KASPERSKY lab

Kaspersky Security Solutions for Enterprise 2017

#TrueCybersecurity

Kaspersky Enterprise Security Solutions

Technologisch

Anti Targeted Attack

Umfassende Erkennung verschiedener Vektoren und Risikominimierung bei fortschrittlichen Bedrohungen und zielgerichteten Angriffen

Endpoint Security

Die zuverlässige mehrschichtige Endpoint-Protection-Plattform, basierend auf True Cybersecurity-Technologien

Cloud Security

Perfekt für Ihre Hybrid-Cloud

Cybersecurity Services

Mit Bedrohungsinformationen, Sicherheitsschulungen, Vorfallsreaktion und Assessments

Security Operations Center

Versorgt Ihr SOC mit den Tools und Informationen zur effizienten Erkennung und Abwehr von Bedrohungen

Fraud Prevention

Frühzeitige Erkennung plattformübergreifender Betrugsversuche in Echtzeit

Nach Branchen

Financial Services Cybersecurity

Bietet Finanzdienstleistern die nötigen Tools, um die Sicherheit zu steigern, Cybervorfälle vorherzusagen und effizient zu reagieren

Telecom Cybersecurity

Effizienter Schutz für Infrastrukturen und IT-Systeme der Telekommunikationsbranche vor den fortschrittlichsten Cyberbedrohungen

Healthcare Cybersecurity

Schutz für Healthcare-Infrastrukturen und vertrauliche medizinische Daten vor Cyberbedrohungen

Data Center Security

Ergänzung für Ihr Rechenzentrum zur Erkennung und Reaktion auf die fortschrittlichsten Cyberbedrohungen

Government Cybersecurity

Sicherheitskontrollen und -services, abgestimmt auf die Anforderungen von Regierungsbehörden und zugehörigen öffentlichen Stellen

Industrial Cybersecurity

Spezieller Schutz für industrielle Steuerungssysteme

Sicherheit für Ihr Unternehmen

Kaspersky Lab ist ein weltweites Unternehmen für Cybersicherheit, das 2017 sein 20-jähriges Jubiläum feiert. 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.

Unternehmenssicherheit ernst nehmen

Mit Sicherheitsverletzungen sind erhebliche Kosten verbunden: Die im Rahmen der Umfrage zu globalen IT-Sicherheitsrisiken von Kaspersky Lab ermittelten unmittelbaren Sanierungskosten für Großunternehmen betrugen durchschnittlich 861 000 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 Entwicklung 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 – unsere Security Intelligence. So helfen wir Unternehmen dabei, zielgerichtete Angriffe frühzeitig zu erkennen und die Risiken zu mindern, bevor größere Schäden entstehen.

Kaspersky Lab bietet eine ganzheitliche, anpassungsfähige und strategische Herangehensweise an das Thema Unternehmenssicherheit. Unsere Philosophie ist eigentlich ganz einfach: Zuverlässige Sicherheitsinformationen in Kombination mit zuverlässigen Technologien ergeben einen höchst zuverlässigen Schutz für Unternehmen.

Anti Targeted Attack

Umfassende Multi-Vector Discovery und Risikominimierung bei hoch entwickelten Bedrohungen und zielgerichteten Angriffen

Gezielte Angriffe sind langfristige Verfahren, die die Sicherheit des Unternehmens gefährden und dem Angreifer Kontrolle über die IT des angegriffenen Unternehmens geben – und sie sollen so lange wie möglich unentdeckt bleiben. Deshalb schützen herkömmliche Sicherheitstechnologien nicht vor zielgerichteten Angriffen.

Während einige Aggressoren sogenannte Advanced Persistent Threats (APTs) nutzen (die sehr effektiv sein können, jedoch auch recht kostspielig sind), sind andere „gezielte Angriffe" weitaus preisgünstiger, jedoch ähnlich verheerend in der Wirkung. Diese zielgerichteten Angriffe sorgen mit ihren grundlegenden Techniken – Social Engineering, Diebstahl von Anmeldeinformationen, legitimer Software oder sogar durch über 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, reichen sie nicht aus: Die Gesamtzahl der Sicherheitsvorfälle und -verletzungen in Unternehmen ist keineswegs rückläufig.

Trotz innovativer Technologien, wie Sandboxing, EDR und anderen Lösungen der „nächsten Generation", bleibt die Herausforderung heute die gleiche: Wie können Sie den richtigen Vorfall ermitteln, und welcher Vorfall ist mit den kritischsten Bedrohungen verbunden? Spezielle Erkennungslösungen spielen eine entscheidende Rolle bei der Identifizierung von Vorfällen, die eine weitere Untersuchung und Reaktion am dringendsten erfordern.

Hoch entwickelte, gezielte Bedrohungen können 200 Tage oder noch länger unbemerkt bleiben, während Cyberkriminelle still und leise wertvolle Informationen sammeln und/oder in wichtige Geschäftsabläufe eingreifen.

Laut unseren Erfahrungswerten kann schon ein einzelner gezielter Angriff in einem Großunternehmen Kosten von mehr als 2,5 Millionen US-Dollar verursachen, bei kleinen und mittleren Unternehmen sind es durchschnittlich 80 000 US-Dollar.

- Wenn nichts dagegen unternommen wird, richtet ein gezielter Angriff in der Regel schweren Schaden in einem Unternehmen an, z. B.:
- Umfassende finanzielle Verluste
- Verlust wichtiger Daten
- Kontrolle über offensichtlich „autorisierte" Geschäftsprozesse durch den Angreifer
- Heimliche Manipulation von Daten

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

Die Lösung: Kaspersky Anti Targeted Attack

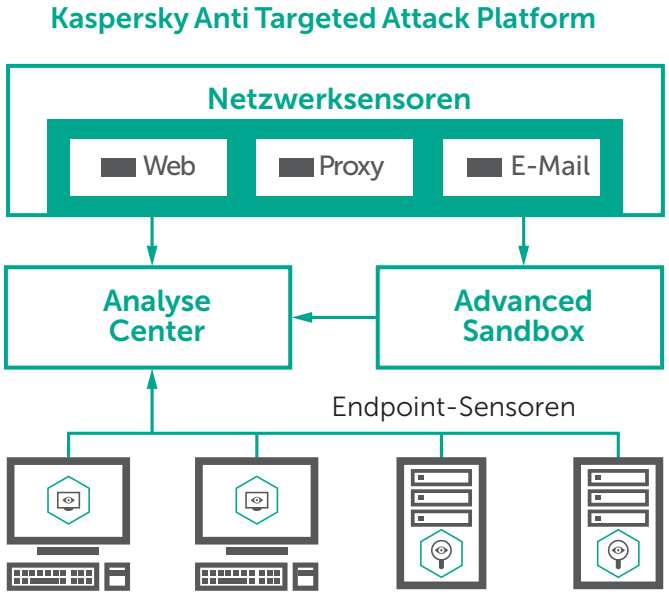
Die Kaspersky Anti Targeted Attack Platform ist Teil eines anpassungsfähigen, integrierten Ansatzes für die IT-Sicherheit in großen Unternehmen. Die Überwachung des Netzwerkverkehrs, kombiniert mit Objekt-Sandboxing und Endpoint-Verhaltensanalyse, bietet einen detaillierten Einblick in die Vorgänge der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

Durch die Korrelation mehrstufiger Ereignisse – einschließlich Netzwerk, Endpoints und Informationen über die globale 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, sehr hohe Erkennungsraten erzielen können. Kaum ein anderer Sicherheitsanbieter verfügt über die Qualität und das breite Spektrum unserer Sicherheitsdaten. Dank dieser Security Intelligence können wir Unternehmen vor den weiter zunehmenden Bedrohungen schützen

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

- **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 und ihre Verhaltensweise beobachtet werden können.
- **Leistungsstarke Analyse-Engines** – für schnelle Ergebnisse und weniger Fehlalarme. Unser Targeted Attack Analyzer bewertet Daten von Netzwerk- und Endpoint-Sensoren und erstellt für Ihr Sicherheitsteam schnell Ergebnisse der Bedrohungserkennung.



Kaspersky Private Security Network

Die umfassende Datenbank mit Bedrohungsinformationen für isolierte Netzwerke und strenge Freigabebeschränkungen

Standard-Sicherheitslösungen 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 erfolgt 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 und 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, wissen wir, dass für einige Unternehmen eine absolute Datensperre unumgänglich ist. Bisher hatte dies zur Folge, dass diese Unternehmen auf Cloud-basierte Sicherheitsservices verzichten mussten.

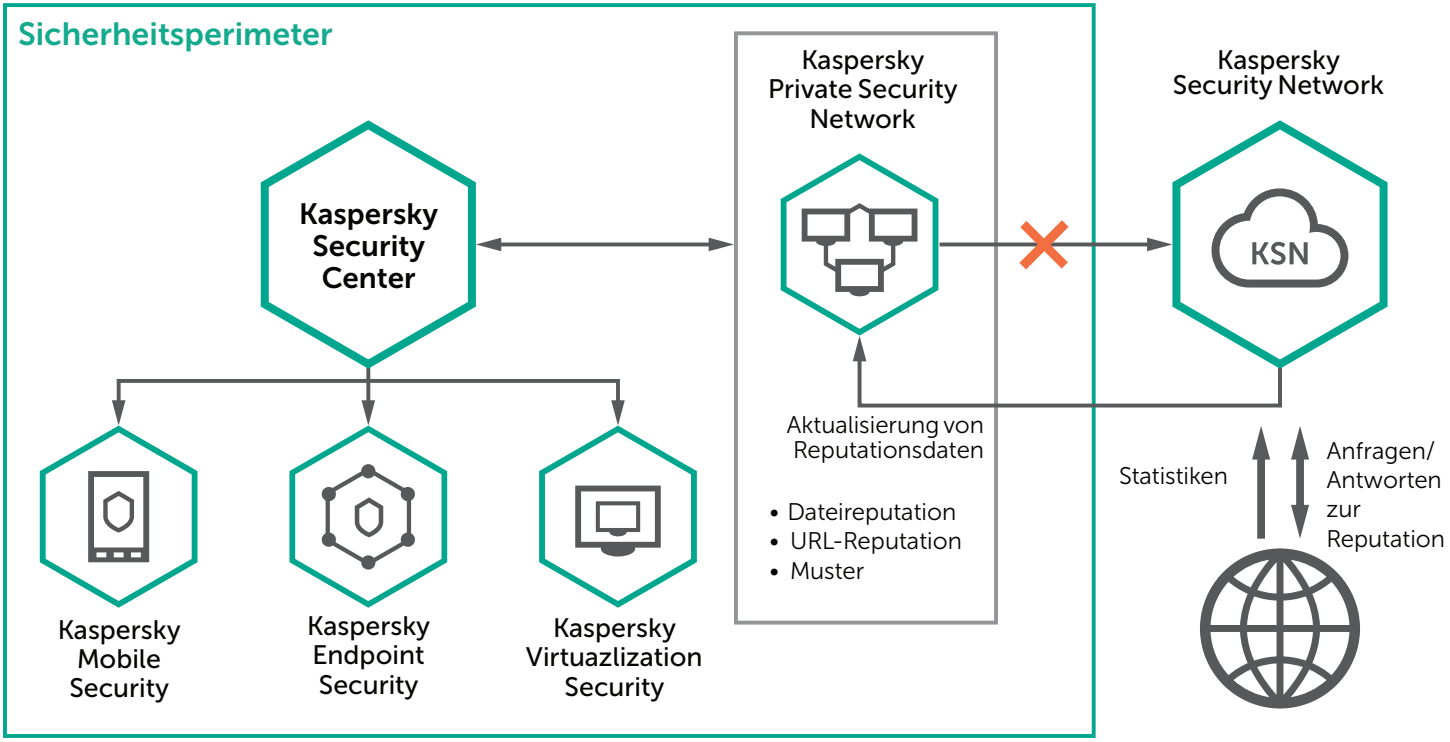
Die Lösung: Kaspersky Private Security Network

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 übernimmt wichtige Funktionen im Hinblick auf die Cybersicherheit, ohne dass dabei ein einziger Datensatz das lokale Netzwerk verlässt. Das Kaspersky Private Security Network:

- Bietet Zugriff auf globale Statistiken zu URLs und Dateien
- Kategorisiert URLs und Dateien als schädliche oder zulässige Objekte
- Minimiert den bei Cybersicherheitsvorfällen verursachten Schaden durch Bedrohungserkennung in Echtzeit
- Kann einzigartige kundenspezifische und Drittanbieter-Einstufungen von Bedrohungsquellen (Datei-Hashfunktionen) nutzen
- Verringert Fehlalarme
- Erfüllt behördliche Auflagen, Sicherheits- und Datenschutznormen

Das Kaspersky Private Security Network wendet unsere einzigartigen Bedrohungsinformationen nicht nur auf Sicherheitslösungen von Kaspersky Lab, sondern auch auf andere Lösungen im Unternehmen an, wie z. B. für SIEM, Risikomanagement und Compliance. All diese Funktionen lassen sich über das SDK, über Direktaufrufe und über die API des Kaspersky Private Security Network integrieren und liefern so wichtige Erkenntnisse zur Sicherheit und Bedrohungsbereitschaft Ihres Unternehmens.



Endpoint Security

Die zuverlässige mehrschichtige Endpoint-Protection-Plattform, basierend auf True Cybersecurity

Die Bedrohungslage hat sich exponentiell verschlechtert: Wichtige Geschäftsprozesse, vertrauliche Daten und finanzielle Ressourcen sind einem ständig steigenden Risiko durch Zero-Day-Attacken ausgesetzt. Um das Risiko für Ihr Unternehmen zu verringern, müssen Sie smarter, besser gewappnet und besser informiert sein als die Cyberkriminellen, die es auf Ihr Unternehmen abgesehen haben. Fakt ist: Die Mehrheit der Cyberangriffe auf Unternehmen werden über Endpoints initiiert. Wenn Sie jeden Endpoint im Unternehmen, ob stationär oder mobil, wirksam sichern können, ist dies eine starke Grundlage für Ihre gesamte Sicherheitsstrategie.

Die fortschreitende Digitalisierung führt zu immer komplexeren IT-Umgebungen in Unternehmen. Parallel dazu wenden Cyberkriminelle immer raffiniertere Angriffsmethoden an und schaffen so neue Wege, in die Infrastruktur eines Unternehmens einzudringen.

Die Mehrheit der Angriffe auf Großunternehmen wird über Endpoints eingeleitet. Ohne effektive und globale Bedrohungsinformationen, die sogenannte Threat Intelligence, sowie lernfähige maschinelle Systeme (Machine Learning) bieten herkömmliche Sicherheitstechnologien einfach keinen ausreichenden Schutz vor diesen hoch entwickelten Bedrohungen.

Mit unseren hoch entwickelten Erkennungstechnologien bieten wir Echtzeitschutz vor unbekannten und komplexen Bedrohungen (ATPs) sowie gezielten Angriffen. Dabei nutzen wir eine Kombination aus Machine Learning und Threat Intelligence.

Ergänzt wird dieser Schutz durch leistungsstarke Kontroll- und Datenschutzmechanismen, darunter integrierte Verschlüsselung, automatisiertes Patching und Schutz von mobilen Endpoints, die alle gemeinsam über das Kaspersky Security Center verwaltet werden.

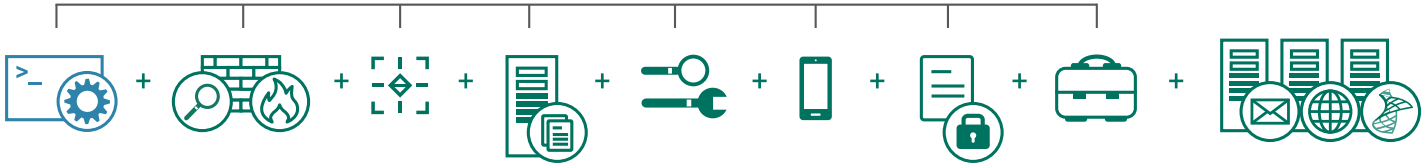
Sämtliche Komponenten werden bei uns im Haus entwickelt und bilden so eine gemeinsame Plattform, die sich problemlos an unterschiedliche Anforderungen im Unternehmen anpasst.

Die Lösung: Kaspersky Endpoint Security

Jeder Endpoint muss vollständig vor allen Arten hoch entwickelter Cyberbedrohungen geschützt werden. Herkömmliche Virenschutzprogramme können das nicht leisten. Nur mit einem mehrstufigen Ansatz und einer modernen Sicherheitsplattform, die Machine Learning zur dynamischen und statischen Erkennung bietet, haben Sie eine Chance, jeden einzelnen Endpoint innerhalb Ihres Netzwerks und darüber hinaus vollständig zu schützen.

Auf der Basis von stets aktuellen Bedrohungsinformationen in Echtzeit entwickeln wir unsere Technologien kontinuierlich weiter. So schützen wir auch Ihr Unternehmen zuverlässig vor den Bedrohungen von heute und morgen. Auch vor Zero-Day-Exploits. Mit Kaspersky Lab setzen Sie auf einen der weltweit führenden Anbieter und auf innovative Lösungen, die Ihr Unternehmen zuverlässig schützen.

Kaspersky Endpoint Security



Zuverlässiger Schutz für alle Endpoints
Unsere erweiterten Schutztechnologien schützen Unternehmen und ihre IT-Infrastrukturen ungeachtet ihrer Komplexität, einschließlich aller Endpoints – von physischen und virtuellen Desktops bis hin zu Servern und mobilen Geräten.

Verhaltensanalyse mit lernfähigen Systemen zum Schutz Ihres Unternehmens
Unsere Lösung wendet Machine Learning basierend auf statischen und dynamischen Datentechnologien an. So schützen wir Sie selbst vor bisher unbekannten Bedrohungen.

Leistungsstarke globale Threat Intelligence
All unsere Technologien beruhen auf unseren bewährten globalen Bedrohungsinformationen. Wir können mehr APT-Erkennungen als die meisten anderen Sicherheitsanbieter vorweisen und zeigen damit unser umfassendes Verständnis moderner Sicherheitsbedrohungen. So können wir Sie dabei unterstützen, sich besser vor diesen Bedrohungen zu schützen.

Automatische Reaktion in Echtzeit
Wenn eine Bedrohung erkannt wird, ermittelt unsere dynamische Engine zur Verhaltensüberwachung automatisch alle Änderungen, die die Malware möglicherweise bereits vorgenommen hat, und macht sie rückgängig.

Fortlaufender dynamischer Schutz vor Zero-Day-Bedrohungen und -Exploits
Automatic Exploit Prevention wurde entwickelt, um Cyberkriminelle an der Ausnutzung von Programmschwachstellen auf geschützten Geräten zu hindern. Das automatisierte Patch Management sorgt für eine zusätzliche Sicherheitsebene.

FIPS 140-2-zertifizierter Datenschutz
Die leistungsstarke, benutzertransparente Verschlüsselung schützt vertrauliche Daten während der Übertragung, auf tragbaren Geräten und im Ruhezustand.

Zuverlässiger Schutz vor Ransomware
Mit unseren Anti-Ransomware-Technologien sichern Sie Ihre Daten, drehen Cyberkriminellen den Geldhahn ab und schützen Ihre freigegebenen Ordner vor erweiterten Kryptolockern.

Geringere Betriebskosten und ein höherer ROI durch zentrale Verwaltung
Verwalten Sie mehrere Plattformen und alle Endpoint-Geräte über eine Konsole. So erhalten Sie mehr Transparenz und Kontrolle ohne zusätzliche Software, Geräte oder Mitarbeiter.

Embedded Systems Security

Zuverlässige Sicherheit speziell für Embedded Systems

Embedded Systems verarbeiten echtes Geld und Kreditkarteninformationen und sind damit ein beliebtes Ziel von Cyberkriminellen. Daher erfordern sie optimalen zielgerichteten und intelligenten Schutz. Bewährte Technologien wie Gerätekontrolle und Default Deny bilde dabei die erste Verteidigungslinie.

Heute finden sich sogenannte Embedded Systems bereits in sehr vielen Bereichen: Geldautomaten, Fahrkarten- und andere Verkaufsautomaten, POS-Systeme im Handel, in Maschinen und Geräten der Industrie und Medizin und auch in Bereichen von Transport und Logistik.

Embedded Systems stellen ein Sicherheitsproblem dar. Im Einsatz an meist geografisch verteilten Standorten sind sie meist schwer zu administrieren. Wenn dann noch eine unzureichende oder schlecht verfügbare Netzanbindung vorhanden ist, werden Aktualisierungen aufwändig und schwer. Systeme, die Bargeld und Kundendaten verarbeiten, müssen jedoch fehlertolerant und zuverlässig funktionieren. Embedded Lösungen müssen nicht nur selbst vor Bedrohungen geschützt sein, sondern dürfen auch für Cyberkriminelle nicht als Eintrittspunkt in das Unternehmensnetzwerk zugänglich sein.

Bestehende Sicherheitsvorschriften für eingebettete Geräte neigen dazu, nur virenschutzbasierte Sicherheit oder eine Systemhärtung abzudecken, was inzwischen nicht mehr ausreicht. Ein rein auf Virenschutz basierender Ansatz ist im Fall der aktuellen Bedrohungen von Embedded Systems nur von eingeschränkter Wirkung, was bei den neuesten Angriffen deutlich wurde.

Bewährte Technologien wie Gerätekontrolle und Default Deny (ggf. mit einem zusätzlichen Virenschutzmodul) bilden einen zuverlässigen Schutz für die oftmals veralteten, aber kritischen Systeme.

Die Lösung: Kaspersky Embedded Systems Security

Kaspersky Lab hat eine Sicherheitslösung entwickelt, die sich speziell an Unternehmen richtet, die Embedded Systems betreiben. Diese Lösung berücksichtigt die einzigartigen Funktionen, Betriebssysteme, Kanäle und Hardware-Anforderungen der verschiedenen Systeme sowie ihre aktuelle Bedrohungslage und unterstützt auch weiterhin Windows XP.

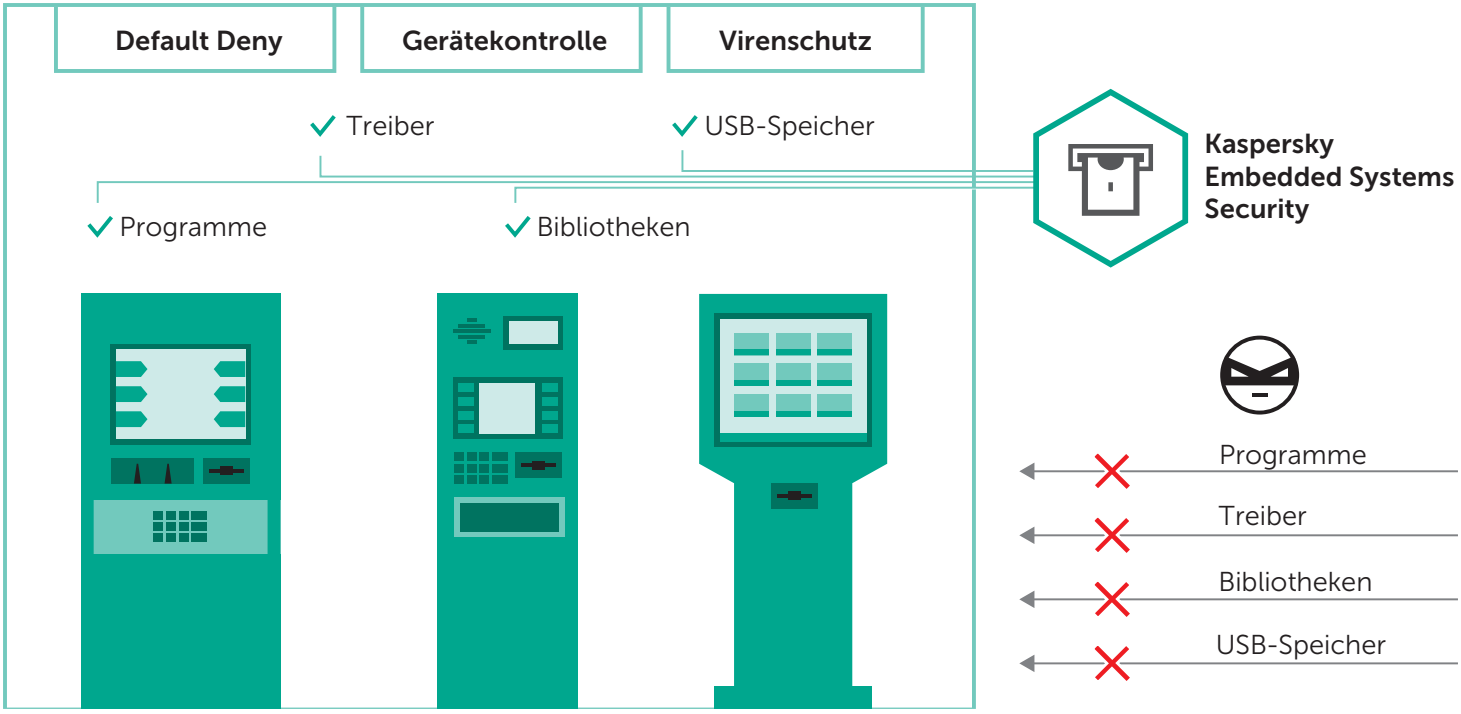
Kaspersky Embedded Systems Security bietet einen „Nur Default Deny"-Betriebsmodus, für den lediglich 256 MB RAM und nur 50 MB Speicherplatz auf der Festplatte notwendig sind – ideal für Systeme, die auf Windows XP basieren und mit Low-End-Hardware betrieben werden.

Ein optionales Antiviren-Modul bietet zudem einen Modus, in dem bei Bedarf manuelle Scans ausgeführt werden können, einschließlich Firewall-Verwaltung. 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

Die Lösung ist speziell auf den Schutz von Systemen ausgelegt, die auf Embedded-Betriebssystemen basieren. So schützen sie alle spezifischen Angriffsflächen dieser Architekturen, ohne dabei die Hardware und Effizienz außer Acht zu lassen. Eine einzige intuitive Konsole bietet Ihnen die Kontrolle und Transparenz, die Sie benötigen, um eine effiziente, mehrstufige Sicherheitslösung für Ihre Endpoints, Systeme und IT-Infrastruktur zu verwalten.



Cybersecurity Services

Beinhaltet Threat Intelligence, Sicherheitsschulungen, Vorfallsreaktion und Assessments von einem der führenden Anbieter

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

Bedrohungen werden immer komplexer, und auch Cyberkriminelle entwickeln ständig neue Angriffsmethoden zur Überwindung von Sicherheitstechnologien. Herkömmliche Sicherheitslösungen, wie z. B. Virenschutz, Firewalls und Systeme zur Angriffsüberwachung, für einen umfassenden Schutz nicht mehr aus. Heute muss ein neuartiger Sicherheitsansatz, der auf Bedrohungsinformationen und umfassendem Fachwissen basiert, diese Sicherheitslücke schließen.

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 Ihr Security Operations Center (SOC) und Ihr IT-Sicherheitsteam in der Lage ist, das Unternehmen vor den neuesten Online-Bedrohungen zu schützen.

Schulungen zur Cybersicherheit

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.

Ihre internen Sicherheitsexperten müssen sich mit den fortschrittlichen Sicherheitstechniken auskennen, die eine wichtige Komponente für ein effektives Bedrohungsmanagement und Strategien zur Risikominimierung im Unternehmen bilden. Darüber hinaus sollten alle Mitarbeiter über ein allgemeines Verständnis der bestehenden Gefahren verfügen 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 – von den Grundlagen bis hin zu Expertenwissen.

- Mit der **Sensibilisierung für Cybersicherheit** können Unternehmen das Sicherheitsbewusstsein ihrer Mitarbeiter verbessern – und gleichzeitig etwas für ihre eigene Sicherheit tun.

- **Security Education für IT-Sicherheitsprofis** (alle Niveaus) verbessern die Kenntnisse und Fertigkeiten Ihrer internen Sicherheitsexperten, 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 forensischen Fertigkeiten mithilfe aktueller Bedrohungsinformationen.
- **APT Intelligence Reporting** ermöglicht den exklusiven und frühzeitigen Zugang zu Informationen über hochkarätige Cyberspionage-Aktionen, darunter auch Gefährdungsindikatoren (Indicators of Compromise, IOCs).
- **Kundenspezifisches Threat Intelligence Reporting** identifiziert die extern verfügbaren, entscheidenden Komponenten Ihres Netzwerks.

Expert Services

Reicht Ihre interne Fachkompetenz aus, um einen Sicherheitsvorfall zu beheben? Sind Ihre IT-Infrastruktur bzw. die entsprechenden Programme umfassend vor möglichen Cyberattacken geschützt? Unsere Expertenservices sind darauf ausgelegt, diesen Risiken zu begegnen.

- **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 Programmtypen 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.

Cybersecurity Awareness

Interaktive Schulungsprogramme, die den Aufbau einer sicheren Cyberumgebung im Unternehmen ermöglichen

Mehr als 80 % aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler. Im Schnitt bezahlten große Unternehmen 861 000 US-Dollar für die Wiederherstellung nach einer Sicherheitsverletzung, kleinere Unternehmen rund 86 500 US-Dollar. Alleine Phishing-Angriffe kosten bis zu 400 US-Dollar pro Mitarbeiter im Jahr.

Unternehmen verlieren Millionen durch die Wiederherstellung nach Vorfällen, an denen Mitarbeiter beteiligt waren. Herkömmliche Schulungsprogramme zur Vermeidung dieser Probleme sind jedoch oft nicht sonderlich effektiv. Oftmals gelingt es ihnen nicht, Mitarbeitern die gewünschten Verhaltensweisen und die erforderliche Motivation zu vermitteln.

Kaspersky Lab bietet eine Reihe computergestützter Schulungsprodukte an, die moderne Lerntechniken anwenden und sich an alle Ebenen innerhalb der Unternehmensstruktur richten. Unser Schulungsprogramm hat seine Effektivität bereits unter Beweis gestellt – sowohl für unsere Kunden, als auch für Partner von Kaspersky Lab:

- Bis zu 90 % weniger Vorfälle
- 50 bis 60 % geringerer finanzieller Verlust durch Cyberrisiken
- Bis zu 93 % Wahrscheinlichkeit, dass das vermittelte Wissen im Alltag angewendet wird
- 86 % der Teilnehmer würden ihren Kollegen die Trainings empfehlen

Kaspersky-Schulungsprodukte für Sicherheitsbewusstsein

Gewinnbringender Ansatz

- **Aufbau von Verhaltensweisen statt reiner Inhaltsvermittlung**: Dieser Lernansatz beruht auf Planspielen, praktischem Lernen, Gruppendynamik, simulierten Angriffen, Lernpfaden usw. So fördern Sie feste Verhaltensweisen und erreichen langfristige Verbesserungen in der Cybersicherheit.

- Ernsthafte, praktische Inhalte (basierend auf den Erkenntnissen der Forschung und Entwicklung von Kaspersky Lab) werden in Form von interaktiven Übungen vermittelt, die speziell auf Ihre Anforderungen und den bevorzugten Zeitrahmen und das bevorzugte Format der unterschiedlichen betrieblichen Ebenen ausgerichtet sind: leitende Manager, Bereichsleiter, allgemeine Mitarbeiter.

- **Messung in Echtzeit, problemloses Programmmanagement**: Die speziell entwickelte Schulungssoftware umfasst automatisierte Schulungsaufgaben, Fähigkeitentests und Methoden zur Festigung des Wissens über wiederholte simulierte Phishing-Angriffe. Zudem erfolgt die Anmeldung bei den einzelnen Schulungsmodulen automatisch. Die Kurse können von Kaspersky-Partnern oder von internen Schulungsteams des Kunden verwaltet und geleitet werden. Bei internen Kursen stehen Ihnen Schulungsprogramme für Schulungsleiter sowie Support von Kaspersky Lab zur Verfügung.

Funktionsweise

- Die Schulung deckt ein breites Spektrum an Sicherheitsthemen ab: von Datenlecks und Ransomware über internetbasierte Malware-Angriffe bis hin zu sicheren sozialen Netzwerken und mobiler Sicherheit.

- Die Lernmethode unterstützt eine dauerhafte Festigung der Fähigkeiten und schafft Motivation auf allen Ebenen des Unternehmens.

- Schulungskurse, die sich an unterschiedliche Unternehmensebenen und -funktionen richten, schaffen eine gemeinsame Sicherheitskultur, die alle Mitarbeiter einbezieht und von oberster Stelle aus gefördert wird.

- In der Schulung kommen Analyse- und Reporting-Funktionen zum Einsatz, die die Fähigkeiten und den Lernfortschritt der Mitarbeiter sowie die Effektivität des Programms im gesamten Unternehmen messen.

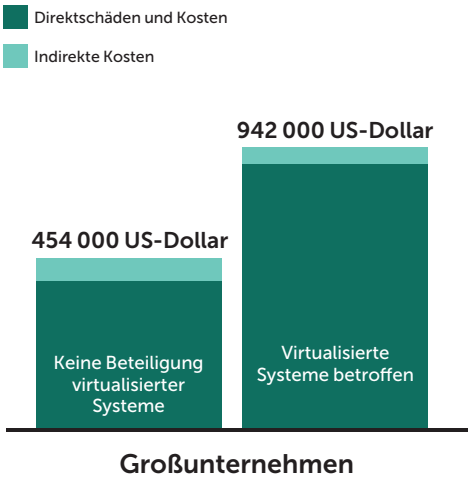
- Bildungspläne und Best Practices von Kaspersky Lab erleichtern die Implementierung des Programms und helfen den IT-Sicherheits- und Schulungsteams des Kunden dabei, den maximalen Wert aus ihren Initiativen zur Förderung des Sicherheitsbewusstseins zu holen.

Cloud Security

Perfekt für Ihre Hybrid-Cloud

Beim Schutz virtualisierter Systeme suchen Unternehmen nach der richtigen Balance zwischen Schutz und Performance und den fortschrittlichsten Sicherheitsfunktionen, um entscheidende Geschäftsprozesse optimal zu schützen.

Datenlecks mit Beteiligung von virtualisierten Systemen sind durchschnittlich mehr als doppelt so kostspielig wie die physischer Systeme.



Quellen: Bericht von Kaspersky Lab zu globalen IT-Risiken 2015

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 Kriminellen noch mehr Möglichkeiten bieten, Großunternehmen anzugreifen.

Die zur Absicherung Ihrer virtualisierten Infrastruktur eingesetzte Lösung sollte 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

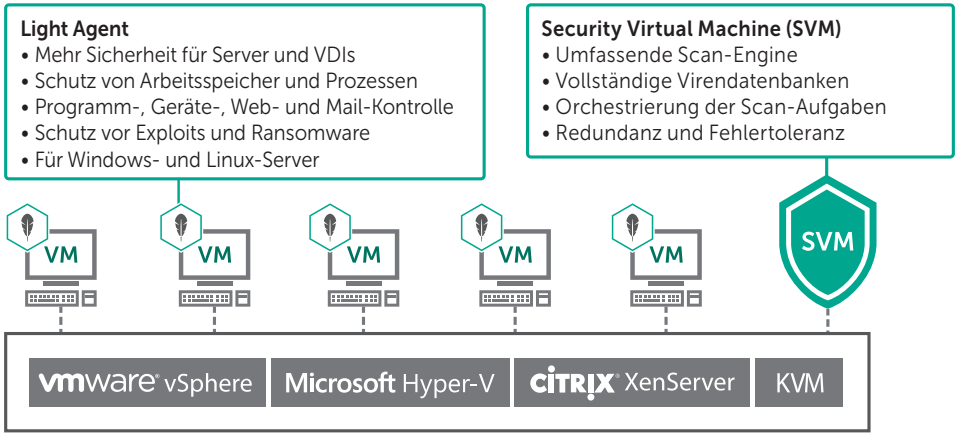
Kaspersky Lab bietet zwei Lösungen mit denen Sie die perfekte Balance zwischen optimaler Sicherheit und uneingeschränkter Leistung erreichen.

Während unsere agentenlose Lösung in Kombination mit den grundlegenden Hypervisor-Technologien (wie z. B. VMware NSX) 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 Ihrer VMs – 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 mit NSX, 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.

Data Center Security

Ergänzung für Ihr Rechenzentrum zur Erkennung und Reaktion auf die fortschrittlichsten Cyberbedrohungen

Softwarezentrierte Rechenzentren brauchen ebenso viel Schutz wie herkömmliche. Wenn Sie dies nicht garantieren können, werden Ihre virtualisierten Systeme und Datenspeicher zum schwächsten Glied in Ihrer Verteidigung.

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 sich jeder Herausforderung stellen können und effektiv skalierbar sein, d. h. sich vollständig in die vorhandene IT-Umgebung integrieren lassen. Ansonsten beeinträchtigt sie die Performance des Rechenzentrums und verschlechtert mit der Zeit die betriebliche Effizienz.

Die Lösung: Kaspersky Security for Data Centers

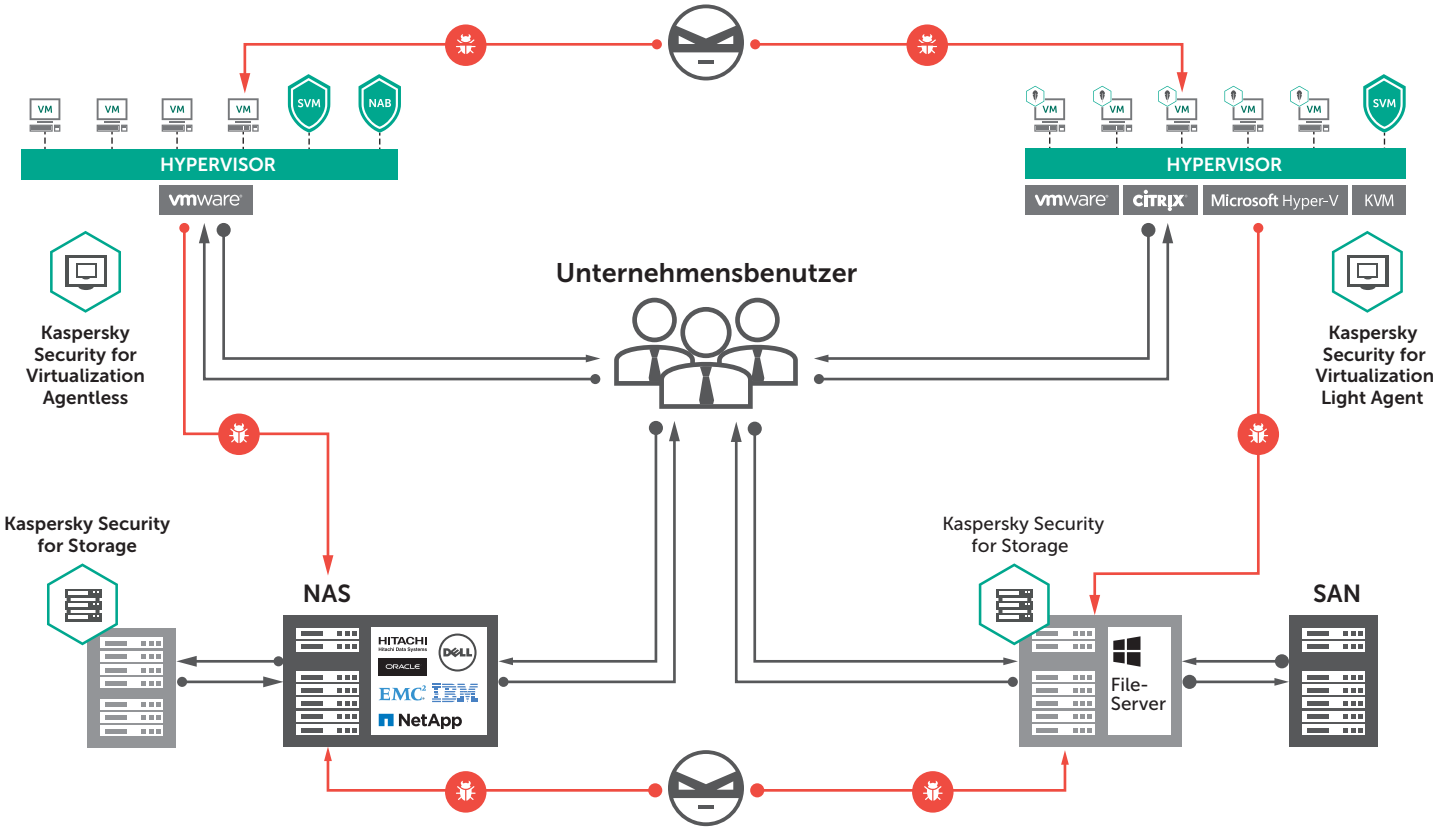
Wir bieten Lösungen, die sich auf den Schutz der beiden zentralen Bereiche Ihres Rechenzentrums konzentrieren: Ihre virtualisierte Infrastruktur und Ihre Speichersysteme. Unsere Lösungen sind speziell auf Systeme mit mehreren Hypervisoren und Speichersystemen zugeschnitten und bieten folgende Vorteile:

- Speziell auf die gängigsten Virtualisierungsplattformen zugeschnitten, darunter VMware mit NSX, 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


VM
SVM
NAB
HYPERVISOR
vmware
HYPERVISOR
vmware
citrix
Microsoft Hyper-V
KVM
Kaspersky Security for Virtualization Agentless
Unternehmensbenutzer
Kaspersky Security for Virtualization Light Agent
Kaspersky Security for Storage
NAS
HITACHI
DELL
ORACLE
EMC²
IBM
NetApp
Kaspersky Security for Storage
SAN
File-Server

Mobile Security

Integrierte Tools für Sicherheit und Management unterstützen Ihre Mobilstrategie.

Innerhalb eines typischen dreimonatigen Zeitraums im Jahr 2016 erkannten wir über 3,5 Millionen schädliche Installationspakete, über 83.000 Ransomware-Trojaner und über 27.000 Banking-Trojaner, die es alle auf die Mobilgeräte unserer Kunden abgesehen hatten.

Schädliche Software und Webseiten sowie Phishing-Angriffe auf mobile Geräte nehmen weiter zu, während sich die Funktionalität von mobilen Geräten ungebrochen weiterentwickelt. Da sie sowohl zu Hause als auch beruflich als wichtiges Produktivitätstool eingesetzt werden, stellen sie ein verlockendes Ziel für Cyberkriminelle dar. Die zunehmende Nutzung von privaten Geräten zu beruflichen oder geschäftlichen Zwecken (BYOD) hat zu einer größeren Anzahl unterschiedlicher Geräte innerhalb des Unternehmensnetzwerks und so auch zu zusätzlichen Herausforderungen für IT-Administratoren geführt, die mit der Verwaltung und Kontrolle der IT-Infrastrukturen alle Hände voll zu tun haben.

Persönliche Geräte von Mitarbeitern – ein Risiko für das ganze Unternehmen

Mitarbeiter, die ihre eigenen mobilen Endgeräte sowohl privat als auch beruflich 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 WLAN-Netzwerke ohne ausreichende Sicherung, Phishing-Angriffe und infizierte Textnachrichten. Besucht ein Benutzer aus Versehen eine schädliche Webseite bzw. eine legitime Webseite, die mit Schadcode infiziert wurde, gefährdet er damit die Sicherheit seines Geräts und der darauf gespeicherten Daten. Das Anschließen eines Smartphones an einen Computer, z. B. um den Akku nachzuladen, kann schon zu einer Infizierung des Smartphones mit Malware führen. (Diese Bedrohungen betreffen alle gängigen Mobilplattformen: Android, iOS und Windows Phone).

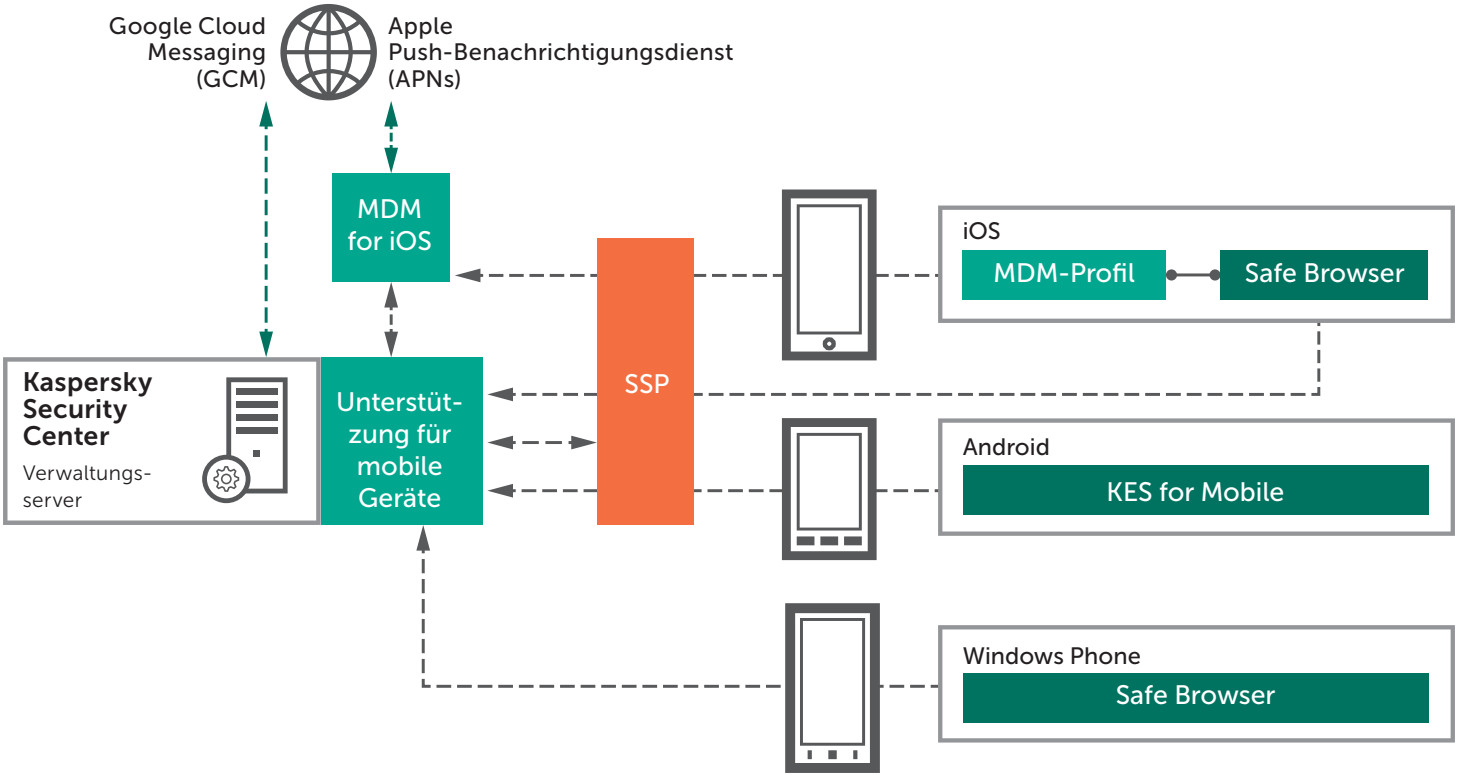
Die Lösung: Kaspersky Security for Mobile

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 der Integration in alle führenden Plattformen können mobile Geräte per OTA-Schnittstelle (Over the Air) gescannt und kontrolliert werden. So werden Schutz und Verwaltung von Android-, iOS- und Windows Phone-Geräten erheblich verbessert.
- **Mobile Application Management:** Isolierte Container für Programme und die Option, den Gerätespeicher selektiv zu löschen, ermöglichen es, geschäftliche und persönliche Daten einzuzäunen 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



DDoS Protection

Vollständiger Schutz vor allen Arten von DDoS-Angriffen auf Ihre Infrastruktur

Ein einziger DDoS-Angriff kann je nach Größe des Unternehmens einen Schaden zwischen 106.000 und 1.600.000 US-Dollar anrichten. Und was kostet es, einen DDoS-Angriff vorzubereiten? Nur ca. 20 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. Die Flexibilität dieser Angriffsmethode macht eine gründlichere Verteidigung erforderlich.

Im Gegensatz zu Malware-Attacken, 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 umfassenden, integrierten Schutz vor DDoS-Angriffen und schafft so eine DDoS-Abwehr, die alle Maßnahmen für den Schutz Ihres Unternehmens vor DDoS-Angriffen abdeckt. Ihnen stehen drei Deployment-Optionen zur Auswahl: Connect, Connect+ und Control.
Sobald ein mögliches Angriffsszenario erkannt wurde, wird das Security Operations Center (SOC) von Kaspersky Lab alarmiert. Bei den Deployment-Szenarien Kaspersky DDoS Protection Connect und Connect+ wird die Abwehr automatisch eingeleitet, während unsere Techniker sofort detaillierte Prüfungen durchführen, um diese Abwehr je nach Größe, Typ und Raffinesse des DDoS-Angriffs zu optimieren. Bei Kaspersky DDoS Protection Control entscheiden Sie selbst, wann die Abwehr im Einklang mit Ihrer Sicherheitsrichtlinie, Ihren Geschäftszielen und Ihrer Infrastrukturumgebung eingeleitet werden soll.

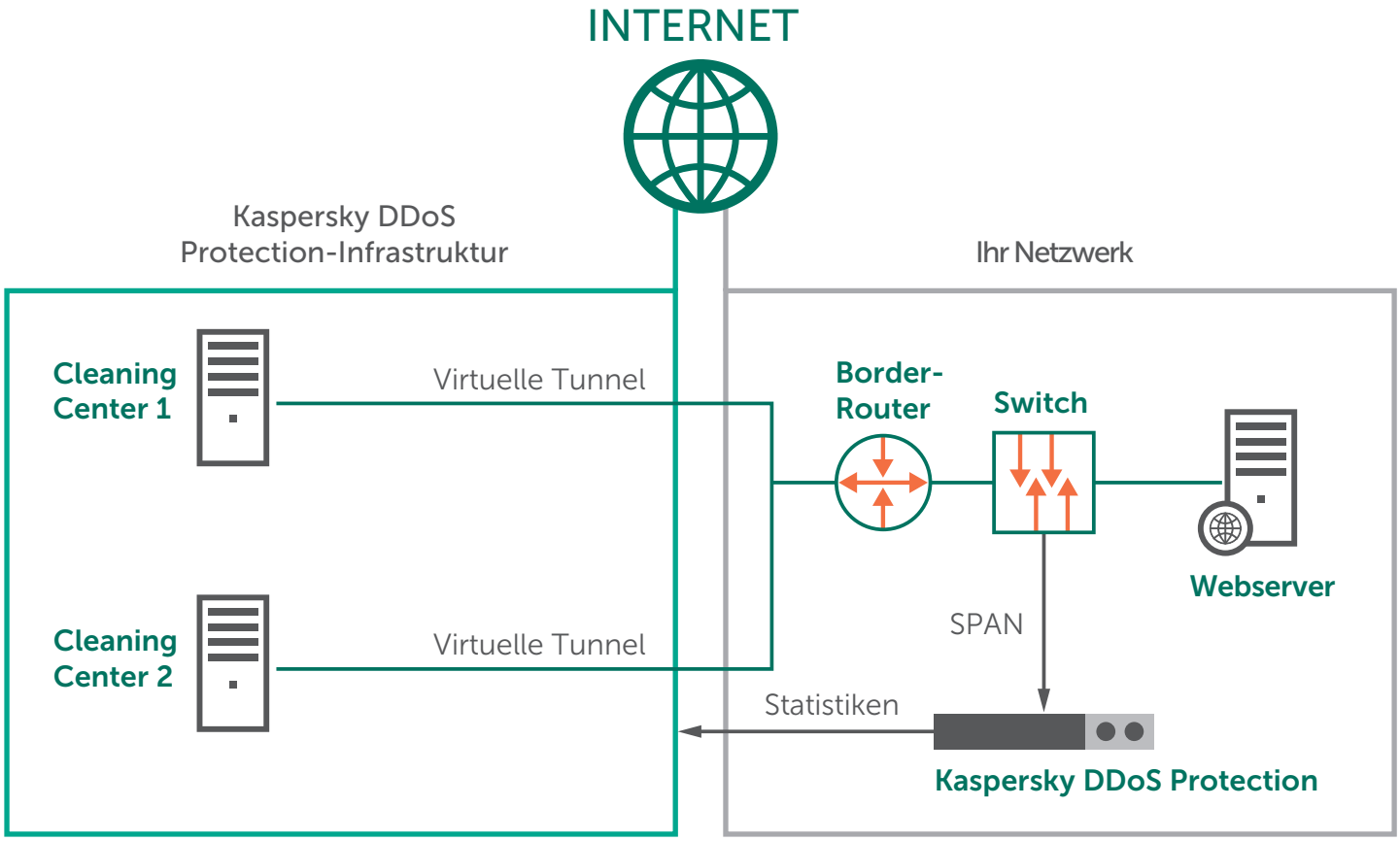
Dank der flexiblen Ausrichtung auf unterschiedliche Konfigurationen stellen wir sicher, dass wir die Anforderungen Ihres Unternehmens und Ihrer Online-Ressourcen vollständig erfüllen.

Aufbau von Kaspersky DDoS Protection

Diese umfassende Verteidigungslösung bietet Ihnen Folgendes:

- Umfassender Schutz für geschäftskritische Online-Ressourcen und Netzwerkinfrastrukturen
- Flexible Bereitstellungsoptionen: Kaspersky DDoS Protection Connect, Connect+ und Control
- Hochgradig skalierbare Cleaning Center in ganz Europa
- Globale DDoS-Informationen in Echtzeit basierend auf Big-Data-Sicherheitsanalysen
- Schneller Schutz und Support rund um die Uhr über Emergency Response Teams

Kaspersky DDoS Protection Control



Industrial Cybersecurity

Spezieller Schutz für industrielle Steuerungssysteme

Früher reichten „Luftschleusen" (Air Gaps) zwischen Industrieanlagen und der Außenwelt aus, um ausreichenden Schutz zu bieten, aber dies ist nicht länger der Fall. In Untersuchungen konnte 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.

Der Bereich der industriellen Sicherheit hat eine Tragweite, die weit über den Schutz von Unternehmen und geschäftlicher Reputation hinausgeht. In vielen Fällen spielen beim Schutz von industriellen Systemen vor Cyberbedrohungen ökologische, soziale und makroökonomische Faktoren eine erhebliche Rolle. Alle 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 Erkennung und Vermeidung von Aktionen (beabsichtigt oder unbeabsichtigt) gewährleistet, die zu Unterbrechungen oder dem Stillstand wichtiger Prozesse führen würden.

Die Lösung: Kaspersky Industrial CyberSecurity

Kaspersky Industrial CyberSecurity ist ein Portfolio aus Technologien und Services, das umfassenden Schutz für jede einzelne Ebene von Industriesystemen bietet, darunter auch für SCADA-Server, HMI-Panele, Engineering-Workstations, SPS, Netzwerkverbindungen und Mitarbeiter, ohne dabei die Geschäftskontinuität und Konsistenz der technologischen Prozesse zu beeinträchtigen. Dank der flexiblen und vielseitigen Einstellungen lässt sich die Lösung so konfigurieren, dass die speziellen Anforderungen einzelner industrieller Einrichtungen erfüllt werden.

Die Lösung wurde zum Schutz wichtiger Infrastrukturen entwickelt und basiert auf verschiedenen industriellen Steuersystemen (ICS). Die Vielseitigkeit und der Umfang von Kaspersky Industrial CyberSecurity ermöglichen es Unternehmen, die Lösung exakt auf die Anforderungen der jeweiligen Umgebung ihres ICS zuzuschneiden. Die optimale Konfiguration von Sicherheitstechnologien und -services wird im Rahmen einer vollständigen Infrastrukturprüfung durch die Kaspersky-Experten ermittelt.

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 im Bereich Systemschwachstellen sowie unserer engen Zusammenarbeit mit den führenden Vollzugs- und Regierungsbehörden sowie Industrieorganisationen – darunter Interpol, das Industrial Internet Consortium, verschiedene ICS-Anbieter und Behörden – konnten wir bei der Erfüllung der speziellen Anforderungen industrieller Cybersicherheit eine Führungsrolle übernehmen.

Diese Speziallösung bietet Ihnen Folgendes:

- Umfassender Cybersicherheitsansatz 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

KASPERSKY INDUSTRIAL CYBERSECURITY

TECHNOLOGIEN

ERKENNUNG ANORMALEN VERHALTENS

INTEGRATION IN ANDERE SYSTEME

MALWARE-SCHUTZ

INTEGRITÄTSKONTROLLE

ZENTRALISIERTE VERWALTUNG

VORFALLSUNTERSUCHUNG

INTRUSION PREVENTION SYSTEM

SERVICES

SCHULUNG UND SECURITY INTELLIGENCE

- Cybersecurity Trainings
- Awareness-Programme
- Simulationen

EXPERTENSERVICES

- Cybersecurity Assessments
- Lösungsintegration
- Maintenance
- Incident Response

Fraud Prevention

Frühzeitige Erkennung plattformübergreifender Betrugsversuche in Echtzeit

Finanzdienstleister, die Wachstum erreichen und Kunden gewinnen möchten, kommen heute nicht mehr um digitales Banking herum. Digitales Banking ist jedoch nicht nur für Kunden, sondern auch für Betrüger sehr attraktiv.

Cyberkriminelle werden immer geschickter bei der Entwicklung ausgeklügelter 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 gehört einer neuen Generation von Systemen an, die eine Echtzeitanalyse des Verhaltens, der Geräte und der Benutzerumgebung gestattet. Über lernfähige Systeme erkennt die Lösung erweiterte Betrugsszenarien und Geldwäschesysteme. Sie bietet der Betrugsabteilung einer Bank darüber hinaus die Möglichkeit, exakte Informationen zu jedem einzelnen Vorfall zu erfassen, einschließlich der Methoden, mit denen der Zugriff erlangt wurde.

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 zugrunde liegenden Ursachen von Malware und Online-Attacken.

- **Kaspersky Fraud Prevention Cloud** ist ein Produkt zur Erkennung von Betrug beim Online- und mobilen Banking. Zu seinen Hauptfunktionen zählen risikobasierte Authentifizierung, Verhaltensanalyse, fortlaufende Erkennung von Sitzungsanomalien und passive Biometrik basierend auf lernfähigen Systemen und statistischen Modellen.

Diese umfassende Betrugsschutzlösung bietet Ihnen Folgendes:

- Multi-Channel-Sicherheit für Online-Banking und -Zahlungen
- Vorausschauende Erkennung erweiterter Betrugsversuche in Echtzeit, bevor die Transaktion verarbeitet wird
- 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
- Geringere Kosten durch Automatisierung und maschinelle Lernfunktionen

Premium-Support und Professional Services

Eine Palette von Services, mit denen Unternehmen alle Vorteile von Kaspersky-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 Ihnen Kaspersky Lab 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

Unsere Maintenance Service Agreements (MSA) werden 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 reaktionsschnellen 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.

Implementation Service: 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 Ihnen einen vollständigen Bericht einschließlich praktischer Empfehlungen dazu, wie Sie die Sicherheit bzw. die Effizienz des Systems Management erhöhen können.

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 Malware-Vorfälle
- Überwachung und Reporting
- Ein einziger Ansprechpartner

Über Kaspersky Lab

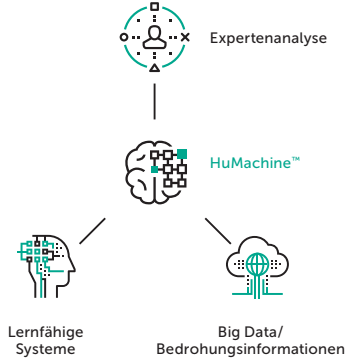
Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 1997 gegründet wurde. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen 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.

Durch unsere Unabhängigkeit sind wir flexibel und können schnell reagieren. Innovationen sind die Antriebskraft hinter unserem Anspruch, stets effektiven, praktisch umsetzbaren und leicht zugänglichen Schutz zu bieten. Dank unserer weltweit führenden Sicherheitstechnologien sind wir und unsere 400 Mio. Benutzer und 270 000 Firmenkunden potentiellen Bedrohungen immer einen Schritt voraus.

Unser Engagement nicht nur für hoch entwickelte Technologien, sondern auch für den Menschen verschafft uns einen Wettbewerbsvorteil. Als einer der vier international führenden Hersteller von Endpoint-Sicherheitslösungen baut Kaspersky Lab seine Marktposition stetig aus. So haben etwa die drei namhaften Analyse-Agenturen Gartner, IDC und Forrester unser Unternehmen als „Leader" beim Endpoint-Schutz benannt.

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

Für Ihre Notizen



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **www.viruslist.de**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de