KASPERSKY lab

ENTERPRISE SECURITY. POWERED BY INTELLIGENCE.

Kaspersky Security Solutions for Enterprise 2017

SICHERHEIT FÜR IHR UNTERNEHMEN

Cyberbedrohungen werden immer raffinierter. Ohne eine effektive Lösung zu ihrer Abwehr können finanzielle Schäden entstehen, Geschäftsprozesse beeinträchtigt, vertrauliche Daten gefährdet und der Ruf des Unternehmens geschädigt werden. Erfolgreiche Angriffe haben bei Unternehmen aller Branchen oft gravierende Folgen.

UNTERNEHMENSSICHERHEIT ERNST NEHMEN

Mit Sicherheitsverletzungen sind erhebliche Kosten verknüpft: Die im Rahmen der Umfrage zu globalen IT-Sicherheitsrisiken von Kaspersky Lab ermittelten unmittelbaren Sanierungskosten für Großunternehmen betrugen durchschnittlich 551.000 US-Dollar – hinzu kommen indirekte Kosten von durchschnittlich 69.000 US-Dollar. Um diese Kosten und die mit ihnen einhergehenden Betriebsstörungen zu vermeiden, müssen Unternehmen die Art und den Umfang der Schutzmaßnahmen für ihre IT-Infrastruktur stärken.

Basierend auf der umfassenden Sicherheitsexpertise, die in alle Produkten und Services von Kaspersky Lab einfließt, bieten unsere Lösungen die Funktionalität zu Prognose, Prävention, Erkennung und Reaktion für eine Vielzahl von Infrastruktursegmenten und aufkommende Technologien. Hierzu zählen Endpoints, Online- und Mobile-Technologien, virtualisierte Infrastrukturen, Rechenzentren, industrielle Steuerungssysteme usw.

Kaspersky Lab ist Vorreiter in der Aktualisierung von Sicherheitsstrategien für Unternehmen, um diese besser vor aktuellen, hoch entwickelten Bedrohungen und gezielten Angriffen zu schützen. Wir bieten eine einzigartige Kombination aus Technologien und Services, gestützt von relevanten Sicherheitsdaten. So helfen wir Unternehmen dabei, gezielte Angriffe frühzeitig zu erkennen und die Risiken zu mindern, bevor größere Schäden entstehen.

Kaspersky Lab bietet mit seinem Angebot, das alle möglichen Stufen von IT-Sicherheitsvorfällen umfasst, eine ganzheitliche, anpassungsfähige und strategische Herangehensweise an das Thema Unternehmenssicherheit. Unsere Philosophie ist im Grunde ganz einfach: Zuverlässige Sicherheitsinformationen in Kombination mit zuverlässigen Technologien ergeben einen höchst zuverlässigen Schutz für Unternehmen.

ENDPOINT SECURITY

Zuverlässiger Schutz vor bekannten, unbekannten und hoch entwickelten Bedrohungen, die gezielt Ihre Endpoints und Benutzer angreifen

Schwachstellen in beliebter Software, wie z. B. Java, Internet Explorer und Adobe, waren in der Vergangenheit für einige der gravierendsten Sicherheitsverletzungen verantwortlich. Und es sind nicht nur die Zero-Day-Schwachstellen, die ein Problem darstellen: 2015 beruhten mehr als 40 % der Sicherheitsverletzungen auf Schwachstellen, die bereits zwischen zwei und vier Jahre lang bekannt waren. Ganze 84 % aller Cyberattacken erfolgen auf der Anwendungsschicht.

Die IT-Umgebungen in Großunternehmen sind komplex. Hacker und Cyberkriminelle nutzen immer raffiniertere Methoden, um sie anzugreifen. Ohne angemessene Maßnahmen zur Handhabung ihrer IT-Sicherheit setzen sich Unternehmen unnötigen Risiken aus.

Die Mehrheit der Angriffe auf Großunternehmen wird über Endpoints eingeleitet. Gelingt es einem Unternehmen, sämtliche stationären, virtualisierten oder mobilen Endpoints zu sichern, schafft es eine solide Grundlage für eine wirkungsvolle Sicherheitsstrategie.

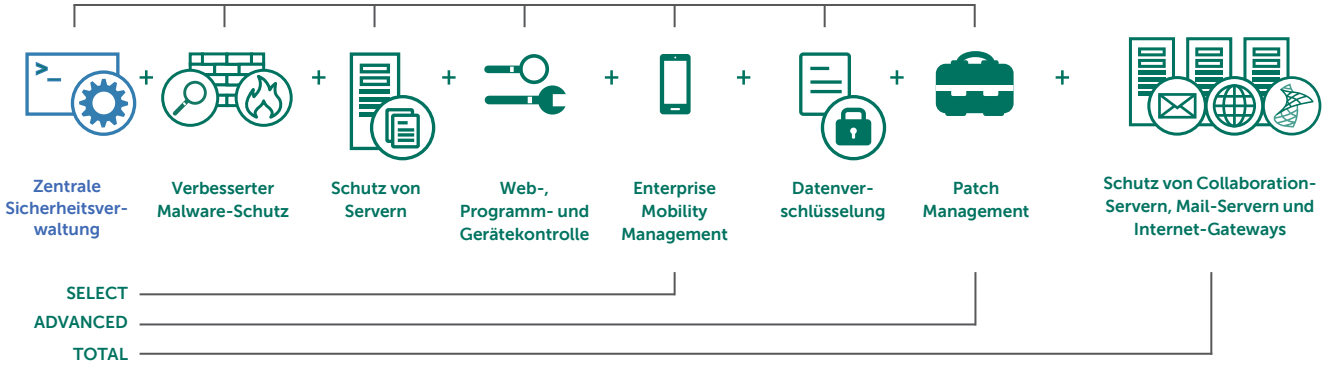
Um Echtzeitschutz vor unbekannten und hoch entwickelten Bedrohungen und eine wirksame Erkennung von zielgerichteten Attacken zu ermöglichen, entwickeln wir unsere Technologien und Bedrohungsexpertise laufend weiter, damit Ihr Unternehmen selbst vor den neuesten und raffiniertesten Bedrohungen und Exploits geschützt ist.

Der Schutz wird durch leistungsstarke Kontroll- und Datenschutz-Tools zusätzlich erhöht: Programmkontrolle mit „Default Deny" und System-Hardening, integrierte Full-Disk- und File-Level-Verschlüsselung mit sicherem Preboot, intelligentes Applikations- und System-Patching sowie eine zentrale Verwaltung durch das Kaspersky Security Center.

DIE LÖSUNG: KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Kaspersky Lab bietet eine ganze Palette von Sicherheitslösungen mit maßgeschneiderten Technologien an, die eine Vielzahl von Fähigkeiten mit zunehmendem Funktionsumfang bieten. Sämtliche Komponenten werden bei uns im Haus entwickelt und bilden so eine gemeinsame Plattform, die sich problemlos an unterschiedliche geschäftliche Anforderungen anpasst.

LIZENZSTUFEN VON KASPERSKY ENDPOINT SECURITY FOR BUSINESS



SELECT

Unsere SELECT-Edition enthält Tools für die Verwaltung von Endpoints, Servern und Mobilgeräten. Es stehen Ihnen auch eine Reihe von Kontroll-Tools zur Verfügung, darunter die Geräte- und Programmkontrolle einschließlich Default-Deny-Modus. Diese erlauben die effektive Durchsetzung von Richtlinien, mit denen sich wichtige Komponenten der IT-Infrastruktur in Unternehmen absichern lassen. Die Edition enthält darüber hinaus auch Schutzfunktionen für Server, darunter Schutz für freigegebene Netzwerkordner vor Cryptor-Angriffen.

ADVANCED

Die ADVANCED-Edition enthält alle Tools aus SELECT plus Verschlüsselungsfunktionen, darunter Full-Disk- und File-Level-Verschlüsselung sowie Verschlüsselung für Wechseldatenträger. Vulnerability-Assessment-Tools und automatisches Patching für Betriebssysteme und Programme sowie die Programmkontrolle für Server sind ebenfalls in ADVANCED enthalten.

TOTAL

Kaspersky TOTAL Security for Business enthält zusätzliche Technologien zum Schutz von Mail-Servern, Internet-Gateways und Collaboration-Servern.

VIRTUALIZATION SECURITY

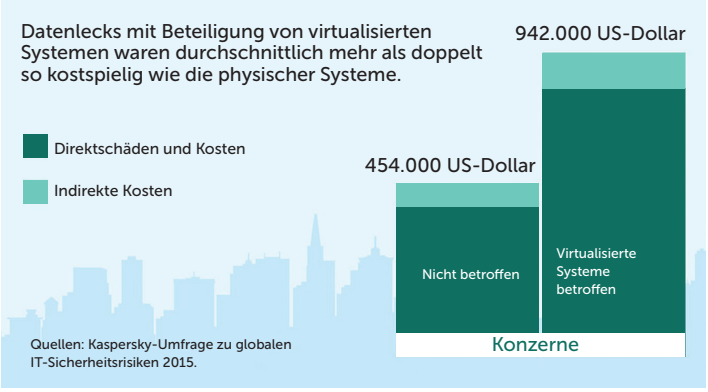
Verlässlicher, flexibler und effizienter Schutz für virtualisierte Server und VDI

Beim Schutz von virtualisierten Systemen müssen Unternehmen die richtige Balance zwischen Schutz und Performance erreichen und die fortschrittlichsten Sicherheitsfunktionen nutzen, damit entscheidende Geschäftsprozesse optimal geschützt werden.

Je umfassender Unternehmen ihre IT-Infrastruktur auf virtualisierte Umgebungen umstellen, umso größer der Bedarf an Sicherheitslösungen, die speziell für die Virtualisierung entworfen wurden. Eine Sicherheitslösung sowohl für die wachsende virtuelle Desktop-Infrastruktur (VDI) und Ihre virtualisierte Serverumgebung zu finden und gleichzeitig die Vorteile der Virtualisierung zu bewahren, ist nicht so einfach. Trotz ihrer vielen Vorteile entstehen bei der Virtualisierung auch zusätzliche Angriffsflächen, die Cyberkriminellen noch mehr Möglichkeiten bieten, Großunternehmen anzugreifen.

Die zur Absicherung Ihrer virtualisierten Infrastruktur eingesetzte Lösung sollte einen unterbrechungsfreien Schutz bieten, aber nicht die Effizienz Ihrer virtualisierten Umgebung beeinträchtigen.

Die einzigartige Architektur der Speziallösung von Kaspersky Lab ermöglicht einen wirkungsvollen, mehrschichtigen Schutz von virtuellen Maschinen (VMs), der nicht zu Lasten der Performance geht. Das Ergebnis sind erheblich höhere Konsolidierungsraten als bei herkömmlichen Anti-Malware-Lösungen. Darüber hinaus können jetzt Update- und Scan-Storms sowie Zeitfenster mit Schwachstellen oder „Instant-on"-Lücken vermieden werden. Dank zusätzlicher Schutzebenen und Mechanismen zur Abwehr von Netzwerkattacken eröffnet die Kaspersky-Lösung eine ganz neue Dimension von Sicherheit für Virtualisierungsplattformen in Unternehmen.



In Großunternehmen liegen die Kosten nach einer Sicherheitsverletzung in einer virtualisierten Umgebung bei durchschnittlich 940.000 US-Dollar – doppelt so hoch wie bei einem vergleichbaren Vorfall, der nur die physische Infrastruktur betroffen hätte.

Während bei einem Angriff auf physische Nodes in 36 % der gemeldeten Fälle der Zugriff auf geschäftskritische Informationen vorübergehend unmöglich ist, steigt dieser Wert auf 66 % an, wenn virtualisierte Server und Desktops betroffen sind.

DIE LÖSUNG: KASPERSKY SECURITY FOR VIRTUALIZATION

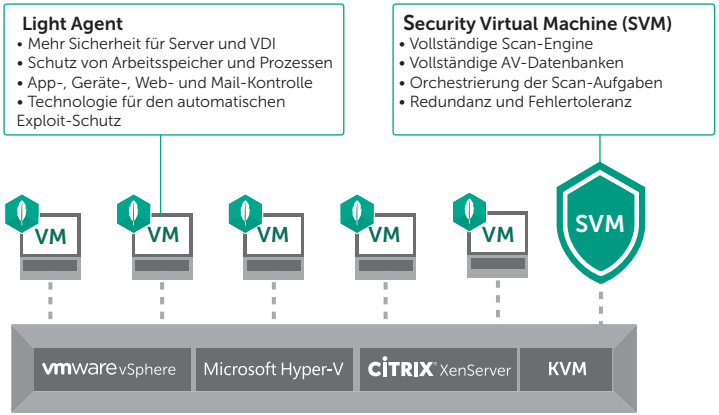
Kaspersky Lab hat zwei Lösungen im Angebot, mit denen Sie die perfekte Balance zwischen optimaler Sicherheit und uneingeschränkter Leistung erreichen.

Während unsere agentenlose Lösung im Verbund mit den grundlegenden Hypervisor-Technologien agiert, bietet unsere Light-Agent-Lösung zusätzlichen Schutz für jede einzelne VM.

Zum Schutz von VMs müssen Unternehmen lediglich eine einzige, so genannte Security Virtual Machine (SVM) bereitstellen, an die die Scanprozesse auf Dateiebene ausgelagert werden können. Diese SVM bietet zentralen Malware-Schutz für alle VMs, ohne dabei die Ressourcen zusätzlich zu belasten. Dank systemeigener Fehlertoleranz und Redundanz bietet Ihre Sicherheitslösung die Zuverlässigkeit, die Sie für einen erfolgreichen Geschäftsbetrieb benötigen.

Durch den Einsatz eines Light Agent auf jeder Ihrer VMs kommen ein mehrstufiger Schutz und funktionsreiche Sicherheitskontrollen hinzu. Die Sicherheit für Ihre VMs – egal ob agentenlos, Light Agent oder beides – lässt sich zusammen mit Ihren physischen Endpoint-Servern und Mobilgeräten über eine einzige Konsole verwalten.

EINZIGARTIGE LIGHT-AGENT-TECHNOLOGIE VON KASPERSKY LAB



Kaspersky Security for Virtualization ist eng in die gängigen Virtualisierungsplattformen integriert: VMware vSphere, KVM, Microsoft Hyper-V und Citrix XenServer. Unsere Sicherheitslösung ist darauf ausgelegt, die Leistungsfähigkeit Ihrer Plattform beizubehalten. Hierzu nutzen wir die systemeigenen Kerntechnologien Ihres Hypervisors voll aus und ergänzen und erweitern so die Sicherheit, beispielsweise bei VMware Horizon und Citrix XenDesktop VDI.

Kaspersky Security for Virtualization kann je nach geschäftlichen Anforderungen und Eigenarten Ihrer virtualisierten Infrastruktur unterschiedlich lizenziert werden: entweder auf Grundlage der VM-Anzahl (Desktops plus Server) oder der Anzahl der vorhandenen physischen Prozessorkerne der Hostserver.

MOBILE SECURITY

Sicherheits-, Management- und Kontrollfunktionen für Mobilgeräte

Im dritten Quartal 2015 entdeckten mobile Sicherheitslösungen von Kaspersky Lab 323.374 neue Schadprogramme – ein 1,1-facher Anstieg im Vergleich zum zweiten Quartal und ein 3,1-facher Anstieg gegenüber dem ersten Quartal desselben Jahres.

Schädliche Software und Webseiten sowie Phishing-Angriffe auf mobile Geräte wachsen weiterhin an, während sich die Funktionalität von mobilen Geräten ungebrochen weiterentwickelt. Als wichtige Produktivitätstools zuhause wie bei der Arbeit sind sie ein verlockendes Ziel für Cyberkriminelle. Die zunehmende Nutzung von privaten Geräten zu beruflichen oder geschäftlichen Zwecken (BYOD) führt zu einer größeren Anzahl unterschiedlicher Geräte innerhalb des Unternehmensnetzwerks und damit zu zusätzlichen Herausforderungen für IT-Administratoren, die mit der Verwaltung und Kontrolle der IT-Infrastrukturen alle Hände voll zu tun haben.

PRIVATE GERÄTE VON MITARBEITERN – EIN RISIKO FÜR DAS GANZE UNTERNEHMEN

Mitarbeiter, die ihre eigenen mobilen Endgeräte sowohl privat als auch für die Arbeit einsetzen, erhöhen das Risiko einer Sicherheitsverletzung für das Unternehmensnetzwerk. Haben Hacker erst einmal Zugang zu ungesicherten persönlichen Informationen auf einem mobilen Gerät erlangt, dann ist der Zugriff auf Unternehmenssysteme und Geschäftsdaten leicht.

KEINE PLATTFORM IST SICHER

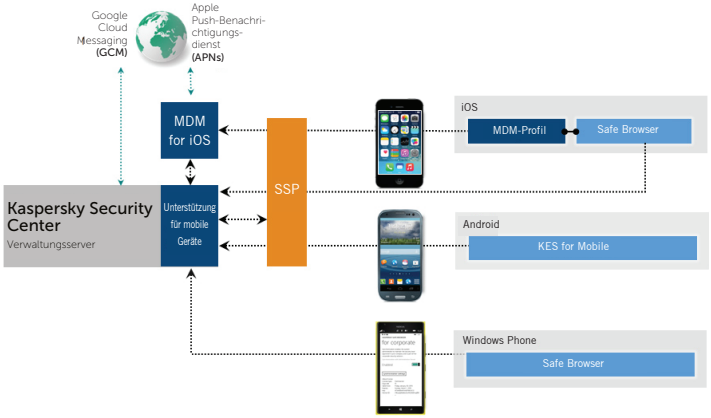
Cyberkriminelle kennen eine Vielzahl von Methoden, um sich Zugang zu mobilen Geräten zu verschaffen, darunter infizierte Programme, öffentliche Wi-Fi-Netzwerke ohne ausreichende Sicherung, Phishing-Angriffe und infizierte Textnachrichten. Besucht ein Benutzer aus Versehen eine schädliche Webseite bzw. eine seriöse Webseite, die mit Schadcode infiziert wurde, gefährdet er damit die Sicherheit seines Geräts und der darauf gespeicherten Daten. Das Anschließen eines iPhones an einen Computer, z. B. um den Akku nachzuladen, kann schon zu einer Infizierung des iPhones mit Malware führen. (Diese Bedrohungen betreffen alle gängigen Mobilplattformen: Android, iOS und Windows Phone.)

DIE LÖSUNG: KASPERSKY SECURITY FOR MOBILE

Kaspersky Security for Mobile löst diese Probleme durch mehrstufigen Schutz und eine große Bandbreite von Funktionen für das Mobile Device Management (MDM) und das Mobile Application Management (MAM). Durch diese lässt sich der zeitliche Aufwand für die Wartung von mobilen Geräten erheblich reduzieren und ein sicherer mobiler Zugriff auf Unternehmenssystemen garantieren.

- **Mobile Security:** Unsere mobilen Sicherheitstechnologien bieten mehrstufigen Schutz vor den neuesten mobilen Bedrohungen sowie eine Reihe von Diebstahlschutz-Funktionen, die per Fernzugriff bedient werden können.
- **Mobile Device Management:** Dank Integration in alle führenden Plattformen können mobile Geräte per OTA-Schnittstelle (Over-the-Air) gescannt und kontrolliert werden. Dies verbessert den Schutz und das Management von Android-, iOS- und Windows Phone-Geräten erheblich.
- **Mobile Application Management:** Isolierte Container für Programme und die Option, den Gerätespeicher selektiv zu löschen, ermöglichen es, geschäftliche und persönliche Daten voneinander zu trennen und effektiv zu schützen.

Dank der Kombination aus funktioneller Verschlüsselung und Schutz vor Malware können Sie mit Kaspersky Security for Mobile Geräte von Anfang an schützen – und nicht nur das Gerät und seine Daten isolieren.



Die Architektur der Lösung

ANTI TARGETED ATTACK

Spezieller, analysebasierter Schutz vor gezielten Angriffen

Gezielte Angriffe sind langfristige Verfahren, die die Sicherheit des Unternehmens gefährden und dem Angreifer Kontrolle über die IT des angegriffenen Unternehmens geben – außerdem vermeiden sie die Entdeckung durch herkömmliche Sicherheitstechnologien.
Während einige Aggressoren so genannte Advanced Persistent Threats (APTs) einsetzen (die sehr effektiv sein können, jedoch recht kostspielig sind), sind andere „gezielte Angriffe" weitaus preisgünstiger, jedoch ähnlich verheerend in der Wirkung. Diese zielgerichteten Angriffe („targeted attacks") sorgen mit ihren grundlegenden Techniken – Social Engineering, Diebstahl von Anmeldeinformationen, legitimer Software oder sogar durch ein gestohlenes Zertifikat verschleierte Malware – zwar nicht für Schlagzeilen, sind dafür aber sehr weit verbreitet.

Die meisten Unternehmen haben bereits beträchtliche Investitionen in herkömmliche IT-Sicherheitslösungen getätigt, meist auf Gateway-Ebene. Aber auch wenn diese präventiven Sicherheitstechnologien beim Schutz vor gängigen Bedrohungen, einschließlich Malware, Datenlecks, Netzwerkangriffen usw., sehr gute Dienste leisten, sind sie offensichtlich nicht ausreichend: Die Gesamtzahl der Sicherheitsvorfälle und -verletzungen in Unternehmen ist nicht im Geringsten zurückgegangen.

Hoch entwickelte, gezielte Bedrohungen können 200 Tage lang oder noch länger unbemerkt bleiben, während Cyberkriminelle still und leise wertvolle Informationen sammeln und/oder in wichtige Geschäftsabläufe eingreifen. Präventionsbasierte Sicherheitstechnologien erkennen möglicherweise einige Vorfälle, erkennen jedoch nicht, dass diese einzelnen Vorfälle Teil eines weit gefährlicheren und komplexeren Angriffs sind.

Wenn nichts dagegen unternommen wird, richtet ein gezielter Angriff in der Regel schweren Schaden in einem Unternehmen an, z. B.:

- Hohe Verluste

  Laut unseren Erfahrungswerten kann selbst ein einzelner gezielter Angriff in einem Großunternehmen Kosten von mehr als 2,5 Millionen US-Dollar verursachen, verglichen mit einem Ausgangspunkt von durchschnittlich 80.000 US-Dollar für kleine und mittlere Unternehmen.
- Wirtschaftsspionage
- Verlust vertraulicher Daten
- Kontrolle über offensichtlich „autorisierte" Geschäftsprozesse durch den Angreifer
- Heimliche Manipulation von Finanz- oder anderen wichtigen Daten

In einer Kaspersky-Studie für Großunternehmen aus dem Jahr 2015 bestätigte fast jedes vierte Unternehmen (23 %), dass es mindestens einmal von einem gezielten Angriff betroffen war.

DIE LÖSUNG: KASPERSKY ANTI TARGETED ATTACK PLATFORM

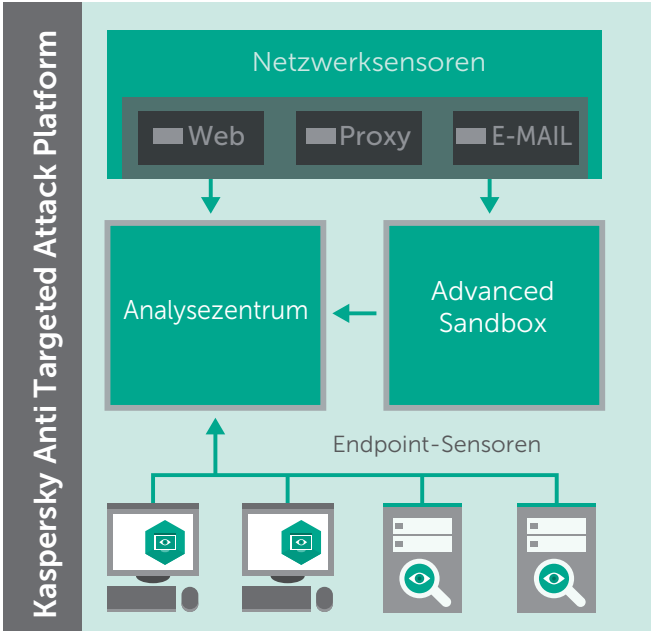
Die Kaspersky Anti Targeted Attack Platform ist Teil eines anpassungsfähigen, integrierten Ansatzes für die Unternehmenssicherheit. Eine Echtzeitüberwachung des Netzwerkverkehrs, kombiniert mit Objekt-Sandbox und Endpoint-Verhaltensanalyse, bietet einen detaillierten Einblick in die Vorgänge der IT-Infrastruktur eines Unternehmens. Diese anpassungsfähige Sicherheitsstrategie schützt Unternehmen vor hoch entwickelten Bedrohungen, gezielten Angriffen, neuer Malware, einschließlich Ransomware und Crimeware und, natürlich, hartnäckigen Bedrohungen (Advanced Persistent Threats, APTs).

Durch die Korrelation von mehrstufigen Ereignissen – einschließlich Netzwerk, Endpoints und globaler Bedrohungslage – ermöglicht die Kaspersky Anti Targeted Attack Platform die Erkennung von komplexen Bedrohungen nahezu in Echtzeit und generiert entscheidende forensische Daten, welche die Grundlage für eine erfolgreiche Vorfallsuntersuchung bilden.

Unsere Global Security Intelligence ist einer der Gründe dafür, warum wir diese ausgezeichnete Erkennungsleistung bieten können. Kaum ein anderer Sicherheitsanbieter verfügt über die Qualität und das breite Spektrum unserer Sicherheitsdaten, die uns in die Lage versetzen, Unternehmen vor einem zunehmend größeren Bedrohungspotential zu schützen.

Global Security Intelligence-Lösungen sind jedoch erst der Anfang. Die Kaspersky Anti Targeted Attack Platform bietet darüber hinaus leistungsstarke Erkennungs- und Analysetechnologien, z. B.:

- **Mehrstufige Sensorarchitektur** – für umfassende Transparenz. Durch die Kombination aus Netzwerksensoren, Web- und E-Mail-Sensoren sowie Endpoint-Sensoren bietet die Kaspersky Anti Targeted Attack Platform hoch entwickelte Erkennung auf allen Ebenen der IT-Infrastruktur Ihres Unternehmens.
- **Advanced Sandbox** – zur Beurteilung neuer Bedrohungen. Unsere Advanced Sandbox, das Ergebnis aus mehr als 10 Jahren kontinuierlicher Entwicklung, bietet eine isolierte, virtualisierte Umgebung, in der verdächtige Objekte sicher verwahrt werden können. Dadurch kann ihre Verhaltensweise beobachtet werden.
- **Leistungsstarke Analyse-Engines** – für schnelle Ergebnisse und weniger Fehlalarme (False-Positives). Unser Targeted Attack Analyzer bewertet Daten von Netzwerk- und Endpoint-Sensoren und erstellt für Ihr Sicherheitsteam schnell Ergebnisse der Bedrohungserkennung.



KASPERSKY PRIVATE SECURITYNETWORK

Alle Vorteile von cloud-basierten Bedrohungsinformationen innerhalb Ihres Perimeters

Standardsicherheitslösungen benötigen bis zu vier Stunden, um die von Kaspersky Lab täglich entdeckten, beinahe 310.000 neuen Schadprogramme zu erkennen, zu erfassen und abzuwehren. Die Weitergabe von Bedrohungsinformationen über das Kaspersky Private Security Network erledigt dies in 30 bis 40 Sekunden.

Die Cyberkriminalität nimmt nicht nur stetig zu, sie wird auch immer raffinierter: Während es sich bei 70 % der Bedrohungen, denen Unternehmen ausgesetzt sind, um bekannte Malware handelt, sind 30 % unbekannte, hoch entwickelte Bedrohungen, gegen die herkömmliche signaturbasierte Sicherheitsverfahren allein machtlos sind.

Das Kaspersky Security Network stellt die Security Intelligence von Kaspersky Lab jedem Partner oder Kunden zur Verfügung, der mit dem Internet verbunden ist, und garantiert so schnelle Reaktionszeiten, geringe Fehlalarmquoten und maximalen Schutz – selbst vor unbekannten, hoch entwickelten Bedrohungen.

Obwohl alle vom Kaspersky Security Network verarbeiteten Informationen vollständig anonymisiert werden und damit ihrem Ursprung nicht mehr zugeordnet werden können, ist sich Kaspersky Lab bewusst, dass für einige Unternehmen eine absolute Datensperre unumgänglich ist. Bisher hatte dies zur Folge, dass diese Unternehmen auf cloud-basierte Sicherheitsservices verzichten mussten.

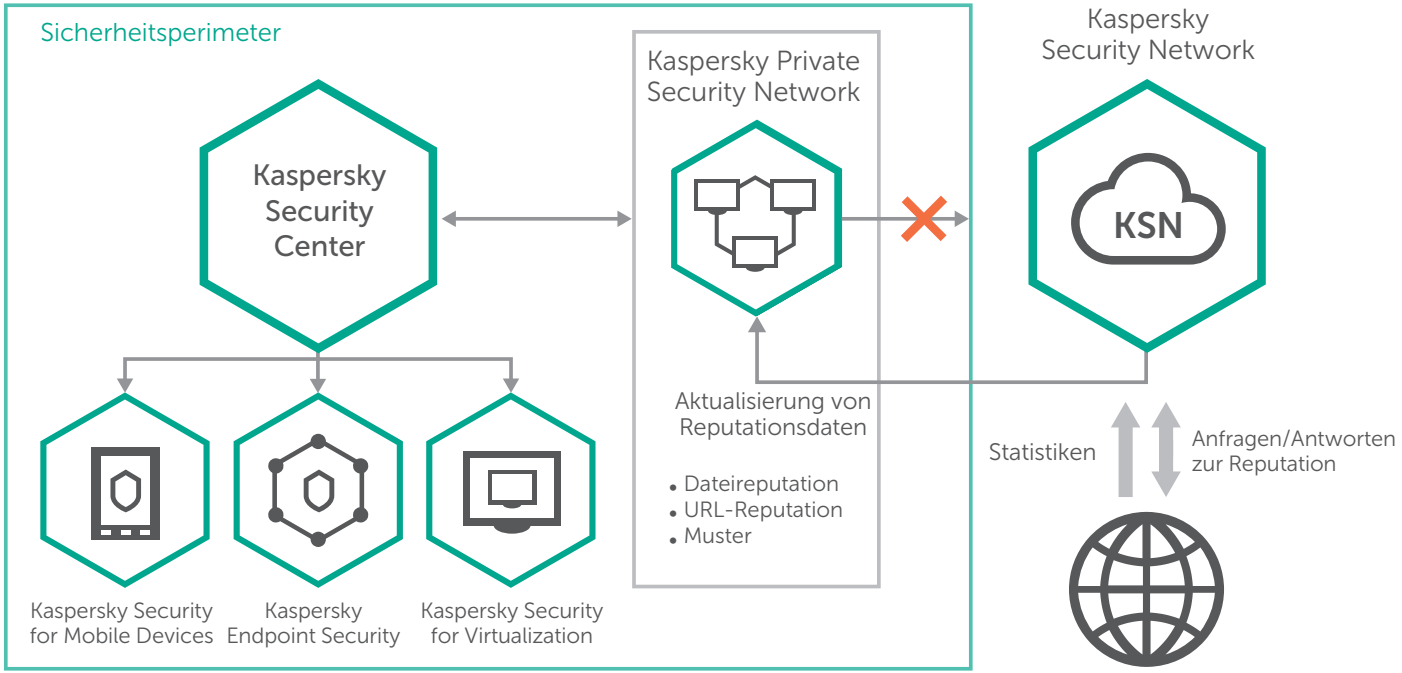
DIE LÖSUNG: KASPERSKY PRIVATE SECURITY NETWORK

Für Kunden mit diesen Anforderungen hat Kaspersky das Kaspersky Private Security Network entwickelt. Dieses ermöglicht es Unternehmen, fast alle Vorteile der cloud-basierten Sicherheit zu nutzen, ohne dass dabei Daten ihren gesicherten Perimeter verlassen. Damit bildet es die vollständig private, lokale Version des Kaspersky Security Network für ein einzelnes Unternehmen.

Das Kaspersky Private Security Network nimmt sich wichtiger Cybersicherheitsaspekte in Unternehmen an, ohne dass dabei ein einziger Datensatz das lokale Netzwerk verlässt. Kaspersky Private Security Network:

- Den Ursprung von Malware identifizieren und die Ausbreitung verhindern
- Zwischen gezielten Angriffen und allgemeinen Bedrohungen unterscheiden
- Den durch Cybersicherheitsvorfälle hervorgerufenen Schaden minimieren
- Anforderungen an Vorfallsuntersuchung und Korrekturmaßnahmen überprüfen
- Die Anzahl von Fehlalarmen verringern
- Behördliche Auflagen, Sicherheits- und Datenschutznormen einhalten

Das KPSN kann auch für andere Lösungen in Unternehmen als wichtige Informationsquelle dienen: Security Operations Center (SOC), SIEM-System, Governance, Risikomanagement und Compliance-, Forensik- und Sanierungsprozesse. All diese Funktionen lassen sich in die Daten-Feeds integrieren und liefern so wichtige Erkenntnisse über die Sicherheit und Bedrohungsbereitschaft Ihres Unternehmens.



SECURITY FOR DATA CENTERS

Speziell für Rechenzentren entwickelte Sicherheitstechnologien

Die Aufrechterhaltung des Geschäftsbetriebs bleibt für Unternehmen bei der Auswahl einer Sicherheitslösung von entscheidender Bedeutung.

Großunternehmen verarbeiten immer größere Datenmengen. Um mit dieser Entwicklung Schritt zu halten, müssen Unternehmen nicht nur eine neue Strategie entwickeln, wie sie Datenspeicherung und -zugriff organisieren, sondern auch wie sie für die Sicherheit und Integrität ihrer Daten garantieren können. Je größer die Infrastruktur, umso größer die vorgehaltene Datenmenge und umso leistungsstärker und zuverlässiger auch die Sicherheitslösung, die für ihren Schutz vonnöten ist.

Unabhängig davon, ob Sie Ihr eigenes Rechenzentrum betreiben oder den Service eines IaaS-Anbieters (Infrastructure-as-a-Service) nutzen: Ihre Sicherheitslösung sollte nicht nur für den effektiven und unterbrechungsfreien Schutz Ihrer kritischen Daten sorgen, sondern dabei auch die Performance des Rechenzentrums nicht beeinträchtigen.

Jedes Rechenzentrum bietet eine Vielzahl von Angriffsflächen, die von Angreifern genutzt werden könnten. Und je größer Ihr Rechenzentrum wird, umso komplexer wird es zwangsläufig auch, und bietet Cyberkriminellen damit sogar noch mehr Möglichkeiten. Ihre Sicherheitslösung muss effektiv skalierbar sein, d. h. sich vollständig in die vorhandene IT-Umgebung integrieren lassen. Ansonsten wird sie die Performance des Rechenzentrums beeinträchtigen und die betriebliche Effizienz mit der Zeit insgesamt verschlechtern.

DIE LÖSUNG: KASPERSKY SECURITY FOR DATA CENTERS

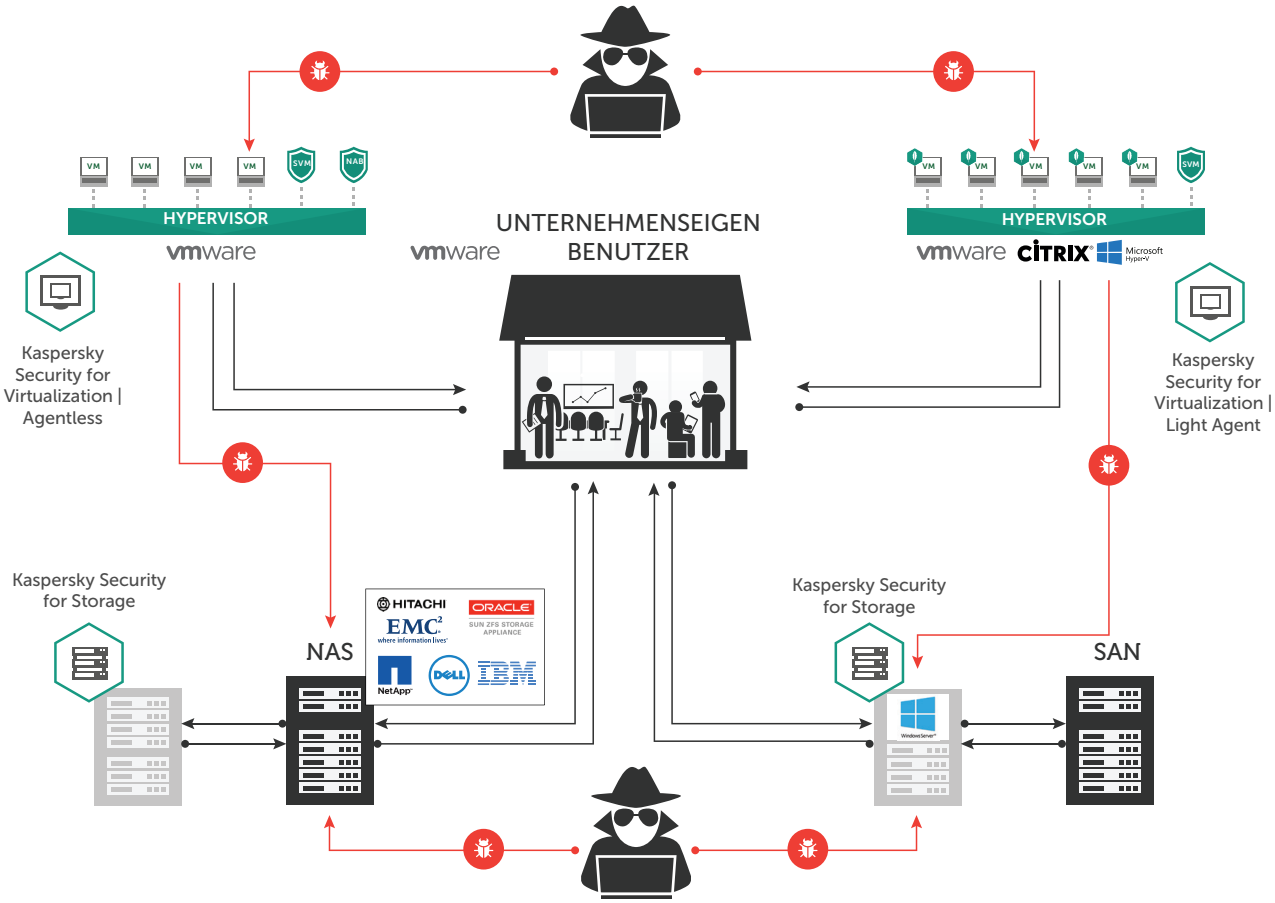
Wir bieten Lösungen, die sich auf den Schutz der beiden zentralen Bereiche Ihres Rechenzentrums konzentrieren: Ihre virtualisierte Infrastruktur und Ihre Speichersysteme. Unsere Lösungen sind speziell auf Systeme mit mehreren Hypervisoren und Speichersystemen zugeschnitten. Sie bieten die folgenden Vorteile:

- Speziell auf die gängigsten Virtualisierungsplattformen zugeschnitten, z. B. VMware, Citrix, Microsoft und KVM
- Sicherheit für NAS-Systeme (Network Attached Storage) wie EMC, NetApp, DELL, IBM, Hitachi und Oracle

Kaspersky Security for Data Centers basiert auf unserer vielfach ausgezeichneten Sicherheits-Engine und fungiert als einzelne, integrierte und einfach zu verwaltende Plattform, die problemlos in verschiedene Rechenzentrumskonfigurationen integriert werden kann. Die zentrale Verwaltung hat den Vorteil, dass einheitliche Sicherheitsrichtlinien im gesamten Rechenzentrum angewendet werden können, was dazu beiträgt, die Betriebskosten zu senken.

DIESE UMFASSENDE LÖSUNG BIETET IHNEN FOLGENDES:

- Schützt Ihre Daten und Systeme vor Cyberattacken
- Bietet effektive Tools zur Erhaltung der Performance und geschäftlichen Kontinuität
- Ermöglicht die Verwaltung aller virtualisierten und physischen Systeme im Rechenzentrum über eine zentrale Konsole


HYPERVISOR
vmware
HYPERVISOR
vmware CITRIX Microsoft Hyper-V
UNTERNEHMENSEIGEN BENUTZER
vmware
Kaspersky Security for Virtualization | Agentless
Kaspersky Security for Virtualization | Light Agent
Kaspersky Security for Storage
Kaspersky Security for Storage
NAS
SAN
HITACHI
EMC²
ORACLE
SUN ZFS STORAGE APPLIANCE
NetApp
DELL
IBM

SECURITY INTELLIGENCE SERVICES

Threat Intelligence, Security Services und Sicherheitsschulungen

60 % der Großunternehmen nutzen Threat Intelligence Services als Teil ihrer Sicherheitsstrategie

Heutige Bedrohungen werden zunehmend komplexer und auch Cyberkriminelle entwickeln ständig neue Angriffsmethoden zur Überwindung von Sicherheitstechnologien. Herkömmliche Sicherheitslösungen, wie z. B. Virenschutz, Firewall und Systeme zur Angriffsüberwachung, reichen nicht mehr aus, um einen umfassenden Schutz zu gewährleisten. Heute muss ein neuartiger Sicherheitsansatz, der auf menschlichem Eingreifen basiert, diese Sicherheitslücke schließen.

Angesichts einer ständig wachsenden Menge immer ausgeklügelterer Bedrohungen ist die Sensibilisierung und Schulung von Mitarbeitern im Bereich der Cybersicherheit für Unternehmen zu einer unerlässlichen Grundvoraussetzung geworden.

Indem wir unser Wissen mit unseren Kunden teilen, hilft Kaspersky Lab Unternehmen dabei, sich vor Bedrohungen zu schützen. Unsere große Bandbreite von Intelligence Services trägt dazu bei, dass das Security Operations Centre (SOC) und/oder IT-Sicherheitsteam über die erforderliche Ausstattung verfügt, um das Unternehmen vor den aktuellsten Online-Bedrohungen zu schützen.

CYBERSICHERHEITSSCHULUNG

Sicherheitsmitarbeiter müssen in den erweiterten Sicherheitstechniken ausgebildet werden, die eine wichtige Komponente für ein effektives Bedrohungsmanagement und Strategien zur Risikominimierung im Unternehmen bilden. Darüber hinaus sollten alle Mitarbeiter ein allgemeines Verständnis der bestehenden Gefahren haben und mit sicheren Arbeitsmethoden vertraut sein.

Wir bieten eine Reihe von Schulungen zur Sensibilisierung im Bereich Cybersicherheit sowie ein breites Portfolio an Schulungsprogrammen in digitaler Forensik und Malware-Analyse an – beginnend bei den Grundlagen bis hin zu Spezialwissen.

- **Mit Cybersecurity Awareness** können Unternehmen das Sicherheitswissen ihrer Mitarbeiter verbessern – und gleichzeitig etwas für ihre eigene Sicherheit tun.
- **Security Education für IT-Sicherheitsprofis** (alle Niveaus) verbessern die Kenntnisse und Fertigkeiten Ihrer unternehmensinternen Sicherheitsfachleute, um so das Risiko von Vorfällen zu minimieren.

THREAT INTELLIGENCE

Besitzt Ihr SIEM-System geeignete Funktionen zur Erkennung von Cyberbedrohungen? Können Sie sicher sein, dass Sie rechtzeitig über die gefährlichsten Bedrohungen informiert werden? Unser Portfolio an Threat Intelligence Services gibt Unternehmen die Mittel an die Hand, mit diesen Risiken umzugehen:

- **Threat Data Feeds:** Erweitern Sie Ihre SIEM-Lösung, und verbessern Sie Ihre Forensikfunktionen mithilfe von Bedrohungsinformationen von Kaspersky Lab.
- **APT Intelligence Reporting** ermöglicht einen exklusiven und frühzeitigen Zugang zu Informationen über hochkarätige Cyberspionage-Aktionen, darunter auch Gefährdungsindikatoren, sogenannte Incidents od Compromise (IOC).
- **Kundenspezifische Threat Intelligence Reportings** identifizieren die extern verfügbaren, entscheidenden Komponenten Ihres Netzwerks.

EXPERTENSERVICES

Reicht Ihre interne Fachkompetenz aus, um einen Sicherheitsvorfall zu beheben? Sind Ihre IT-Infrastruktur bzw. bestimmten Programme umfassend vor möglichen Cyberattacken geschützt? Unsere Expertenservices sind darauf ausgelegt, dieser Risiken Herr zu werden:

- **Penetrationstests:** Lernen Sie, die Schwachpunkte Ihrer Infrastruktur zu identifizieren und Schäden durch Cyberattacken zu vermeiden. Gewährleisten Sie die Einhaltung behördlicher Auflagen sowie von Branchen- und Unternehmensstandards (z. B. PCI DSS).
- **Application Security Assessment** deckt Schwachstellen in beliebigen Anwendungstypen auf, von umfangreichen cloud-basierten Lösungen, ERP-Systemen, Online-Banking und anderen speziellen Geschäftsanwendungen bis hin zu integrierten und mobilen Anwendungen auf unterschiedlichen Plattformen.
- **Digitale Forensik und Malware-Analyse:** Detaillierte Rekonstruktion von Sicherheitsvorfällen durch umfassende Berichte inklusive Korrekturmaßnahmen.

DDOS PROTECTION

Umfassender Schutz vor allen Arten von DDoS-Attacken

Eine einzige DDoS-Attacke kann je nach Größe des Unternehmens einen Schaden zwischen 52.000 und 444.000 US-Dollar anrichten. Und was kostet es, einen DDoS-Angriff vorzubereiten? Ungefähr 200 US-Dollar...

Angesichts sinkender Kosten für einen DDoS-Angriff (Distributed Denial of Service) hat die Anzahl der Attacken zugenommen. Zugleich sind die Angriffe mittlerweile sehr viel raffinierter und schwerer abzuwehren. Der veränderliche Charakter dieser Angriffsmethode macht eine gründlichere Art der Verteidigung erforderlich.

Im Gegensatz zu Virenattacken, die in der Regel automatisch ablaufen, sind DDoS-Attacken von menschlichem Sachverstand und Wissen abhängig. Normalerweise machen sich Cyberkriminelle im Vorfeld mit ihrem Angriffsziel vertraut, bewerten vorhandene Schwachstellen und suchen sorgfältig das angemessene Instrument zum Angriff aus. Während ein Angriff läuft, ändern die Cyberkriminellen ständig ihre Taktik und passen ihre Vorgehensweise sowie die verwendeten Tools an – alles mit dem Ziel, den angerichteten Schaden zu maximieren.

Zum Schutz vor DDoS-Angriffen benötigen Unternehmen eine Lösung, die einen Angriff so früh wie möglich erkennt.

DIE LÖSUNG: KASPERSKY DDOS PROTECTION

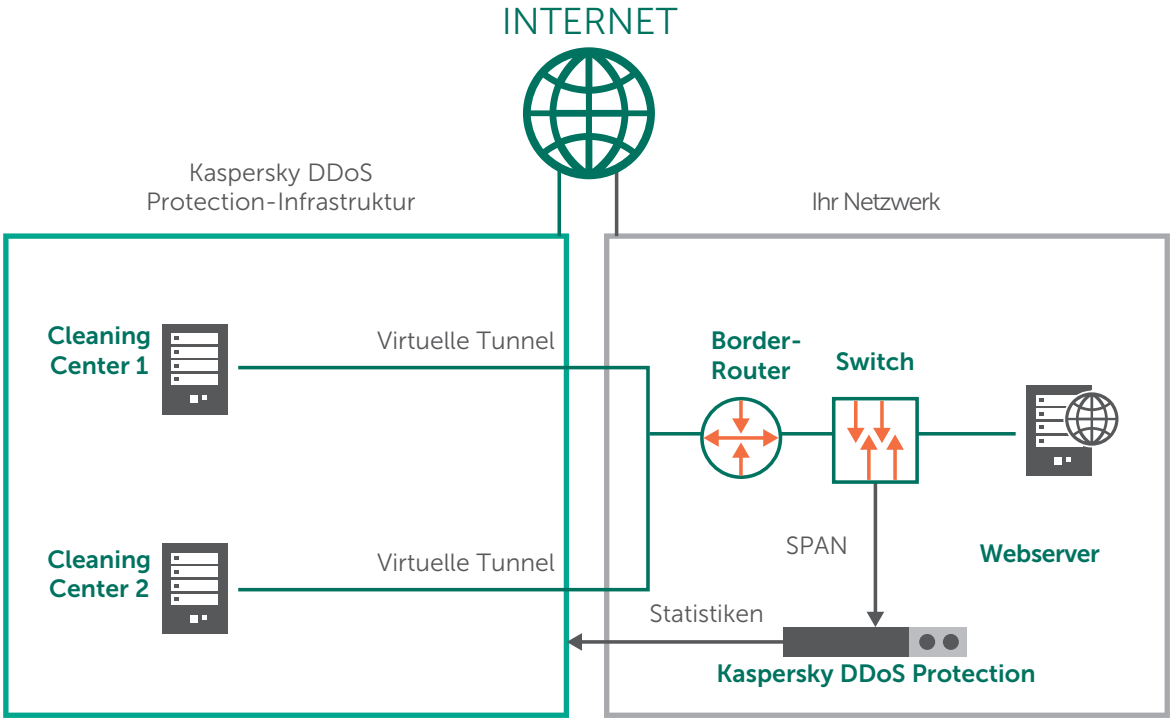
Kaspersky DDoS Protection bietet einen umfassenden, integrierten Schutz vor DDoS-Angriffen und eine Lösung zur DDoS-Minimierung, die alle Maßnahmen für den Schutz Ihres Unternehmens vor allen Arten von DDoS-Angriffen abdeckt.

Kaspersky DDoS Protection beginnt mit spezieller Sensorsoftware, die in der Infrastruktur des Kunden ausgeführt wird und den Netzwerkverkehr überwacht. Durch die fortlaufende Generierung von statistischen Werten und Verhaltensanalysedaten wird die Software mit der Zeit immer besser darin, selbst geringfügige Anomalien zu entdecken, welche für den Beginn eines DDoS-Angriffs charakteristisch sind. Bei Auftreten eines DDoS-Angriffs alarmieren wir bei Kaspersky Lab den Kunden und geben ihm die Möglichkeit, seinen Netzwerkverkehr an eines unserer Cleaning Center umzuleiten. Zum Schutz seiner Privatsphäre hat keiner unserer Prozesse Einblicke in die Inhalte seines Datenverkehrs: Es werden lediglich Metadaten ausgewertet.

AUFBAU VON KASPERSKY DDOS PROTECTION

Diese umfassende Verteidigungslösung bietet Ihnen Folgendes:

- Spezielle Softwaresensoren, die innerhalb der IT-Infrastruktur am Kundenstandort ausgeführt werden
- Ein verteiltes Netzwerk aus Cleaning Centern
- Rechtzeitige Warnungen bei bevorstehenden Angriffen
- Sicherheit für den Datenverkehr: Das Bereinigungszentrum filtert den Datenverkehr nur während eines Angriffs
- Detaillierte Analysen und Berichte zum Ablauf von erfolgten Angriffen



AUFBAU VON KASPERSKY DDOS PROTECTION

FRAUD PREVENTION

Minderung des Betrugsrisikos bei Finanztransaktionen, die online oder per Mobilgerät ausgeführt werden

Alleine im ersten Quartal 2015 haben Kaspersky-Lösungen die Computer von 929.082 Endbenutzern vor dem Versuch geschützt, Malware zu starten, um Geld per Online-Banking zu stehlen. Dieser Wert stellt einen Anstieg um 64,3 % gegenüber dem vorherigen Quartal dar.

Cyberkriminelle werden immer geschickter bei der Entwicklung von ausgeklügelten Tools, die herkömmliche Schutzmaßnahmen umgehen, den Weg in Banking-Systeme ebnen, Zugriff auf Kundenkonten ermöglichen und ihnen die Auslösung und Manipulation von Transaktionen gestatten.

Noch vor einigen Jahren schien es ausreichend, nach dem Auftreten eines Betrugsversuchs zu reagieren. Diese Herangehensweise reicht heute jedoch nicht mehr aus, um den Schutz zu bieten, den Banken brauchen und Kunden fordern.

Deloitte ist der Ansicht, dass der Finanzdienstleistungssektor dem größten Risiko bezüglich Cybersicherheit ausgesetzt ist und gezwungen sein wird, die Sicherheit, Wachsamkeit und Widerstandsfähigkeit seiner Cybersicherheitsmodelle durch die Aufstockung von Ressourcen zu verbessern.

DIE LÖSUNG: KASPERSKY FRAUD PREVENTION

Kaspersky Fraud Prevention verstärkt das vorhandene Sicherheitssystem einer Bank und bietet ein ganz neues Niveau an Schutz vor Betrug. Die Lösung schützt die Online-Konten, Computer und mobilen Geräte von Benutzern und die Systeme der Bank. Indem Kaspersky Fraud Prevention Konten schützt und für die Sicherheit bei Kundentransaktionen sorgt, unterstützt unsere Lösung Banken dabei, das Vertrauen von Kunden zu gewinnen.

Kaspersky Fraud Prevention hindert Hacker daran, ihre Ziele zu erreichen, indem Kontenübernahmen, die Manipulation von Transaktionen und Identitätsdiebstahl frühzeitig vereitelt werden. Auf diese Weise wird Betrug verhindert, noch bevor er stattfinden kann.

Die Lösung bietet der Betrugsabteilung einer Bank darüber hinaus die Möglichkeit, exakte Informationen zu jedem einzelnen Vorfall zu erfassen, einschließlich der verwendeten Methoden, um Zugriff auf ein Konto zu erhalten. Mit diesen Informationen lässt sich u. a. nachweisen, dass eine Bank in einem bestimmten Betrugsfall nicht regresspflichtig ist, wodurch die Kosten für Schadenersatz und Entschädigungen sinken.

Kaspersky Fraud Prevention fügt der vorhandenen Betrugsprävention von Banken eine wichtige Schicht hinzu.

- **Kaspersky Fraud Prevention Clientless Malware Detection** bietet serverseitige Technologien, die Ihren gesamten Kundenstamm schützen, unabhängig davon, welches Gerät oder welche Plattform Ihre Kunden nutzen. Das System erkennt den Zugriff über das infizierte Gerät eines Kunden so früh wie möglich.
- **Kaspersky Fraud Prevention for Mobile** hilft dabei, Benutzer zu schützen, die über Mobilgeräte (Android, iOS und Windows Phone) auf ihre Bankkonten zugreifen.
- **Kaspersky Fraud Prevention for Endpoints** wird auf den Windows-PCs und Mac-Computern Ihrer Kunden ausgeführt und verhindert die zugrundeliegenden Ursachen von Malware und Online-Attacken.
- **Kaspersky Fraud Prevention User Assessment Service** schützt Online-Bankkonten vor Kontenübernahmen durch Kriminelle, die versuchen, sich Zugang zu legitimen Kundenkonten zu verschaffen.

Diese umfassende Betrugsschutzlösung bietet Ihnen Folgendes:

- Multi-Channel-Sicherheit für Online-Banking und -Zahlungen
- Frühzeitige Eliminierung der Betrugsursache, sodass Ihre Bank schneller reagieren kann
- Schutz aller Benutzer – unabhängig vom verwendeten Gerät
- Reibungslose Sicherheit für eine ungestörte Benutzererfahrung
- Stärkere Kundenbindung, Gewinnung von Neukunden sowie höhere Akzeptanz und Nutzung von margenstarken Online- und Mobile-Banking-Services

EMBEDDED SYSTEMS SECURITY

Leistungsstarker Schutz speziell für kritische Bezahlungssysteme

Insbesondere eingebettete Systeme, sogenannte „embedded systems" stellen ein Sicherheitsproblem dar, da sie geographisch oft weit verbreitet und daher schwer zu verwalten sind und nur selten aktualisiert werden. Geldautomaten und POS-Systeme sind ein beliebtes Ziel für Cyberkriminelle, da sie echtes Geld und Kreditkartendaten verarbeiten. Deshalb benötigen diese ein höchst fokussiertes und intelligentes Sicherheitssystem.

Der Payment Card Industry Data Security Standard (PCI DSS) reguliert viele der technischen Anforderungen und Einstellungen für Systeme zur Abwicklung von Kreditkartentransaktionen. Die Sicherheitsvorschriften für Geldautomaten und POS-Systeme scheinen jedoch nur den Virenschutz abzudecken. Ein rein auf Virenschutz basierender Ansatz ist im Fall der aktuellen Bedrohungen von Geldautomaten und POS-Systemen jedoch nur von eingeschränkter Wirkung, was bei den neuesten Angriffen deutlich wurde. Die Zeit ist gekommen, Ansätze wie Gerätekontrolle und Default Deny auf Ihre kritischen eingebetteten Systeme anzuwenden, da sich diese Technologien bereits in anderen Sicherheitskontexten bewährt haben. Auf den meisten Geldautomaten werden immer noch Betriebssysteme der Windows XP-Familie ausgeführt, obwohl nach zwölf Jahren am 12. Januar 2016 der Support für Windows XP Embedded und am 12. April 2016 der für Windows Embedded for Point of Service eingestellt wurde. Für das Betriebssystem Windows XP wird es keine weiteren Sicherheits-Updates und auch keinen technischen Support mehr geben.

Der Wechsel der Software von Geldautomaten und POS-Systemen ist im Allgemeinen ein langwieriger, kostspieliger und komplexer Prozess. Abgesehen vom Ersatz der Software bedeutet dies oft auch den Austausch einer nach wie vor funktionsfähigen, wenn auch technisch veralteten Hardware.

DIE LÖSUNG: KASPERSKY EMBEDDED SYSTEMS SECURITY

Kaspersky Lab hat eine Sicherheitslösung entwickelt, die sich speziell an Unternehmen richtet, die Geldautomaten und POS-Systeme betreiben. Hierbei werden die einzigartige Funktionalität und das Betriebssystem, der Kanal sowie die Hardware-Anforderungen berücksichtigt, während Windows XP vollständig unterstützt wird.

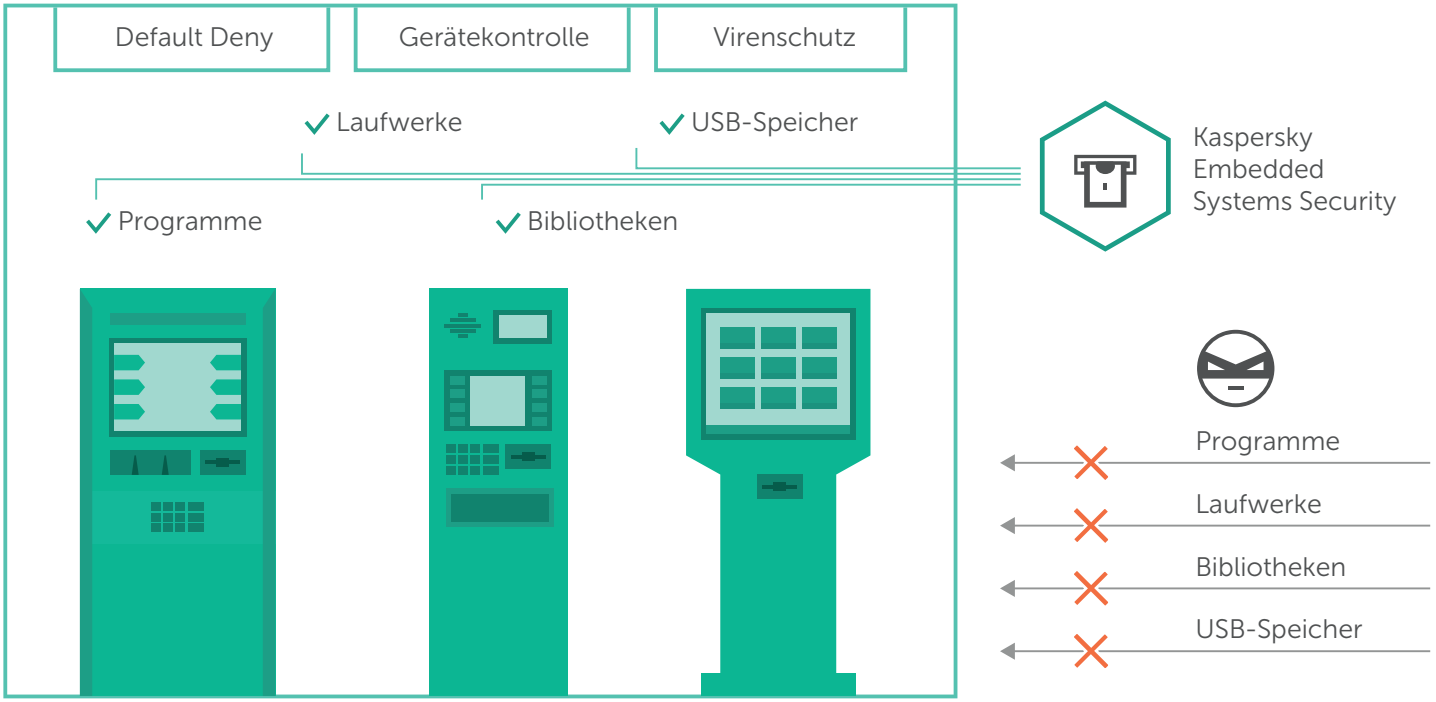
Default Deny für Anwendungen, Laufwerke und Bibliotheken sowie eine unterstützende Funktion zur Gerätekontrolle bilden den einzigen Ansatz, mit dem die Sicherheit kritischer, technisch veralteter Systeme gewährleistet werden kann, die sich weiterhin in Betrieb befinden.

Kaspersky Embedded Systems Security bietet einen „Nur Default Deny"-Betriebsmodus, für den lediglich 256 MB RAM und nur 50 MB Speicherplatz auf der Festplatte notwendig sind – ideal für Systeme, die auf Windows XP basieren und mit Low-End-Hardware betrieben werden. Ein optionales Antiviren-Modul bietet zudem einen Modus, in dem bei Bedarf manuelle Scans ausgeführt werden können. Dieses Modul basiert auf dem Kaspersky Security Network, das bei Bedarf auch Patch Management-Funktionen umfasst.

Daher erfüllt diese Einzellösung drei verschiedene Kriterien:

- Effiziente Sicherheit für „schwierig zu verwaltende" Systeme
- Einhaltung der PCI DSS-Anforderungen 5.1, 5.1.1, 5.2, 5.3 und 6.2
- Komfortable Zeitplanung für den Ersatz veralteter Systeme und Hardware

Kaspersky Embedded Systems Security verringert die Sicherheitsrisiken für eingebettete Systeme. Die Lösung wurde speziell für Geldautomaten und POS-Systeme entwickelt und schützt die für diese Architekturen typischen Angriffsflächen, während gleichzeitig entsprechende Hardware- und Effizienz-Aspekte berücksichtigt werden. Eine einzige intuitive Konsole bietet Ihnen die Kontrolle und Transparenz, die Sie benötigen, um eine effiziente, mehrstufige Sicherheitslösung für Ihre Endpoints, unerlässlichen Systeme und die gesamte IT-Infrastruktur zu verwalten.



INDUSTRIAL CYBERSECURITY

Spezieller Schutz für industrielle Steuerungssysteme

Früher reichten „Luftschleusen" zwischen Industrieanlagen und der Außenwelt aus, um ausreichenden Schutz zu bieten, aber dies ist nicht länger der Fall. In Untersuchungen konnte vor kurzem nachgewiesen werden, dass 35 % der Fehlfunktionen in industriellen Netzwerken auf Cyberattacken zurückgehen.

Angriffe auf industrielle Systeme haben in den letzten Jahren stark zugenommen. Unterbrechungen der Lieferkette und der Geschäftsaktivitäten wurden in den letzten drei Jahren als globales Geschäftsrisiko Nr. 1 eingestuft. Risiken im Bereich Cybersicherheit stellen die größte aufkommende Bedrohung dar. Die Risiken für Unternehmen mit industriellen oder anderen kritischen Infrastruktursystemen sind heute so hoch wie nie zuvor.

Die industrielle Sicherheit hat Konsequenzen, die weit über den Schutz von Unternehmen und geschäftlicher Reputation hinausgehen. In vielen Fällen spielen beim Schutz von industriellen Systemen vor Cyberbedrohungen ökologische, soziale und makroökonomische Faktoren eine erhebliche Rolle. Wichtige Infrastruktureinrichtungen müssen stets mit dem größtmöglichen Schutz vor einer wachsenden Vielfalt von Bedrohungen ausgestattet sein.

Gleichzeitig benötigen Industrieanlagen eine integrierte Lösung, die die Verfügbarkeit industrieller Prozesse durch die Erkennung und Vermeidung von Aktionen (beabsichtigt oder unbeabsichtigt) erhöht, die zu Unterbrechungen oder dem Stillstand wichtiger Prozesse führen.

DIE LÖSUNG: KASPERSKY INDUSTRIAL CYBERSECURITY

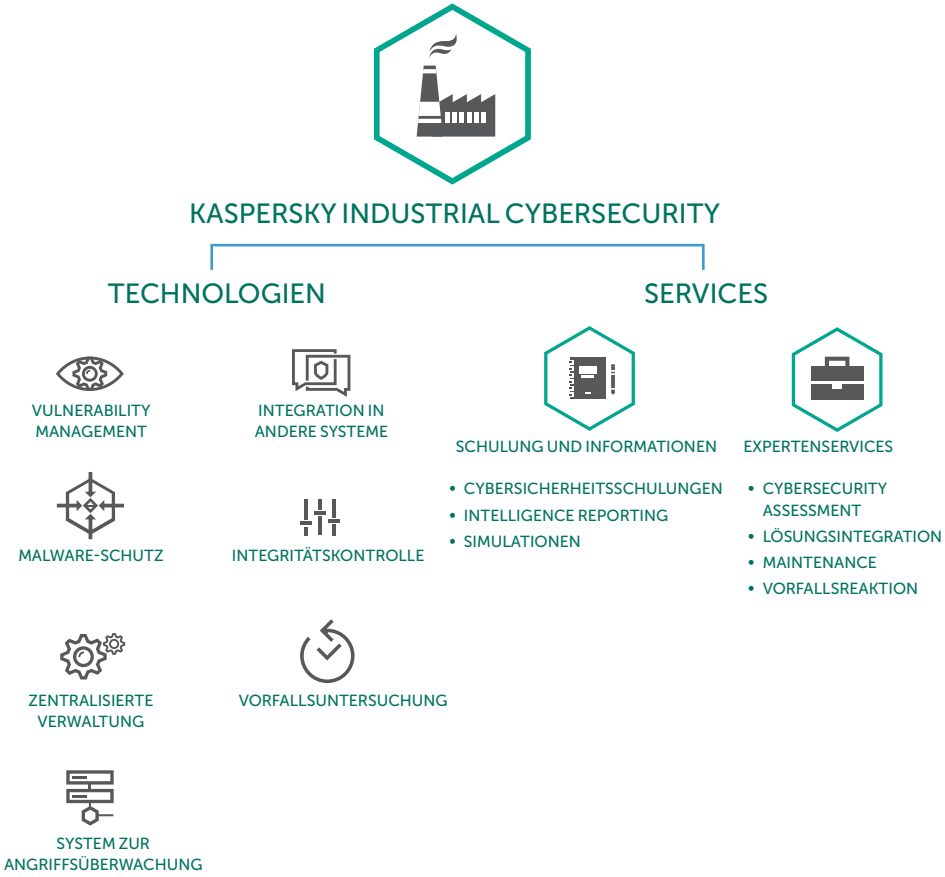
Kaspersky Industrial CyberSecurity ist eine Lösung, die auf die speziellen Anforderungen industrieller Cybersicherheit zugeschnitten ist. Ein besonderer Schwerpunkt liegt dabei auf der Aufrechterhaltung unterbrechungsfreier technologischer Prozesse. Dank der flexiblen und vielseitigen Einstellungen lässt sich die Lösung so konfigurieren, dass die speziellen Anforderungen einzelner industrieller Einrichtungen erfüllt werden.

Die Lösung ist auf den Schutz komplexer Umgebungen ausgelegt, die auf verschiedenen industriellen Steuersystemen basieren. Die Vielseitigkeit von Kaspersky Industrial CyberSecurity ermöglicht es Unternehmen, die Lösung exakt auf die Anforderungen der jeweiligen Umgebung für das industrielle Steuersystem zuzuschneiden. Nachdem die Infrastruktur von Kaspersky-Spezialisten eingehend geprüft wurde, erfolgt eine optimale Konfiguration von Sicherheitstechnologien und -services.

Der Ansatz von Kaspersky Lab für den Schutz industrieller Systeme basiert auf dem in über zehn Jahren gewachsenen Know-how in der Aufdeckung und Analyse einiger der ausgeklügeltsten Bedrohungen für Industrieanlagen weltweit. Dank unserer umfassenden Kenntnisse und Einsichten im Bereich Systemschwachstellen sowie unserer engen Zusammenarbeit mit den führenden Vollzugs- und Regierungsbehörden sowie Industrieorganisationen, darunter Interpol, das Industrial Internet Consortium, verschiedene CERTS und Behörden, ist es uns gelungen, beim Erfüllen der speziellen Anforderungen der industriellen Cybersicherheit eine Führungsrolle zu übernehmen.

Diese Speziallösung bietet Ihnen Folgendes:

- Umfassende Cybersicherheit für industrielle Umgebungen
- Vollständige Palette von Sicherheitsservices, vom Cybersicherheits-Assessment bis hin zur Vorfallsreaktion
- Spezielle Sicherheitstechnologien, die eigens für industrielle Systeme entwickelt wurden
- Geringere Ausfallzeiten und weniger Verzögerungen bei technologischen Prozessen



TARGETED SECURITY-LÖSUNGEN

Targeted Security-Lösungen stellen eine kostengünstige Möglichkeit dar, Kaspersky-Technologien gezielt dort einzusetzen, wo sie benötigt werden.

Einheitslösungen sind nicht in der Lage, den speziellen Anforderungen unterschiedlicher Geräte gerecht zu werden – alle Geräte im Unternehmensnetzwerk benötigen zuverlässigen und speziellen Schutz. Die Bandbreite unserer zielgerichteten Lösungen stellt den Schutz einzelner Netzwerkkomponenten sicher – von File- und Mail-Servern, Internet-Gateways und Collaboration-Servern.

SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server schützt den E-Mail-Verkehr vor Spam, Phishing-Links und Malware. Die Lösung unterstützt gängige E-Mail-Plattformen wie Microsoft Exchange, Linux Mail Server und IBM Domino. Außerdem wurde ein DLP-Modul (Data Loss Prevention), mit dem die Weitergabe von vertraulichen Informationen kontrolliert werden kann, für die E-Mail-Plattform Microsoft Exchange implementiert.

SECURITY FOR FILE SERVER

Kaspersky Security for File Server ist eine effiziente, zuverlässige und skalierbare Lösung für den Schutz von Dateispeicherlösungen mit allgemeinem Zugriff ohne erkennbare Beeinträchtigung der Systemleistung. Die Lösung bietet Schutz vor Malware für Linux- und Windows-Server.

SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway kontrolliert den HTTP- und FTP-Datenverkehr und bietet umfassenden Perimeterschutz vor Malware und gefährlichen Programmen durch Blockierung von aktuellen und potentiellen Bedrohungen.

SECURITY FOR COLLABORATION

Kaspersky Security for Collaboration bietet maximale Sicherheit für die gesamte SharePoint-Umgebung und ihre Benutzer. Die Lösung kombiniert wirkungsvolle Technologien für den Schutz vor Angriffen und Datenlecks mit hohem Nutzerkomfort.

PREMIUM-SUPPORT UND PROFESSIONAL SERVICES

Eine Palette von Services, mit denen Unternehmen alle Vorteile von Kaspersky Lab-Produkten voll ausschöpfen

Wenn eine Sicherheitslücke zum Ausfall von IT-Systemen führt, kann sich dies auf den gesamten Betrieb eines Unternehmens auswirken. Um dies zu verhindern, bietet Kaspersky Lab Ihnen eine Auswahl an Premium-Support-Programmen, die dafür Sorge tragen, dass Ihre IT-Sicherheitsprobleme jederzeit mit hoher Priorität gelöst werden und Ihre geschäftlichen Abläufe reibungslos weiterlaufen.

PREMIUM-SUPPORT: MSA ENTERPRISE

Unser Maintenance-Service-Agreement-Programm (MSA) wird Unternehmen empfohlen, die auf die Kontinuität der betrieblichen Abläufe und die durchgehende Bereitstellung wichtiger Prozesse auf ihre IT-Infrastruktur angewiesen sind. MSA Enterprise ist auf Großunternehmen mit komplexen IT-Umgebungen ausgelegt, die einen eigenen persönlichen und proaktiven Support erfordern, der rund um die Uhr verfügbar ist.

PROFESSIONAL SERVICES

Unsere Sicherheitsexperten arbeiten gemäß unserer Best Practices, helfen in Ihrer gesamten IT-Unternehmensinfrastruktur beim Deployment, der Konfiguration und der Aktualisierung von Kaspersky-Produkten und arbeiten dabei im Rahmen Ihrer Richtlinien für die Änderungskontrolle.

- Unser Implementierungsservice bietet Ihnen kompetente Unterstützung, damit das Deployment Ihres Kaspersky-Produkts reibungslos verläuft und sichergestellt ist, dass Sie Best Practices befolgen, mit optimal konfigurierten Systemen arbeiten und unsere zentrale Managementsoftware optimal nutzen.
- Health Check Service: Nach einer umfassenden Prüfung der Produkteinstellungen und der Netzwerkumgebung liefern unsere Experten dem Kunden einen vollständigen Bericht einschließlich praktischer Empfehlungen, wie er die Sicherheit bzw. die Effizienz des Systems Management erhöhen kann.

Mit den Premium-Support- und Professional Services von Kaspersky Lab erhalten Sie Zugang zu Sicherheitsexperten, die Ihr Problem schnell, sicher und effektiv lösen und Ihnen außerdem noch Folgendes bieten:

- SLAs für die Vorfallsreaktion
- Maßgeschneiderte Patches
- Umgehende Reaktion auf Virenvorfälle
- Überwachung und Reporting
- Ein einziger Ansprechpartner

ÜBER KASPERSKY LAB

Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 1997 gegründet wurde. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen Einrichtungen sowie Privatanwendern weltweit. Das umfassende Sicherheitsportfolio des Unternehmens beinhaltet führenden Endpoint-Schutz sowie eine Reihe spezialisierter Sicherheitslösungen und -Services zur Verteidigung vor komplexen und neu aufkommenden Cyberbedrohungen. Mehr als 400 Millionen Nutzer und 270.000 Unternehmenskunden werden von den Technologien von Kaspersky Lab geschützt.

Weitere Informationen zu Kaspersky Lab finden Sie unter http://www.kaspersky.com/de/.

KASPERSKY lab