine E-Mail, die sich auf eine echte Stellenanzeige bezieht, oder eine Rechnung an die richtige Person in der Buchhaltung, die sich auf eine Firma bezieht, mit der Sie tatsächlich eine Geschäftsbeziehung haben.

In letzter Zeit war eine Zunahme an „Business E-Mail Compromise" (BEC)-E-Mails zu beobachten, die scheinbar von jemandem innerhalb Ihres eigenen Unternehmens kommen, z. B. dem CEO. Diese haben dann meist die Überweisungen „genehmigt" oder „erbitten" die Herausgabe sensibler Daten. Da diese Angriffe so fein auf den Empfänger abgestimmt sind, entgehen solche E-Mails oft den normalen Spam-Fallen: Sie werden nicht in großen Mengen gesendet, sondern in der Regel nur an ein paar geschickt ausgewählte Mitarbeiter.

Durch das Ausblenden der Dateierweiterung aus der oberflächlichen Ansicht oder durch Verschleierung der E-Mail-Adresse, sodass es aussieht, als käme sie beispielsweise vom CEO, können Cyberkriminelle die Sicherheitsschwachstellen leicht ausnutzen.

3: Verizon Data Breach Investigation Report 2017

Anti-Phishing-Technologien

Kaspersky Security for Microsoft Office 365 verwendet Sandbox-Umgebungen und lernfähige Systeme, um auch unbekannte Bedrohungen herauszufiltern, bevor der Benutzer einen Fehler machen kann. Selbst wenn eine Dateierweiterung ausgeblendet ist, kann sie mittels Erkennung echter Dateitypen erkannt und blockiert werden.

Die Next-Generation-Anti-Phishing-Technologien in Kaspersky Security for Microsoft Office 365 schützen E-Mail-Programme vor komplexen und unbekannten Bedrohungen, ohne die Produktivität zu beeinträchtigen:

Auf neuronalen Netzwerken basierende Anti-Phishing-Engine

Schützt vor unbekanntem und Zero-Hour-Phishing mithilfe von über 1000 Kriterien zur Erstellung von Erkennungsmodellen. Unterstützt durch das Kaspersky Security Network, schützen unsere ständig aktualisierten Bedrohungsdatenbanken vor schädlichen URLs und anderen Phishing-Bedrohungen.

Threat Intelligence für Malware- und Phishing-URLs

Unterstützt vom Kaspersky Security Network (unserem unter realen Bedingungen arbeitenden, Big-Data-basierten Threat Intelligence-Netzwerk), werden den ständig aktualisierten Datenbanken automatisch ermittelte Daten und auch die Ergebnisse der Bedrohungsanalysen unserer Experten zugeführt.
Dies trägt zur Verhinderung von Drive-by- und Waterholing-Angriffen sowie von Betrugsversuchen über schädliche Webseiten bei.

Die Phishing-Nachrichten können gelöscht, verschoben oder mit Tags versehen werden:

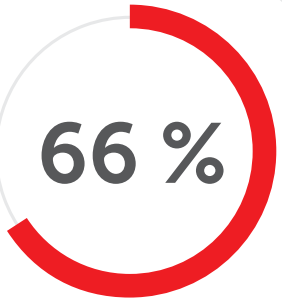
Nicht alle unerwünschten E-Mails sind Junk; werden sie automatisch gelöscht, kann dies zu Produktivitätsproblemen führen oder Auswirkungen auf potentiell wichtige Kommunikation haben. Der Anti-Phishing-Schutz von Kaspersky Lab ermöglicht die einfache Tag-basierte Filterung und Markierung potentiell nützlicher Massen-E-Mails mit benutzerdefinierten Tags und das Verschieben in den Junk-Ordner, statt die E-Mails direkt zu löschen.

Anhanganalyse in der Vorschau:

Schützen Sie sich mit diesem einzigartigen System vor hochentwickelten Phishing-Angriffen, die zu erheblichem Datenverlust oder finanziellen Verlusten führen würden. Diese Funktion analysiert die Anhänge, die in der Vorschau angezeigt werden können, darunter PDF, RTF und MSOffice-Dateien, auf Phishing-Inhalt.

Malware: Ransomware, Zero-Hour-Nutzung und dubiose Anhänge

66 % der Malware wird über schädliche Anhänge installiert.[4] Zero-Hour- und Zero-Day-Angriffe lauern oft in Word-, Excel-, PowerPoint- und anderen Dateien für Unternehmensprogramme, die nur auf den Klick des Benutzers warten.

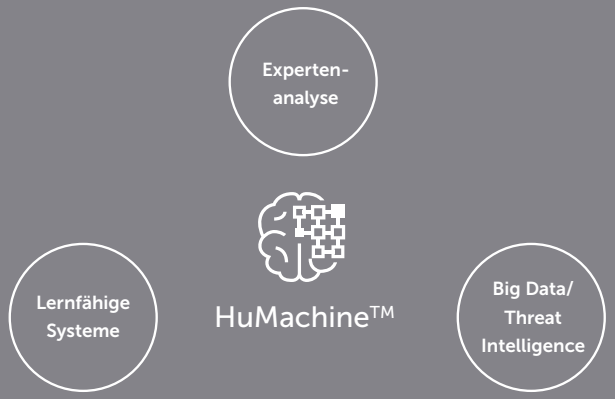


der Malware installiert sich über schädliche Anhänge

In vielen Fällen führen schädliche Anhänge Malware mit sich, die mittels Spyware Authentifizierungsdaten oder Anmeldedaten stehlen. Die Malware installiert sich ohne Wissen des Benutzers. Zu den weiteren häufigen Anhang-basierten Angriffen gehört die Ransomware. Einmal gestartet, werden die Daten des Benutzers verschlüsselt, bis ein Lösegeld gezahlt wird.

Was ist HuMachine™?

Die HuMachine© von Kaspersky Lab kombiniert das Beste aus menschlicher Expertise, Big-Data-Threat Intelligence und lernfähigen Systemen, um Sie vor allen Arten von Unternehmensbedrohungen zu schützen.



4: Verizon Data Breach Investigation Report 2017.

Anti-Malware-Technologien

Kaspersky Security for Microsoft Office 365 verwendet Sandbox-Umgebungen und lernfähige Systeme, um die wahre Natur eines Anhangs oder einer Datei zu ermitteln, bevor der Anhang oder die Datei zugelassen wird. Verdächtige Dateien können an einem sicheren Ort ausgeführt werden, um festzustellen, ob es sich um Malware handelt, bevor sie zugelassen werden.

Mehrschichtige Bedrohungserkennung durch HuMachine

Die bewährten Funktionen der Bedrohungserkennung von Kaspersky Lab umfassen mehrere proaktive Sicherheitsebenen, die schädliche Anhänge aus E-Mails herausfiltern. Auf maschinellem Lernen basierende Erkennungsmodelle filtern bisher unbekannte Zero-Hour-Malware heraus.

Kaspersky Security Network

Unser Cloud-basiertes, globales Threat Intelligence-Netzwerk nutzt anonymisierte reale Daten von über 60 Millionen Endpoint-Sensoren weltweit und ermöglicht so schnellste Reaktionszeiten und höchstmögliche Sicherheitsebenen, selbst vor dem Hintergrund ständiger Weiterentwicklungen in der Bedrohungslandschaft.

Filtern von Anhängen

Blockieren Sie gefährliche Dateien, bevor sie zu einem Problem werden, und verwalten Sie unerwünschte Nachrichten. Durch die Erkennung echter Dateitypen wird verhindert, dass schädliche Dateien, die als sichere Dateien getarnt sind, zugelassen werden. Durch Filtern von Anhängen nach Erweiterung können unerwünschte Dateitypen blockiert oder getaggt werden, während die Makroerkennung es ermöglicht, Aktionen auf potentiell gefährliche Office-Dateien mit aktivierten Makros anzuwenden. Flexible Ausschlüsse und Tagging helfen, den Verlust legitimer E-Mails, die in die Filterkriterien fallen, zu reduzieren.

Einfach zu verwaltender, kostengünstiger Next-Generation-Schutz

Sie arbeiten in der Cloud, weil es bequem, ressourceneffizient und kostengünstig ist. Mit Kaspersky Security for Microsoft Office 365 gibt es keine Notwendigkeit, irgendeinen dieser Faktoren um der E-Mail-Sicherheit willen zu opfern. Eine einzige, intuitive Verwaltungskonsole hilft Ihnen, sich um alles zu kümmern, und bietet eine einzige Ansicht der erkannten Bedrohungen und Statistiken. Es besteht keine Notwendigkeit für zusätzliche Hardware oder Schulungen des IT-Sicherheitspersonals. Und es ist auch keine Installation erforderlich.

Und das alles ohne Beeinträchtigung oder versehentliches Löschen des legitimen Datenverkehrs:

Einfache Verwaltung, Administration und Integration

Dashboard für den schnellen Überblick:

Nur ein einziger Bildschirm für die tägliche, wöchentliche oder monatliche Überwachung und für den Status hinsichtlich Bedrohungen, Statistiken, Erkennungen usw.

Einfache Konfiguration:

Alle Einstellungen sind zwecks ultimativ einfacher Konfiguration und Überprüfung auf einem einzigen Bildschirm gruppiert.

Test vor dem Rollout:

Wählen Sie aus, welche Posteingänge geschützt werden sollen, und ermöglichen Sie so das einfache Testen einer Konfiguration oder die flexible Anwendung von Richtlinien.

Mehrmandantenfähigkeit:

Es können mehrere Administratoren aktiviert werden, die die Lösung über verschiedene Konten verwalten.

Backup:

Viele Benutzer haben das Problem, dass legitime E-Mails mit Spam verwechselt werden. Mit weniger Fehlalarmen und Administratorkontrolle über das, was mit verdächtigen E-Mails geschieht, reduziert Kaspersky Security for Microsoft Office 365 die Wahrscheinlichkeit solcher Vorfälle erheblich. Gelöschte E-Mails werden in Backups hinterlegt und können dort gesucht und wiederhergestellt werden – keine „verschwundenen" E-Mails mehr.

Benachrichtigung:

Schnelle Reaktionen auf Vorfälle mit Administratorbenachrichtigungen bei Spam, Phishing, Virenattacken oder Richtlinienverstößen durch Anhänge.

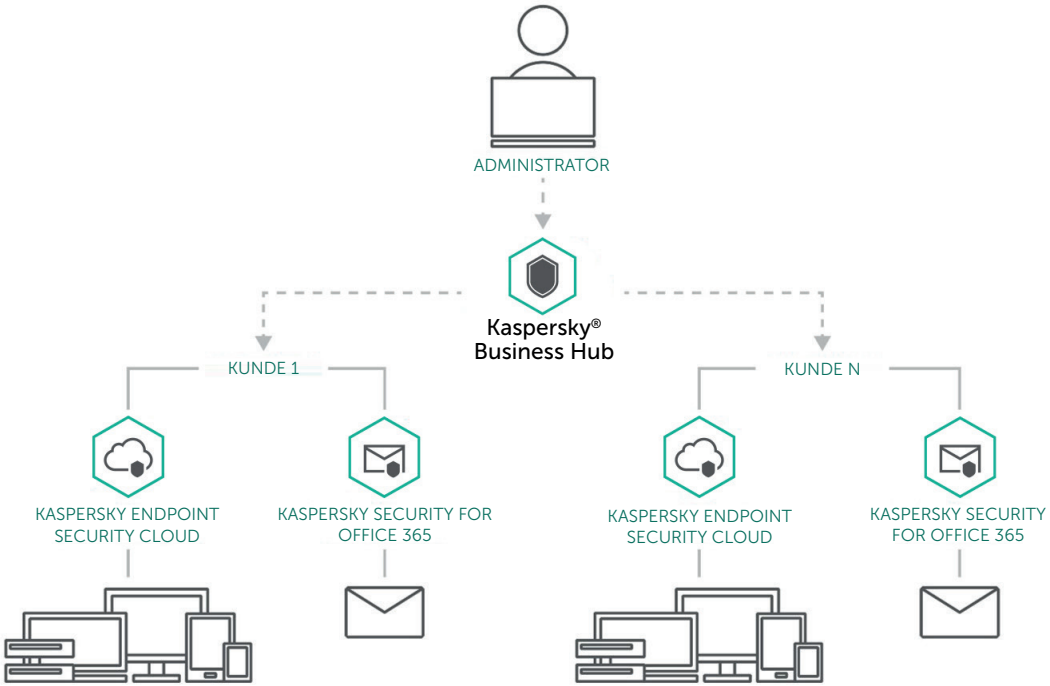
Einmalige Anmeldung:

Nur eine Konsole und eine Anmeldung zur Verwaltung der Sicherheit für verschiedene Endpoints, Geräte und für Exchange Online.

Kaspersky® Business Hub

Kaspersky Business Hub – Verwaltung für den Schutz Ihres Unternehmens über nur eine Konsole.

Erleben Sie die intuitive Oberfläche, die einfache Verwaltung und erhalten Sie erstklassigen Schutz für verschiedene Geräte sowie Produktivitätstools. Verbinden Sie sich von Ihrem gewünschten Gerät – jederzeit und überall – Sie haben die Kontrolle.



Die folgenden Produkte werden im Kaspersky Business Hub verwaltet:

- Kaspersky Endpoint Security Cloud
- Kaspersky Security for Microsoft Office 365

Kaspersky® Security for Microsoft Office 365

Wenn es um den Schutz Ihrer E-Mails in Microsoft Office 365 geht, besteht die beste Strategie darin, Bedrohungen zu erkennen und zu blockieren, bevor sie zu einem Problem werden.

Kaspersky Security for Microsoft Office 365 wurde dafür entwickelt, dass dies ohne Beeinträchtigung oder versehentliches Löschen des legitimen Datenverkehrs geschieht.

Entdecken Sie, wie Sie Ihre E-Mails in Microsoft Office 365 mit unseren Next-Generation-Sicherheitstechnologien noch einfacher schützen und verwalten können.

Die kostenlose Testversion finden Sie unter cloud.kaspersky.com