KASPERSKY lab

Kaspersky Security Solutions for Enterprise

#TrueCybersecurity

Kaspersky
Security Solutions for Enterprise

Unternehmenssicherheit im Zeitalter der digitalen Transformation

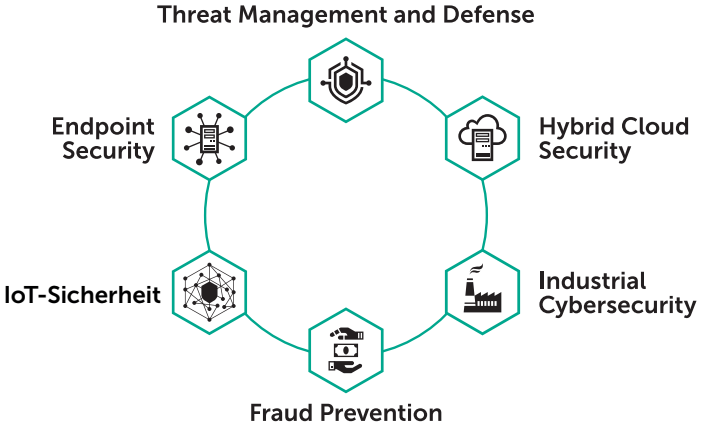
Die Anzahl der Cyberangriffe nimmt auch weiterhin zu, wobei zunehmend professionelle und gezielte Angriffe auf Unternehmensinfrastrukturen zu beobachten sind. Die Frage lautet nicht mehr, ob Sie angegriffen werden, sondern wann, wie schnell und wie vollständig Ihnen die Wiederherstellung gelingt.

Die IT-Infrastruktur von Unternehmen ist in den letzten Jahren immer komplexer geworden und erstreckt sich über das interne Unternehmensnetzwerk hinaus hinaus auch auf Mobilgeräte, öffentliche Clouds und Drittanbieter. Die digitale Transformation bringt zwar massive Vorteile in Bezug auf Effizienz und Flexibilität mit sich, gleichzeitig aber auch neue Sicherheitsherausforderungen. Die Sicherstellung der Geschäftskontinuität, der Schutz der finanziellen Leistungsfähigkeit sowie der Schutz von Unternehmens- und Kundendaten stellen erhebliche Anforderungen an Ihr IT-Sicherheitsteam und Ihr Budget.

Das neue Unternehmensportfolio von Kaspersky Lab spiegelt die Anforderungen heutiger Unternehmen wider: Die Erstellung einer vollständigen Cybersicherheitsplattform mit voll skalierbaren Schutzmöglichkeiten für physische, virtuelle und Cloud-basierte Systeme, einschließlich statischer und mobiler Endpoints, Server, Netzwerke und spezieller Hardware und Software.

Durch eine einzigartige Kombination aus führenden Technologien und Serviceleistungen kann Ihr Sicherheitsteam die meisten Angriffe verhindern, neue Angriffe erkennen, zukünftige Bedrohungen vorhersagen und auf unvorhergesehene Ereignisse reagieren, damit die Geschäftskontinuität gewahrt bleibt und gesetzliche Vorschriften eingehalten werden.

Unser Portfolio besteht aus folgenden Lösungen, die alle durch ein breites Spektrum von kompetenten Dienstleistungen, Sicherheitsschulungen und professionellem Support ergänzt werden:



Durch die Verzahnung dieser Lösungen und ihrer technologischen Komponenten entsteht ein anpassungsfähiges Security Framework. Es ermöglicht das Vorhersagen, Verhindern, Erkennen und Beseitigen selbst modernster Cyberbedrohungen und zielgerichteter Angriffe, kommt dadurch der Geschäftskontinuität und Belastbarkeit zugute und hat nur minimale Auswirkungen auf die Performance.

Die Kombination aus maschinellem Lernen, menschlicher Expertise und globaler Threat Intelligence bietet zuverlässigen Schutz für Ihr Unternehmen. Und Sie profitieren von einer einfachen und einheitlichen Verwaltung und umfassendem Support für Ihre digitale Transformation.

Im Einsatz für Ihre digitale Freiheit

Ihre Daten und Ihre Privatsphäre sind unter Beschuss durch Cyberkriminelle und Wirtschaftskriminelle deshalb brauchen Sie einen Partner, der Ihnen im Kampf um die Unternehmensressourcen zur Seite steht. Seit 20 Jahren hat Kaspersky Lab vielfältige Cyberbedrohungen aufgedeckt und abgewehrt, ganz gleich, ob sie von Skript-Kiddies, Cyberkriminellen oder Regierungen aus dem Norden, Süden, Osten oder Westen kamen. Wir sind der Überzeugung, die Online-Welt sollte frei von Angriffen und staatlich unterstützter Spionage sein. Deshalb setzen wir uns weiterhin für eine freie und sichere digitale Welt ein.

Getestet

Kaspersky Lab erzielt regelmäßig Top-Ergebnisse in unabhängigen Auswertungen und Umfragen.

- Im Vergleich mit mehr als **80 bekannten Anbietern** in der Branche
- **72 erste Plätze** in 86 Tests und Rezensionen im Jahr 2017
- **Platzierung in den Top 3*** in 90 % aller Produkttests
- Im Jahr 2017 wurde Kaspersky Lab der **Platinstatus** im Rahmen des „Gartner's Peer Insight** Customer Choice Award" im Bereich Plattform zugesprochen

Unser „Global Research & Analysis"-Team (GReAT) war aktiv an der Entdeckung und Offenlegung einer Reihe der bedeutendsten Malware-Angriffe in Verbindung mit Regierungsbehörden und staatlichen Organisationen beteiligt.

Transparent

Wir sind vollkommen transparent und machen es noch einfacher nachzuvollziehen, was wir tun:

- Unabhängige Prüfung des Unternehmens-Quellcodes, der Software-Updates und der Regeln zur Erkennung von Bedrohungen
- Unabhängige Prüfung interner Prozesse
- Drei Transparenz-Zentren bis 2020
- Erhöhte Prämien für das Aufspüren von Programmfehlern mit bis zu 100 000 US-Dollar pro aufgedeckter Schwachstelle

Unabhängig

Als Privatunternehmen sind wir unabhängig von kurzfristigen Geschäftserwägungen und institutionellen Einflüssen.

Wir teilen unsere Fachkenntnisse, unser Wissen und unsere technischen Erkenntnisse mit der Sicherheitscommunity weltweit, mit IT-Sicherheitsanbietern, internationalen Organisationen und Strafverfolgungsbehörden.

Unser Team arbeitet global und zählt einige der weltweit renommiertesten Sicherheitsexperten zu seinen Mitgliedern. Wir erkennen und neutralisieren alle Arten von APTs, unabhängig von deren Herkunft und Zweck.

* www.kaspersky.com/de/top3
** https://www.gartner.com/reviews/customerchoice- awards/endpoint-protection-platforms

Endpoint Security

Die zuverlässige mehrschichtige-Plattform, basierend auf Next Gen-Cybersicherheitstechnologien

Die Bedrohungslage hat sich exponentiell verschlechtert: Wichtige Geschäftsprozesse, vertrauliche Daten und finanzielle Ressourcen sind einem ständig steigenden Risiko durch Zero-Day-Angriffen 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.

Bei den „Gartner Peer Insights Customer Choice Awards" 2017 für Endpoint-Protection-Plattformen **waren wir der einzige Anbieter, der Platinstatus erreichen konnte***.

* Das Gartner Peer Insights Customer Choice Logo ist ein Markenzeichen bzw. eine Handelsmarke von Gartner, Inc. und/oder seinen Tochterunternehmen und wird hier mit Genehmigung ihres Eigentümers verwendet. Alle Rechte vorbehalten. Die „Gartner Peer Insights Customer Choice Awards" (https://www.gartner.com/reviews/customerchoice-awards/endpointprotection-platforms) werden aufgrund der subjektiven, auf ihren eigenen Erfahrungen beruhenden Meinungen einzelner Endanwender, der Anzahl der veröffentlichten Rezensionen auf Gartner Peer Insights und der Gesamtbewertung für einen bestimmten Anbieter auf dem Markt entsprechend den näheren Angaben unter http://www.gartner.com/reviews-pages/peer-insights-customer-choice-awards/ vergeben und geben in keiner Weise die Meinung von Gartner oder den Tochtergesellschaften von Gartner wieder.

Digitale Transformation bringt zusätzliche Risiken mit sich

Die zunehmende Komplexität vieler IT-Netzwerke in Unternehmen kann zu „Sichtbarkeitslücken" führen, in denen sich Bedrohungen verbergen können.

Ein gezielter Angriff kann sich im Zielsystem durchschnittlich 214 Tage (völlig unbemerkt) versteckt halten.

In dieser Zeit kann die Bedrohung auch weiterhin eine Reihe schädlicher Aktivitäten ausführen. Es ist also äußerst wichtig, effiziente Werkzeuge zu verwenden, die sie schnell erkennen, entfernen und beseitigen.

Trotz der großspurigen Behauptungen einiger Anbieter gibt es keinen Königsweg, der hundertprozentigen Schutz vor allen Arten von Risiken gewährleisten kann. Ebenso gibt es keine Sofortlösung. IT-Sicherheit ist ein ständiger Prozess der Bewertung sich weiterentwickelnder Gefahren, und dann:

- der Anpassung und Aktualisierung von Richtlinien und
- der Einführung neuer Sicherheitstechnologien

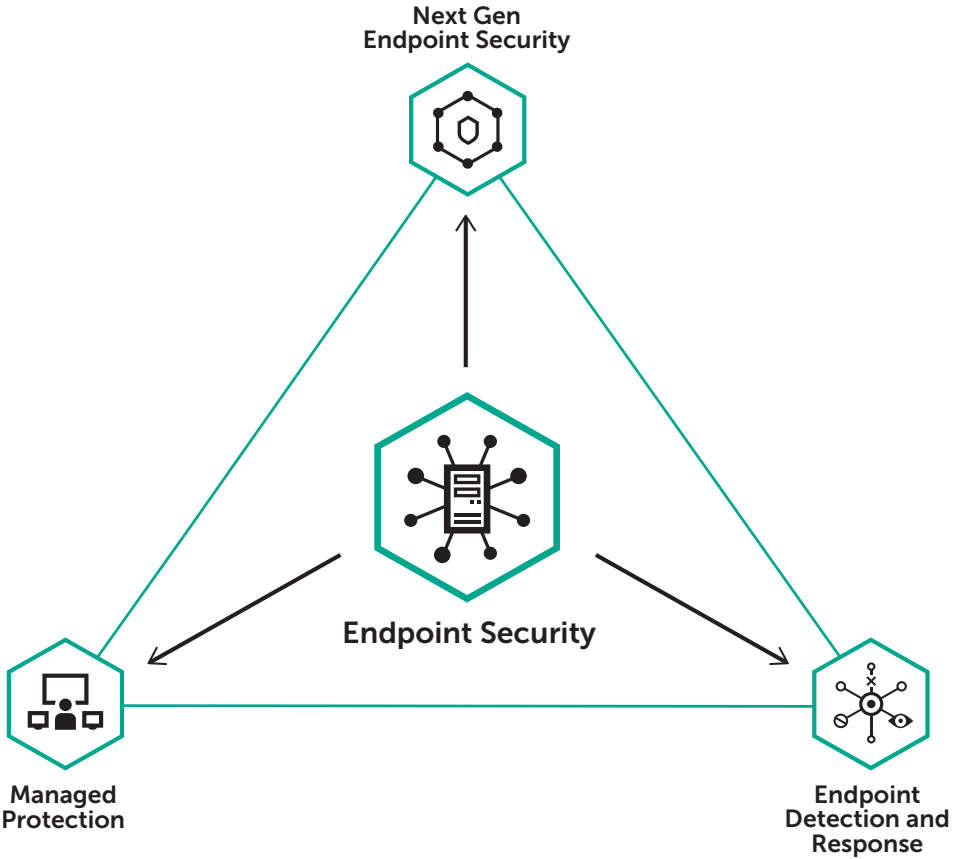
... um neuen Risiken entgegenzutreten.

Kaspersky Endpoint Security erfüllt diese Ansprüche durch eine zuverlässige und bewährte mehrstufige Sicherheitsplattform, die Ihr Unternehmen absichert. Diese integrierte Lösung kombiniert den Schutz vor mit dem Erkennen von Bedrohungen und der Reaktion auf Störfälle. All das basiert auf globaler Threat Intelligence und Next Gen Machine Learning. so erhält Ihr SOC umfangreiche Informationen zur Abwehr von Bedrohungen. Der Schutz für alle physischen, virtuellen und Cloud-basierten Endpoints wird über eine gemeinsame Konsole verwaltet – so erhöhen Sie die Effizienz und senken die Betriebskosten.

Diese Plattform umfasst:

- **Next Gen Endpoint Security**
  Vollständig skalierbarer Schutz, der auf unserer vielfach ausgezeichneten Threat Intelligence Engine beruht und fein abgestufte Kontrollfunktionen sowie Anti-Ransomware und Exploit Prevention beinhaltet.
- **Endpoint Detection and Response**
  Hält proaktiv Angreifer und Bedrohungen auf, bevor diese kostspielige Schäden verursachen, und reagiert schnell und effektiv auf Vorfälle und Datenschutzverletzungen.
- **Managed Protection**
  Ein Rund-um-die-Uhr-Service zur Überwachung und Reaktion auf Störfälle vom anerkannten weltweiten Anbieter für die Untersuchung von APTs wird eigens abgestellt, um gegen Sie gerichtete Cyberbedrohungen aufzuspüren.

Endpoint-Sicherheitslösungen



Wie Angriffe zuschlagen

Die meisten Angriffe haben vier Phasen:

- **Auffinden** – Identifizierung geeigneter Angriffspunkte
- **Eindringen** – in einen Endpoint im Unternehmensnetzwerk
- **Infizieren** – breitet sich oft an viele Orte im Unternehmensnetzwerk aus
- **Umsetzen** – der bösartigen Absichten des Cyberkriminellen

Verteidigung in jeder Phase

Einer der Schlüssel zum Umgang mit einem Angriff besteht in der Einrichtung von Abwehrmechanismen, die in jeder der vier Phasen des Angriffs Schutz bieten.

Auffinden – Risikovermeidung
Sperrt den Zugang zu potentiellen Angriffspunkten

Eindringen – Schutz vor der Ausführung
Erkennt Bedrohungen, bevor sie Infektionen verursachen können

Infizieren – Ablauf nach erfolgter Infektion
Hilft, verdächtiges Verhalten zu erkennen und die Durchführung schädlicher Aktionen zu verhindern

Umsetzen – Automatisierte Reaktion
Hilft dem geschädigten Unternehmen, die Systeme und Daten wiederherzustellen und ähnliche Angriffe zukünftig zu vermeiden

Mehrstufiger Schutz – von einem einzigen Anbieter.

Wir bieten für jede Phase eines Angriffs Schutzmechanismen an – und wir verfügen in jeder Phase nicht nur über einen Abwehrmechanismus, sondern mehrere. Auf diese Weise profitieren unsere Kunden in jeder Phase eines Angriffs von mehrstufigem Schutz.

Schutz in Phase 1 – Gefährdungsprävention
Wir helfen, Angriffe an potentiellen Angriffspunkten zu blockieren.

Zu unseren Schutzstufen gehören:

- Netzwerkfilterung
- Cloud-basierte Inhaltsfilterung
- Portkontrollen

Schutz in Phase 2 – Sicherheitsmaßnahmen vor der Ausführung
Wir helfen, den „Eindringling" am Starten zu hindern.

Zu unseren Schutzstufen und -leistungen gehören:

- Endpoint Hardening
- Reputationsdienste
- lernfähige Systeme, die den Eindringling vor der Ausführung erkennen

Schutz in Phase 3 – Laufzeitkontrolle
Wir suchen vorausschauend auf allen an Ihr Unternehmensnetzwerk angeschlossenen Geräten nach verdächtigem Verhalten, auch auf den privaten mobilen Geräten Ihrer Mitarbeiter.

Zu unseren Schutzstufen gehören:

- Verhaltensanalyse – auf der Grundlage maschinellen Lernens, einschließlich:
  - Exploit-Schutz
  - Ransomware-Schutz
- Kontrolle der Ausführungsberechtigungen

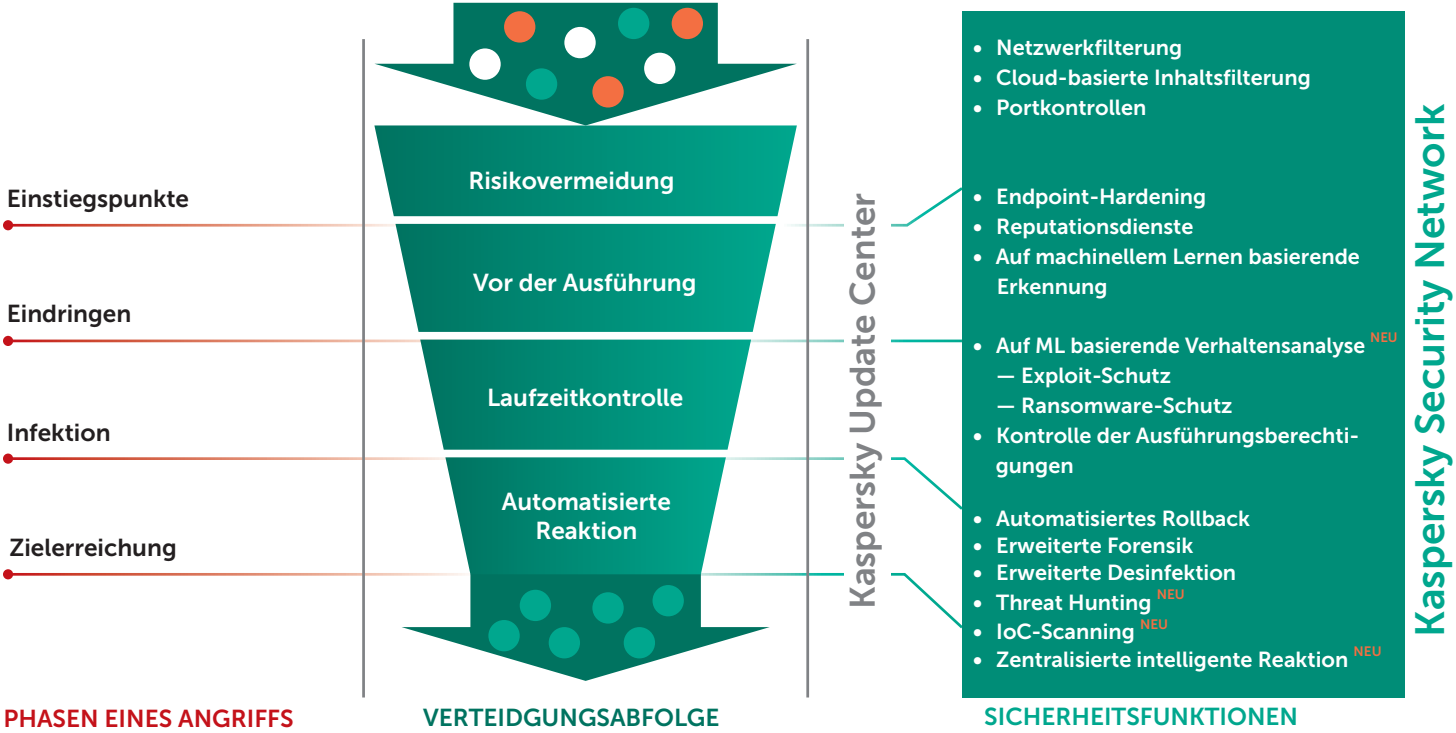
Schutz in Phase 4 – Automatische Reaktion
Wenn Ihr Unternehmen von einem Angriff betroffen war, helfen wir Ihnen bei der schnellen Bewältigung der Nachwirkungen.

Zu unseren Technologien und Dienstleistungen gehören:

- Automatisches Rollback – hilft bei der Wiederherstellung des Systemzustands vor dem Angriff
- Erweiterte Forensik
- Erweiterte Desinfektion
- Threat Hunting
- Scannen nach Gefährdungsindikatoren (Indicator of Compromise, IoC)
- Zentralisierte intelligente Reaktion

Unsere Meta-Stufe hilft Unternehmen, durch Korrelation der Ergebnisse aus den einzelnen Verteidigungsstufen noch mehr gegen gefährliche zielgerichtete Angriffe und APTs zu tun und Bedrohungen zu identifizieren, die möglicherweise von einzelnen Abwehrmechanismen nicht erkannt werden.

Angriffskette



Mobile Sicherheit

Integration von Sicherheit und Management zur Unterstützung Ihrer mobilen Sicherheitsstrategie

Unserer Befragung aus dem Jahr 2017 zufolge wurden 38 % der Unternehmen Opfer von Exploits oder erlitten Verluste, bei denen mobile Geräte als Angriffsvektor fungierten.

1 700 000 USD

Die durchschnittlichen Kosten für ein Unternehmen bei einem Sicherheitsvorfall mit Exploits oder Datenverlust durch mobile Geräte

Schadsoftware, schädliche Webseiten und Phishing-Angriffe auf mobile Geräte nehmen weiter zu, während sich die Einsatzmöglichkeiten von mobilen Geräten immer noch weiterentwickeln. Da sie sowohl zu Hause als auch bei der Arbeit als wichtiges Produktivitätstool eingesetzt werden, stellen sie ein verlockendes Ziel für Cyberkriminelle dar. Die zunehmende Nutzung von persönlichen Geräten zu beruflichen oder geschäftlichen Zwecken (BYOD) führt zu einer größeren Anzahl unterschiedlicher Gerätetypen und Plattformen 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.

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 Ihr 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 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 die Bereitstellung einer mehrstufigen mobilen Gefahrenabwehr (Mobile Threat Defense, MTD) und mobiler Verwaltungsfunktionen. Durch die Kombination dieser Funktionen können Sicherheitsteams vorausschauend im Bereich der mobilen Gefahrenabwehr tätig werden.

Sowohl für Endpoints als auch für mobile Geräte können alle Funktionen von der gleichen Konsole aus verwaltet werden, um die Cyberkriminalität wirksam zu bekämpfen.

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.

Erweiterter Schutz für mobile Geräte

Malware-Schutz wird mit Cloud-basierter Threat Intelligence und maschinellem Lernen verknüpft, um Schutz vor hoch entwickelten mobilen Bedrohungen zu bieten.

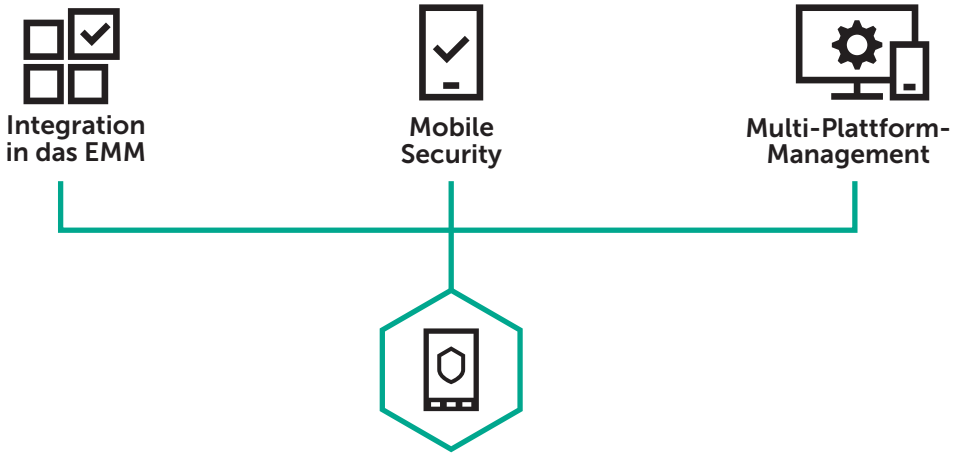
Webkontrolle, Phishing- und Spam-Schutz

Leistungsfähige Internetüberwachung sowie Technologien zur Abwehr von Phishing und Spam schützen vor Phishing-Angriffen sowie unerwünschten Webseiten, Anrufen und Textnachrichten.

Integration in EMM-Plattformen

Vollständige Implementierung und Verwaltung mobiler Sicherheit allein über Ihre EMM-Konsole (VMware, Citrix XenMobile)

Erweiterter Schutz für mobile Geräte



Hybrid Cloud Security

Nahtlose Sicherheit für Umgebungen mit mehreren Clouds optimiert

Unsere Lösung Hybrid Cloud Security bietet einheitlichen mehrstufigen Schutz in Cloud-basierten Umgebungen. Wo auch immer Sie wichtige Geschäftsdaten verarbeiten und speichern – Private oder Public Cloud oder beides – wir bieten die perfekte Kombination aus flexibler, permanenter Sicherheit und Effizienz und schützen Ihre Daten so vor den höchst entwickelten aktuellen und künftigen Bedrohungen, ohne die Leistung des Systems zu beeinträchtigen.

Eine systemeigene Programmierschnittstelle vereinfacht die Bereitstellung, minimiert die Ressourcenbeanspruchung und stellt genau festgelegte Kapazitäten für den Schutz von Umgebungen mit mehreren Clouds gegen Cyberdrohungen aller Art ab. All dies unter einer einheitlichen Sicherheitsorchestrierung und -verwaltung.

Next Generation-Cybersicherheit für jede Cloud

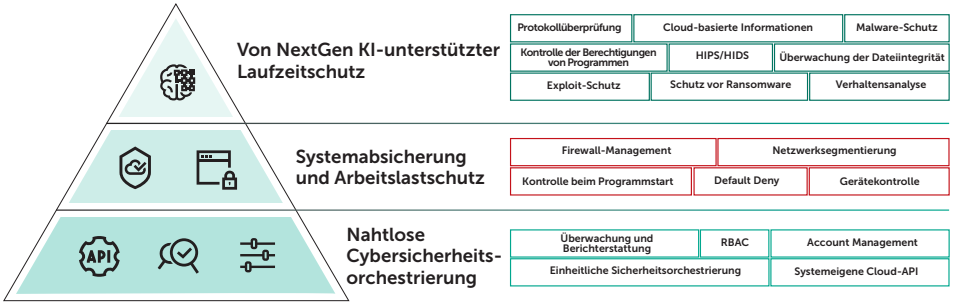
Bietet Schutz in von Ihnen genutzten Public Clouds als Teil Ihrer kollektiven Sicherheitsverantwortung. Durch integrierte Cloud-Programmierschnittstellen machen wir vielfach ausgezeichnete Cybersicherheitstechnologien für jede Cloud-Umgebung einsetzbar.

Einheitliche Orchestrierung und Transparenz

Eine Konsole zur Sicherheitsorchestrierung auf Unternehmensebene sorgt für nahtlose Verwaltbarkeit, Flexibilität und Transparenz. Durch die hervorragende Transparenz wissen Sie über die gesamte Sicherheitsebene Ihrer hybriden Cloud-Umgebung hinweg genau, was geschieht. Zusammen mit der vollständig automatisierten Bereitstellung von Cybersicherheitskapazitäten ermöglicht diese hohe Transparenz eine nahtlose Orchestrierung besserer und schnellerer Sicherheit für Ihre gesamte Cloud-Umgebung.

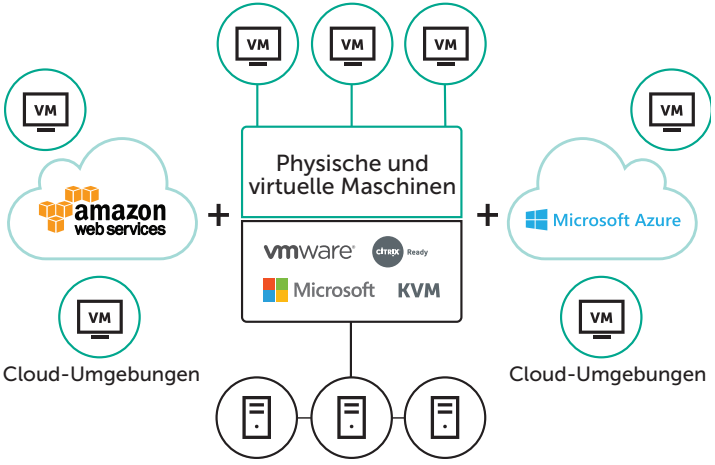
Für flexible und sichere Cloud-Umgebungen

Bewährte Sicherheit für virtualisierte und physische Server, VDI-Bereitstellung, Speichersysteme und sogar Datenkanäle. Eine patentierte Architektur und Integrationskapazitäten ermöglichen die Integration von Cybersicherheit in das Herz Ihrer IT-Umgebung, wobei die operative Leistungsfähigkeit der geschäftskritischen Systeme aufrechterhalten bleibt.



Kaspersky Hybrid Cloud Security

Kaspersky Hybrid Cloud Security bietet Ihnen alles, was für den Aufbau eines perfekt orchestrierten und adaptiven IT-Ökosystems notwendig ist, und stellt Ihnen genau die für die Umgebungen Ihrer Clouds notwendigen Kapazitäten zur Verfügung. Ressourceneffizienz und nahtlose Orchestrierung haben hierbei höchste Priorität. Kaspersky Hybrid Cloud Security wurde konzipiert, um Programme und Daten auf Ihren physischen, virtuellen und in der Cloud angesiedelten Workloads zu schützen, für geschäftliche Nachhaltigkeit zu sorgen und schneller Konformität in Ihrer gesamten hybriden Cloud-Umgebung zu erreichen.



In Ihrem eigenen Rechenzentrum, das Workloads des Unternehmens auf physischen oder virtuellen Servern oder sogar in VDI-Umgebungen übernimmt, sind im Hinblick auf den Erfolg der digitalen Transformationsstrategie eine Reihe von Aspekten zu beachten:

- **Sicherheit bei Datenzugriff und Datenverarbeitung** – unabhängig davon, welche Virtualisierungsplattform oder physische Umgebung Ihre Workloads übernimmt
- **Kompatibilität zwischen IT-Schicht und Sicherheitsschicht** durch systemeigene Programmierschnittstellen, die die Reaktionszeiten auf technisch hochentwickelte Bedrohungen beinahe auf Null reduzieren
- **Effizienter Einsatz betrieblicher Ressourcen** zur Verbesserung der IT-Performance und Aufrechterhaltung der Produktivität geschäftskritischer Systeme

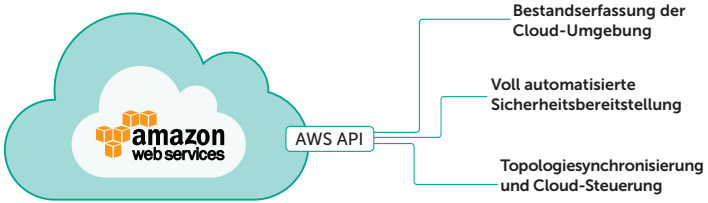
Kaspersky Hybrid Cloud Security bietet nachweislich höchste Qualität beim Schutz Software-definierter Rechenzentren auf Grundlage der Virtualisierungsplattformen VMware NSX, Citrix XenServer, XenDesktop, MS Hyper-V und KVM und nimmt der Verwaltung professioneller IT-Umgebungen ihre Komplexität. Durch Integration in die Kern-IT über systemeigene Programmierschnittstellen werden Sicherheitsanforderungen beinahe ohne Auswirkungen auf die Systemleistung erfüllt.

- Durch die integrierte agentenlose Sicherheit für VMware NSX for vSphere können die Sicherheitsschicht und die IT-Schicht miteinander interagieren und dadurch für erhöhten Schutz sorgen.
- Patentierter Light Agent-Schutz für virtuelle Server und VDI-Plattformen mit ressourceneffizientem und fehlertolerantem Betrieb.
- Herkömmliche mehrstufige Sicherheit für physische Server mit integrierter Anti-Ransomware, Exploit-Prävention und Technologien zur Verhaltenserkennung.

Automatisierte Cybersicherheit für Public Clouds

Der zunehmende Einsatz des Cloud-Modells, bei dem die Ressourcen der eigenen Rechenzentren augenblicklich auf Abruf und nach Bedarf in externe Clouds erweitert werden, bietet hohe Flexibilität, Agilität und klare wirtschaftliche Vorteile. Allerdings macht das Modell der kollektiven Sicherheitsverantwortung hierbei zusätzliche Kapazitäten in Form einer flexiblen Cybersicherheitsschicht notwendig, die Ihre gesamte Cloud-Umgebung abdeckt und Ihre Workloads auf Amazon Web Services (AWS) oder Microsoft Azure schützt.

Lässt sich mit Amazon Web Services (AWS) integrieren



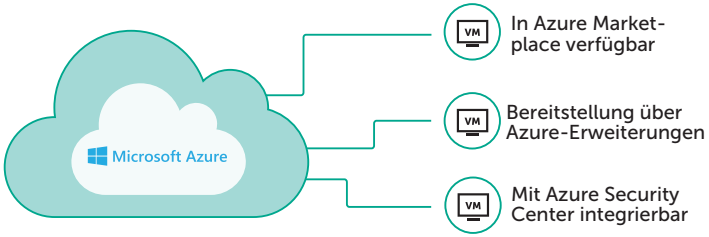
Kaspersky Hybrid Cloud Security hilft beim Schutz von Unternehmensressourcen in der Cloud und erfüllt die Notwendigkeit zum Schutz dessen, was Sie in der Public Cloud bereitstellen, im Rahmen Ihrer kollektiven Sicherheitsverantwortung. Kaspersky Hybrid Cloud Security bietet über MarketPlaces erhältlichen mehrstufigen Schutz, der sich in Cloud-Programmierschnittstellen integrieren lässt und allen Cloud-Umgebungen mit mehr Agilität und nahtloser Verwaltbarkeit vielfach ausgezeichnete Cybersicherheitstechnologien bereitstellt. Hybrid Cloud-Umgebungen werden dadurch einfacher verwaltbar, sicherer und transparenter.

- Führende Cybersicherheit schützt Ihre Workloads in Public Clouds und nutzt eine systemeigene Integration in Erweiterungen von Amazon Web Services (AWS) und Microsoft Azure per Cloud-Programmierschnittstelle.
- Ergänzt Cloud-eigene Sicherheitsfunktionen und hilft unter Einhaltung der DSGVO beim Schutz von Programmen, Betriebssystemen, Daten und Benutzern in der Cloud.
- Durch die intelligente Architektur und die Integration in die Programmierschnittstelle werden die Auswirkungen auf Cloud-Ressourcen minimiert und die Bestandsaufnahme und die Sicherheitsmaßnahmen automatisiert.

Sorgt für noch mehr Schutz

Wir ergänzen Cloud-eigene Tools mit vorausschauender Cybersicherheit, Exploit-Prävention, Integritätsüberwachung, Protokollprüfung, Möglichkeiten zur Programmsteuerung und sogar einer KI-Unterstützung für Laufzeitschutz und Anti-Ransomware. Ein Produkt, das jede Art von Cyberbedrohung bekämpft.

Entwickelt für Microsoft Azure



Zuverlässige Sicherheit für jede Cloud

Noch nie ließ sich die Cloud so nahtlos einsetzen und bot solche Sicherheit. Mit Kaspersky Hybrid Cloud Security ermöglicht die Integration über systemeigene Programmierschnittstellen eine einfachere Bestandsaufnahme der Infrastruktur von Public Clouds und automatisierte Sicherheitsmaßnahmen auf allen Instanzen von AWS und Microsoft Azure.

Kaspersky Hybrid Cloud Security bietet mehrere branchenweit anerkannte Sicherheitstechnologien zur Unterstützung und Vereinfachung der Transformation Ihrer IT-Umgebung und zur Absicherung der Migration von physischen Servern in die virtuelle Cloud, wobei Sichtbarkeit und Transparenz garantieren, dass die Sicherheitsorchestrierung zu einem reibungslosen Erlebnis wird.

Kaspersky Security for Storage

Kaspersky Security for Storage bietet robusten, hochwirksamen und skalierbaren Schutz für wertvolle und vertrauliche Daten, die sich auf Netzwerkspeichern (Network Attached Storages, NAS) und Dateiservern von Unternehmen befinden.

Reibungslose Integration durch schnelle Protokolle wie z. B. ICAP und RPC hält die Effizienz von Speichersystemen aufrecht, sorgt für zuverlässigen und ressourceneffizienten Schutz und optimiert die Benutzerfreundlichkeit. Zuverlässiger Echtzeitschutz für Speicher, einschließlich Selbstschutzfunktionen für eine optimale Kontinuität.

Zuverlässiger und transparenter Datenschutz

- Systemeigene Integrierbarkeit sorgt für Flexibilität, Skalierbarkeit und herausragende betriebliche Effizienz ohne nachteilige Auswirkungen auf die Leistung oder Produktivität der Datenspeichersysteme.
- Innovative Technologien ermöglichen den Einsatz technisch hochentwickelter Datensicherungsfunktionen, sorgen für eine außergewöhnliche Fehlertoleranz und schützen sogar vor Ransomware-Angriffen.

Datensicherheit an allen Speicherorten

- Systemeigene Integration mit den neuesten NAS und Betrieb auf unternehmenseigenen Dateiservern
- Alle Dateien in den Datenspeichern sind sicher – ohne dass Sie den Malware-Schutz an Endpoints oder auf mobilen Geräten prüfen müssen.
- Flexible und granulare Konfiguration ermöglicht routinemäßige und bedarfsabhängige Malware-Scans
- Selbstschutzfunktionen sorgen für eine optimale Betriebskontinuität

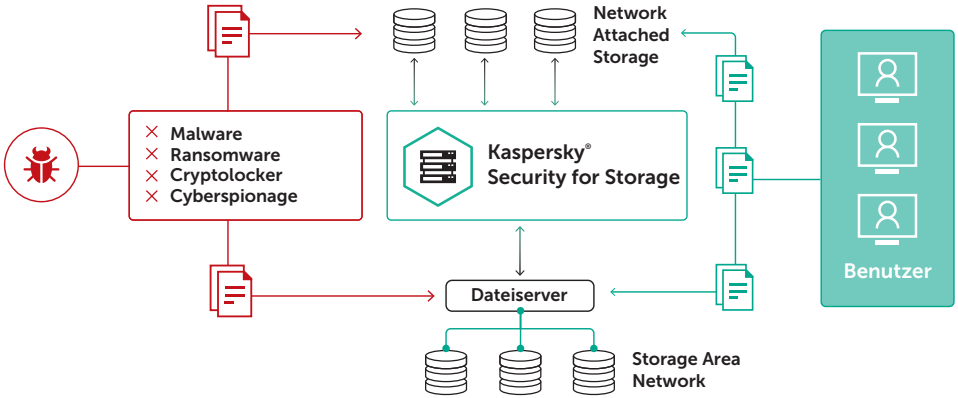
Bekämpft Malware und Ransomware

- Der Malware-Schutz unserer vielfach ausgezeichneten Scan-Engine schützt alle Dateien selbst vor technisch hochentwickelten Angriffen
- Echtzeitschutz vor Ransomware für NetApp-Netzwerkspeicher mithilfe von FPolicy (von Kaspersky Lab)
- Unterstützung für eine breite Palette von Speichergeräten dank Integration über mehrere Protokolle

"Leichte", aber dennoch zuverlässige Sicherheit

- Integration über systemeigene Programmierschnittstelle bedeutet mehr Sicherheit mit weniger Auswirkungen auf die Produktivität der Endbenutzer
- Load Balancing und Fehlertoleranz sorgen für unterbrechungsfreien Schutz
- Vollständige Transparenz der Cybersicherheit Ihrer Dateien über Ihre gesamte Speicherinfrastruktur hinweg

Kaspersky Security for Storage kann mit Kaspersky Hybrid Cloud Security kombiniert werden, um sowohl die physischen als auch die virtuellen Komponenten Ihres unternehmenseigenen Rechenzentrums mit dem besten verfügbaren Schutz auszustatten.



Kaspersky DDoS Protection

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-Angriffen, die in der Regel automatisch ablaufen, sind DDoS-Angriffe 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.

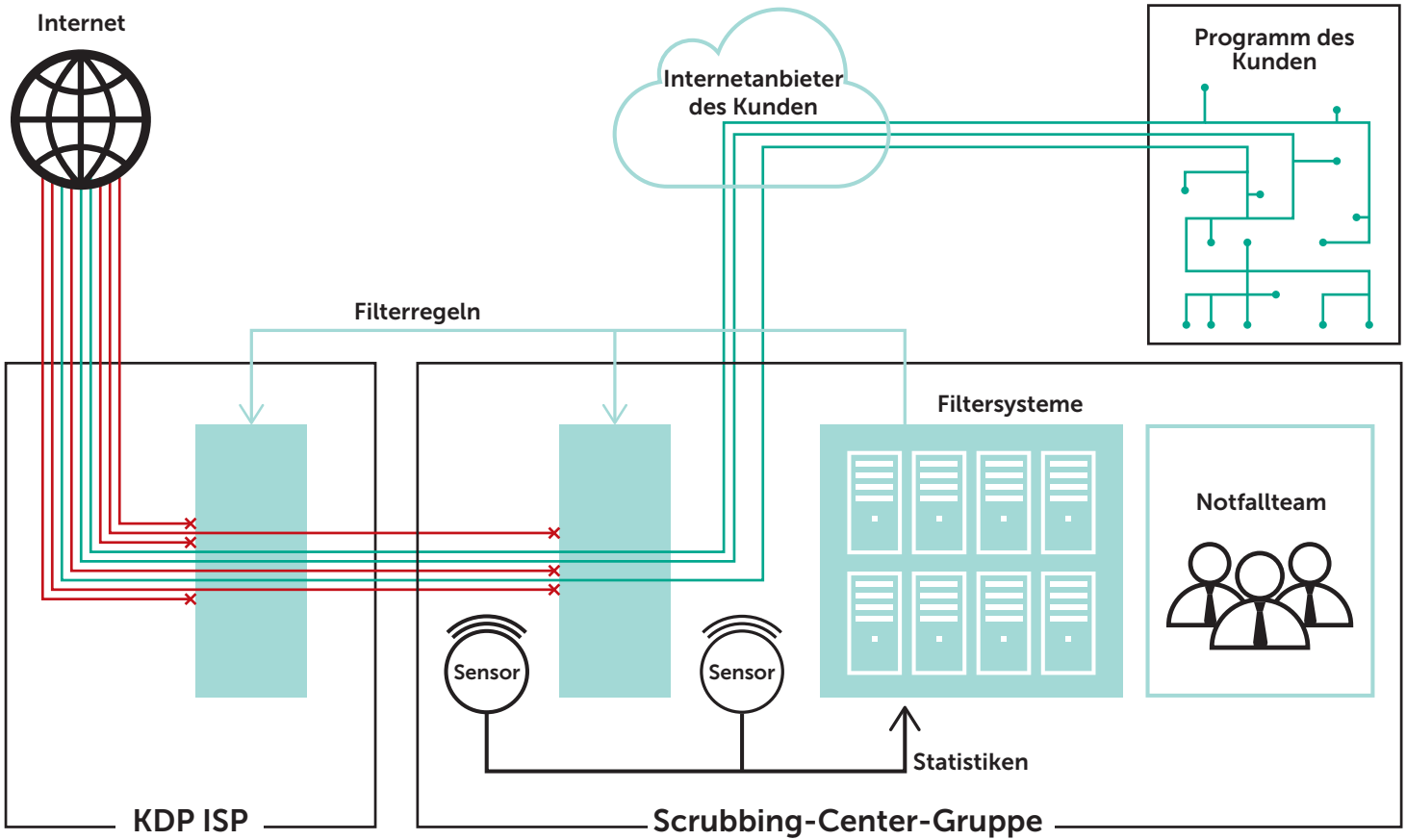
Sobald ein mögliches Angriffsszenario erkannt wurde, wird das Security Operations Center (SOC) von Kaspersky Lab alarmiert. Bei den Deployment-Szenarien Kaspersky DDoS Protection Connect und Connect+ wird die Abwehr automatisch eingeleitet, während unsere Techniker sofort detaillierte Prüfungen durchführen, 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 Geschäfts 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


Internet
Internetanbieter des Kunden
Programm des Kunden
Filterregeln
Filtersysteme
Notfallteam
Sensor
Sensor
Statistiken
KDP ISP
Scrubbing-Center-Gruppe

Threat Management and Defense

Erweiterter Schutz und Threat Intelligence

Der Schutz hochgradig digitalisierter Infrastrukturen stellt Unternehmen vor erhebliche neue Herausforderungen:

- Bei der Reaktion auf Vorfälle fallen umfangreiche manuelle Aufgaben an
- Unterbesetzte IT-Sicherheitsteams und ein Mangel an Fachwissen
- Zu viele Sicherheitsvorfälle, die in einem begrenzten Zeitraum eine Verarbeitung, Analyse, Triage und Reaktion erfordern
- Mangel an Vertrauen und Probleme bei der Einhaltung von Vorschriften zur gemeinsamen Datennutzung, wenn die digitale Infrastruktur erweitert wird
- Mangelnde Sichtbarkeit und Probleme bei der Beweiserhebung für die Analyse nach einem Vorfall

Mehrwert durch Investition in Threat Management und Gefahrenabwehr:

- Reduzierung finanzieller und betrieblicher Schäden, die durch Cyberkriminalität verursacht werden
- Reduzierung der Komplexität durch eine einfache, für Unternehmen konzipierte Verwaltungsschnittstelle
- Geringere Verwaltungskosten durch Automatisierung und vereinfachte Prozesse zur Einhaltung von Sicherheitsvorschriften
- ROI-Steigerung durch nahtlose Workflow-Automatisierung ohne Unterbrechung der Geschäftsabläufe
- Abgeschwächte Folgen technisch hochentwickelter Bedrohungen dank schneller Erkennung

Digitale Transformation – eine neue Rolle für die Cybersicherheit

Die digitale Transformation ist ein Schlüsselfaktor für das Wachstum und bietet Unternehmen viele neue Möglichkeiten, beinhaltet aber gleichzeitig Risiken hinsichtlich der Sicherheit der IT-Infrastruktur sowie der Einhaltung gesetzlicher Vorschriften und der sicheren Datennutzung. Zielgerichtete Angriffe und komplexe Bedrohungen wie z. B. hochentwickelte, hartnäckige Bedrohungen (Advanced Persistent Threats, APTs) gehören mittlerweile zu den größten Gefahren, denen Unternehmen ausgesetzt sind. **Kaspersky Threat Management and Defense** ist eine einheitliche Lösung zur Innovationsbeschleunigung bei der digitalen Transformation und passt sich durch Spitzentechnologie in Kombination mit Cybersicherheitsdiensten an die Besonderheiten des Unternehmens und seine laufenden Prozesse an, sodass Sie eine einheitliche Methodik für den kompletten Schutz des Unternehmens gegen hochentwickelte Bedrohungen und spezielle zielgerichtete Angriffe entwickeln können.

Mit Kaspersky Threat Management and Defense kann die Strategie des Unternehmens für das Bedrohungsmanagement weiterentwickelt oder intensiviert werden, indem mithilfe lernfähiger Systeme die Vorfallsanalyse und die Sammlung von Informationen und digitalen Beweismitteln automatisiert und die manuelle Erkennung vereinfacht wird. Der reichhaltige Datenpool ermöglicht komplexe Vorfallsuntersuchungen und bietet die nötige Unterstützung und Expertise zur Abwehr selbst raffiniertester Bedrohungen.

Kaspersky Threat Management and Defense bietet eine einzigartige Kombination aus führenden Technologien und Services, welche die Implementierung einer adaptiven Sicherheitsstrategie unterstützen. Diese Lösung hilft Ihnen dabei, die meisten Angriffe abzuwehren, spezifische neue Bedrohungen schnell festzustellen, auf Vorfälle in Echtzeit zu reagieren und zukünftige Bedrohungen zu antizipieren. Kaspersky Threat Management and Defense umfasst die folgenden Komponenten:

- **Kaspersky Anti Targeted Attack** auf Grundlage hochkarätiger Sicherheitsinformationen und fortschrittlicher Technologien für maschinelles Lernen in Verbindung mit Netzwerk- und Endpoint-Überwachung, hochentwickelter Sandbox-Technologie und durch Threat Intelligence gelenkten Analysen. Kaspersky Anti Targeted Attack setzt verschiedene Ereignisse zueinander in Beziehung und gibt Störfällen Priorität, damit Unternehmen zielgerichtete Angriffe, technisch hochentwickelte Bedrohungen und bereits befallene Systeme erkennen können.
- **Kaspersky Endpoint Detection and Response** verbessert die Sichtbarkeit von Endpoint-Bedrohungen und sammelt automatisch die forensischen Daten, um sie zentral zu speichern. Kaspersky Endpoint Detection and Response verwendet die gleiche Schnittstelle wie Kaspersky Anti Targeted Attack und den gleichen Agenten wie Kaspersky Endpoint Security, um einen vielseitigen Lösungsansatz zur Aufdeckung, Erkennung und Enthüllung komplexer zielgerichteter Angriffe bereitzustellen. Der Schwerpunkt liegt auf der Erkennung von Bedrohungen durch den Einsatz hochentwickelter Technologien, der rechtzeitigen Reaktion auf Angriffe und der Verhinderung böswilliger Handlungen durch Entdeckung von Bedrohungen auf Endpoints.
- **Kaspersky Cybersecurity Services** bietet schnelle und professionelle Unterstützung während eines Vorfalls – und auch danach, indem das Risiko von Datenverlusten sowie der mögliche finanzielle Schaden und Reputationsverlust möglichst gering gehalten werden. Das Portfolio von Cybersecurity Services umfasst einen breit angelegten Lehrplan für Sicherheitsschulungen, auf die Minute aktuelle Threat Intelligence, eine Sofortreaktion bei Vorfällen, vorausschauende Security Assessments, vollständig ausgelagerte Threat Hunting-Leistungen sowie Premium Support rund um die Uhr.

Je nachdem, welchen Bedarf an erweiterten Präventionskapazitäten ein Kunde und welche Anforderungen seine spezifische Infrastruktur hat (z. B. die vollständige Isolierung der Unternehmensdaten), können wir unsere Lösung Threat Management and Defense mit folgenden Produkten weiter verbessern, um Ihnen einen wirklich integrierten strategischen Ansatz zur Risikominderung und Vorbeugung hochentwickelter Bedrohungen und zielgerichteter Angriffe zu bieten:

- **Kaspersky Endpoint Security** ist eine mehrschichtige Endpoint Protection-Plattform, die auf Next Gen-Cybersicherheitstechnologien unter Einsatz von HuMachine Intelligence beruht und durch maschinelles Lernen, Verhaltenserkennung, Steuerungsmöglichkeiten, Datensicherung und vieles mehr flexible, automatisierte Abwehrmechanismen gegen die ausgeklügeltsten bekannten und unbekannten Bedrohungen wie z. B. Fileless-Angriffe und Ransomware bietet.
- **Kaspersky Secure Mail Gateway** funktioniert als Teil des Vorbeugungskonzepts gegen zielgerichtete Angriffe und bietet automatisierte Prävention von E-Mail-Bedrohungen sowie hervorragenden Schutz vor Spam, Phishing und allgemeinen und hochentwickelten Malware-Bedrohungen des Datenverkehrs auf Mailservern. Kaspersky Secure Mail Gateway kann selbst in den komplexesten heterogenen Infrastrukturen effektiv arbeiten, und zwar unabhängig davon, welches Modell für die E-Mail-Zustellung verwendet wird: Cloud, im eigenen Rechenzentrum oder verschlüsselt.
- **Private Kaspersky Security Network** bietet eine Datenbank mit umfassender Threat Intelligence für isolierte Netzwerke und Umgebungen mit strengen Einschränkungen für die Datenweitergabe, sodass Unternehmen die meisten Vorteile Cloud-basierter Sicherheit voll nutzen können, ohne irgendwelche Daten außerhalb des kontrollierten Bereichs zu lassen. 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.

Kaspersky Anti Targeted Attack

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

Kaspersky Anti Targeted Attack bietet Unternehmen Folgendes:

- Integrale Geschäftskontinuität, die durch die Integration von Sicherheit und Compliance in neue Prozesse von Anfang an erreicht wird
- Einblick in Schatten-IT und versteckte Bedrohungen
- Maximale Flexibilität für die Bereitstellung in physischen und virtuellen Umgebungen überall dort, wo Transparenz und Kontrolle erforderlich sind
- Automatisierung von Untersuchungs- und Reaktionsaufgaben, um die Kosteneffizienz Ihrer Sicherheits-, Vorfallsreaktions- und SOC-Teams zu optimieren
- Enge, unkomplizierte Integration in bestehende Sicherheitsprodukte zur Verbesserung des allgemeinen Sicherheitsniveaus und zum Schutz älterer Investitionen in die Sicherheit

Kaspersky Endpoint Detection and Response

Herkömmliche Produkte für die Endpoint-Sicherheit (z. B. Kaspersky Endpoint Security) spielen eine wichtige Rolle beim Schutz gegen eine Vielzahl von Bedrohungen wie Ransomware, Malware, Botnets usw. Um sich vor einer noch breiteren Palette an hochentwickelten Cyberangriffen und intelligenten Gegnern zu schützen, müssen Unternehmen nun an den Endpoints zusätzliche Schutzebenen zum Einsatz bringen, z. B. Endpoint-Erkennung und Reaktionsmechanismen.

Kaspersky Endpoint Detection and Response unterstützt Unternehmen mit:

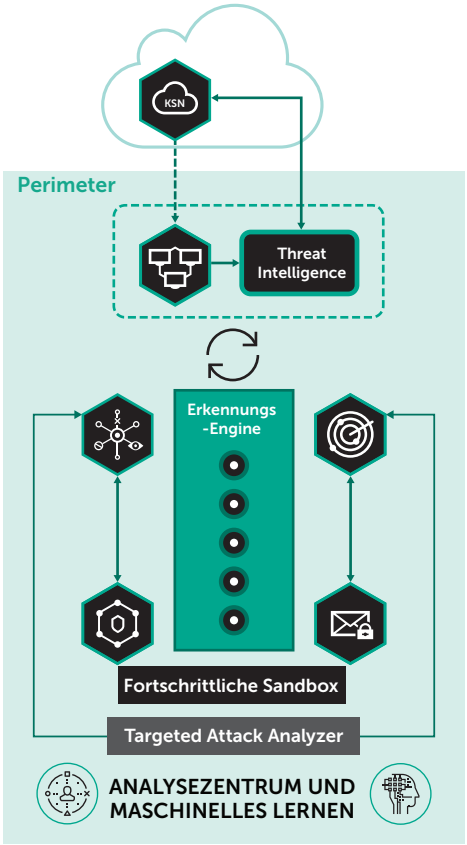
- Automatisierte Erkennung und Reaktion auf Bedrohungen bei unterbrechungsfreiem Geschäftsbetrieb
- Verbesserung der Endpoint-Transparenz und Erkennung von Bedrohungen durch fortschrittliche Technologien wie maschinelles Lernen, Sandboxing, IoC-Scanning und Threat Intelligence
- Verbesserung der Cybersicherheit mit einer benutzerfreundlichen Unternehmenslösung für die Reaktion auf Störfälle
- Aufbau einheitlicher und effektiver Prozesse für Threat Hunting, Incident Management und Vorfallsreaktion

Kaspersky Secure Mail Gateway

Kaspersky Secure Mail Gateway ist eine automatisierte Lösung zur Prävention von E-Mail-Bedrohungen, die als Teil eines einheitlichen Ansatzes zur Erkennung und Vermeidung von zielgerichteten Angriffen hochentwickelte Technologien für den Schutz von E-Mail-Verkehr jeglicher Art bereitstellt. Kaspersky Secure Mail Gateway bietet innovative Cloud-basierte Abwehrfunktionen gegen Spam und Phishing sowie mit Zero-Day-Funktionen und Anti-Exploit-Kapazitäten technisch hochentwickelten Schutz vor Malware, der mithilfe von Threat Intelligence, maschinellem Lernen und fortschrittlichem Sandboxing ein mehrstufiges und automatisiertes E-Mail-Sicherheitskonzept bietet.

Kaspersky Secure Mail Gateway bietet Unternehmen:

- Automatisierte Vermeidung bekannter, unbekannter und zukünftiger Bedrohungen
- Cloud-gestützte Dateianalyse auf Grundlage der Signatur
- Dateianalyse mithilfe von maschinellem Lernen
- Schnelle Benachrichtigung bei Sicherheitsvorkommnissen
- Nahtlose Verbesserung der Cybersicherheit im Unternehmen



Kaspersky Private Security Network

Das Kaspersky Private Security Network ist eine lokale und komplett private Version des Kaspersky Security Network (KSN), durch die Unternehmen, die nicht wünschen, dass irgendwelche Daten ihren kontrollierten Perimeter verlassen, von den meisten Vorteilen globaler Cloud-basierter Threat Intelligence profitieren können.

Das Kaspersky Private Security Network (als patentierte Technologie):

- 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
- Erfüllt behördliche Auflagen, Sicherheits- und Datenschutznormen

Cybersecurity Services

Informationen und Kompetenz sorgen für Cyberimmunität auf einem neuen Niveau

Threat Intelligence Portal

Durch Freigabe unserer auf zeitgenauen aktuellen Daten für unsere Kunden gewährt Kaspersky Lab Unternehmen einen Rundumblick auf die Methoden, Taktiken und Werkzeuge der Bedrohungsakteure und hilft ihnen, sich gegen moderne Cyberbedrohungen zu schützen. Unsere große Bandbreite von Threat Intelligence Services trägt dazu bei, dass Ihr Security Operations Center und/oder IT-Sicherheitsteam bestens zur Abwehr selbst raffiniertester Bedrohungen gerüstet ist.

- **Threat Data Feeds:** Verbessern Sie Ihre Sicherheitskontrollen (SIEM, IDS, Firewalls usw.) und forensischen Fähigkeiten mit unseren auf die Minute aktuellen Cyberbedrohungsdaten, die wir in einer Vielzahl von Formaten und Methoden bereitstellen.
- **APT Intelligence Reporting** ermöglicht den exklusiven und frühzeitigen Zugang zu Informationen über hochkarätige Cyberspionage-Aktionen, darunter auch Gefährdungsindikatoren (Indicators of Compromise, IOCs) und YARA-Regeln.
- **Financial Threat Intelligence Reporting** konzentriert sich auf speziell gegen finanzielle Institutionen gerichtete Bedrohungen wie z. B. zielgerichtete Angriffe, Angriffe auf spezifische Infrastrukturen (z. B. ATM/POS) und von Cyberkriminellen für den Angriff auf Banken, Zahlungsdienstleister und POS-Systeme entwickelte oder verkaufte Tools.
- **Tailored Threat Reporting:** Auf Ihr Unternehmen bzw. Ihr Land zugeschnittene Threat Intelligence aus urheberrechtlich geschützten und offenen Quellen im „Deep Web" und „Dark Web".
- **Threat Lookup:** Über ein Webportal erhalten Sie vollständigen Zugriff auf alle von Kaspersky Lab erworbenen Erkenntnisse zu Bedrohungsindikatoren und ihren Beziehungen untereinander.
- **Cloud Sandbox** ermöglicht es Ihnen, verdächtige Dateien an Kaspersky Lab zu senden, mithilfe unserer weltweit führenden Technologie eine detaillierte Beschreibung des Verhaltens der Datei zu erhalten und dank der engen Integration mit Kaspersky Threat Lookup umfassende und tiefgreifende Untersuchungen durchzuführen.
- **Phishing Tracking:** Sie erhalten Echtzeitbenachrichtigungen zu laufenden Phishing-Angriffen auf Ihr Unternehmen oder Ihre Kunden.
- **Botnet-Überwachung:** Echtzeitbenachrichtigungen über laufende Botnet-Angriffe, die eine Bedrohung für Ihre Kunden und Ihren Ruf darstellen.

Security Assessment

Kaspersky Security Assessment Services – Kompetente Sicherheitsanalysen und neueste Forschungsergebnisse wirken zusammen, um Informationssysteme jeder Komplexität in realen Umgebungen zu testen.

Penetration Testing
Die Simulation böswilliger Handlungen mithilfe von Threat Intelligence zeigt potentielle Angriffsvektoren auf und gibt Ihnen einen Überblick über die Sicherheitsstellung Ihres Unternehmens aus Sicht eines Angreifers.

Application Security Assessment
Eine intensive Suche nach möglichen Fehlern in der Geschäftslogik und Implementierungsschwachstellen in Programmen jeglicher Art, von großen Cloud-basierten Lösungen bis hin zu Embedded Applications und mobilen Apps.

Payment Systems Security Assessment
Umfassende Analyse der Hardware- und Softwarekomponenten von Zahlungssystemen, um potentielle Betrugsszenarien und Sicherheitslücken aufzudecken, die zur Manipulation finanzieller Transaktionen führen können.

ICS Security Assessment
Fallspezifische Bedrohungsmodelle und Vulnerability Assessment für industrielle Steuerungssysteme und ihre Komponenten, die Aufschluss über Ihre aktuellen Angriffsflächen und die potentiellen Geschäftsauswirkungen eines Angriffs geben.

Transportation Systems Security Assessment
Spezialisierte Forschung mit Schwerpunkt auf der Ermittlung von Sicherheitsproblemen in Zusammenhang mit entscheidenden Komponenten moderner Verkehrsinfrastrukturen, vom Straßenverkehr bis hin zur Luft- und Raumfahrt.

Smart Technologies and IoT Security Assessment
Eine detaillierte Bewertung der heutigen, in hohem Grad untereinander vernetzten Geräte und ihrer Backend-Infrastruktur, um Schwachstellen in der Firmware-, Netzwerk- und Programmebene aufzudecken.

Threat Hunting

Auf vorausschauendes Threat Hunting ausgelegte Techniken, die von hoch qualifizierten und erfahrenen Sicherheitsexperten ausgeführt werden, wirken bei der Aufdeckung im Unternehmen verborgener hochentwickelter Bedrohungen mit.

- **Kaspersky Managed Protection**
  Überwachung und kontinuierliche Analyse Ihrer Cyberbedrohungsdaten durch die Experten von Kaspersky Lab rund um die Uhr.
- **Targeted Attack Discovery**
  Ein umfangreiches Angebot, das die proaktive Identifizierung aktueller oder früherer Anzeichen für eine Gefährdung sowie die Reaktion auf zuvor nicht bemerkte Angriffe ermöglicht.

Incident Response

Die Incident Response Services von Kaspersky Lab werden von erfahrenen Experten auf dem Gebiet der Analyse von Cyberbedrohungen sowie von Ermittlern erbracht. Wir setzen unser gesamtes Wissen und unsere globale Erfahrung für die Behebung Ihres Sicherheitsvorfalls ein.

- **Incident Response:** Hier wird der gesamte Zyklus der Vorfallsuntersuchung abgedeckt, um die Bedrohung für Ihr Unternehmen vollständig zu beseitigen.
- **Digital Forensics:** Hierbei werden die digitalen Beweise von Cyberkriminalität zur Erstellung eines umfassenden Berichts mit sämtlichen relevanten Erkenntnissen analysiert.
- **Malware Analysis:** Hier erfahren Sie, wie genau sich bestimmte Malware-Dateien verhalten und wie sie funktionieren.

Sicherheitsschulung

Wir bieten ein Schulungsprogramm an, das alles abdeckt: von den Grundlagen über die fortschrittlichen Techniken und Tools der digitalen Forensik bis hin zur Malware-Analyse und Vorfallsreaktion. So kann Ihr Unternehmen sein Wissen rund um die Cybersicherheit verbessern.

- **Digitale Forensik:** Teilnehmer dieses Kurses können Erfahrungslücken schließen und ihre praktischen Fertigkeiten bei der Suche nach digitalen Spuren von Cyberkriminalität sowie bei der Analyse verschiedener Datentypen zur Ermittlung des zeitlichen Ablaufs und der Quellen des Angriffs entwickeln und verbessern.
- **Malware-Analyse und Reverse Engineering:** In diesen Kursen erfahren die Teilnehmer, wie sie Malware analysieren, IOCs erfassen, Signaturen zur Erkennung von Malware auf infizierten Geräten schreiben und infizierte/verschlüsselte Dateien und Dokumente wiederherstellen.
- **Incident Response:** Die Kurse führen Ihr internes Team durch sämtliche Phasen der Vorfallsreaktion und statten es mit dem umfassenden Wissen aus, das für eine erfolgreiche Wiederherstellung nach Vorfällen erforderlich ist.
- **Effiziente Bedrohungserkennung mit YARA:** Die Teilnehmer erfahren, wie sie effektive YARA-Regeln schreiben, testen und so verbessern können, dass durch andere Methoden nicht auffindbare Bedrohungen entdeckt werden.

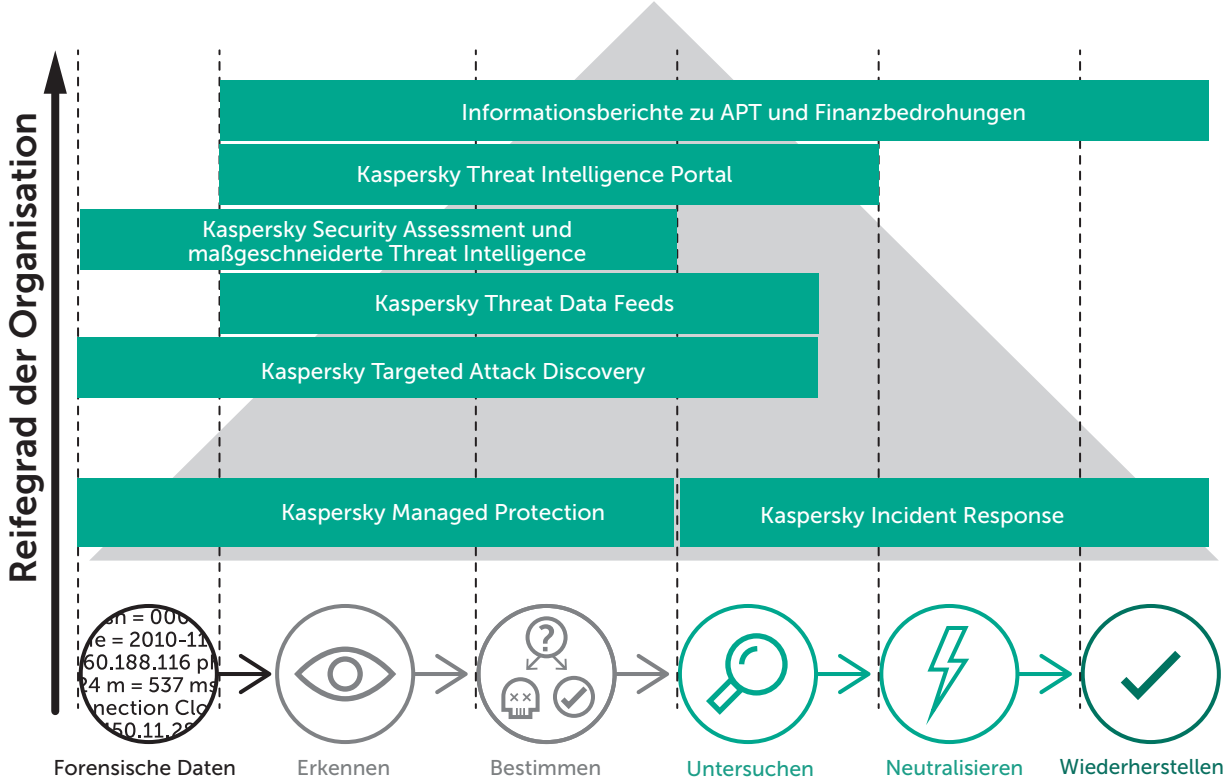
Kaspersky Cybersecurity Services

Programm „Kaspersky Security Training“

Hochentwickelte digitale Forensik und Malware-Analyse

Digitale Forensik und Malware-Analyse

Cybersecurity Awareness



Cybersecurity Awareness

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

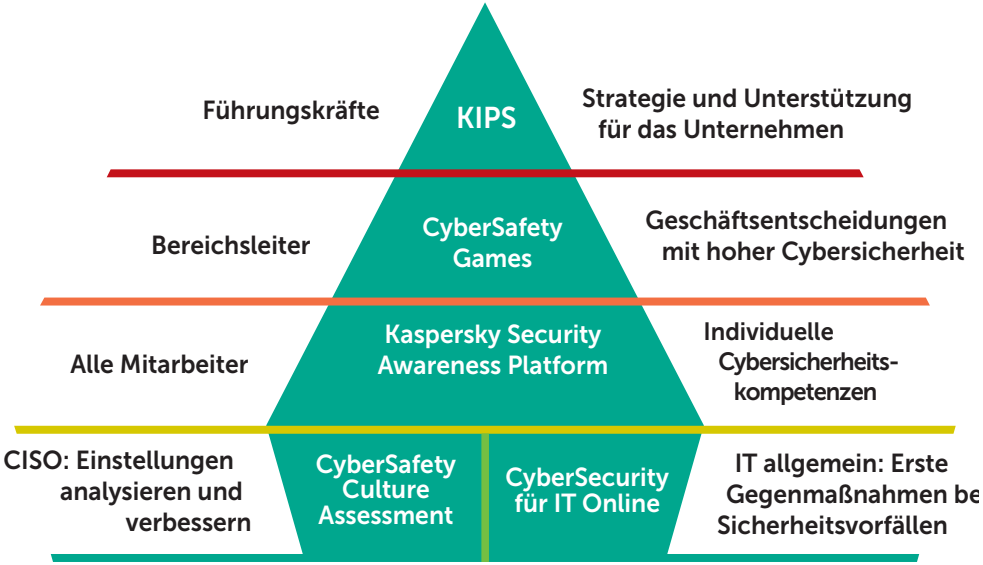
Im Durchschnitt müssen große Unternehmen rund 1 155 000 US-Dollar für die Wiederherstellung nach Angriffen zahlen, die durch unachtsame oder unwissende Mitarbeiter verursacht wurden, während kleine und mittlere Unternehmen nur 83 000 US-Dollar ausgeben. Mehr als 80 % aller Cybersicherheitsvorfälle entstehen durch menschliche Fehler. 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

Security Awareness von Kaspersky Lab



Erfolgreicher 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.

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. Im Zeitalter von Industry 4.0 sind die meisten nicht kritischen Industrienetzwerke über das Internet zugänglich, ob gewollt oder nicht.

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, Engineering-Workstations, SPS, Netzwerkverbindungen und Mitarbeiter, ohne dabei die Geschäftskontinuität und Konsistenz der industriellen 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 Cybersecurity Assessment bis hin zur Vorfallsreaktion
- Spezielle Sicherheitstechnologien, die eigens für industrielle Systeme entwickelt wurden
- Geringere Ausfallzeiten und weniger Verzögerungen bei industriellen Prozessen

Kaspersky Industrial CyberSecurity

Technologien

Anomalieerkennung (DPI)

Integration in andere Systeme

Anti-Malware

Integritätskontrolle

Zentralisierte Verwaltung

Vorfallsuntersuchung

Intrusion Detection System

Services

Schulung und Intelligence

- Cybersecurity Training
- Awareness-Programme
- Threat Intelligence

Expert Services

- Cybersecurity Assessments
- Lösungsintegration
- Wartung
- Vorfallsreaktion

Fraud Prevention

Die erweiterte Lösung für ein nahtloses Benutzererlebnis und die vorausschauende Vereitelung von Betrugsversuchen in Echtzeit

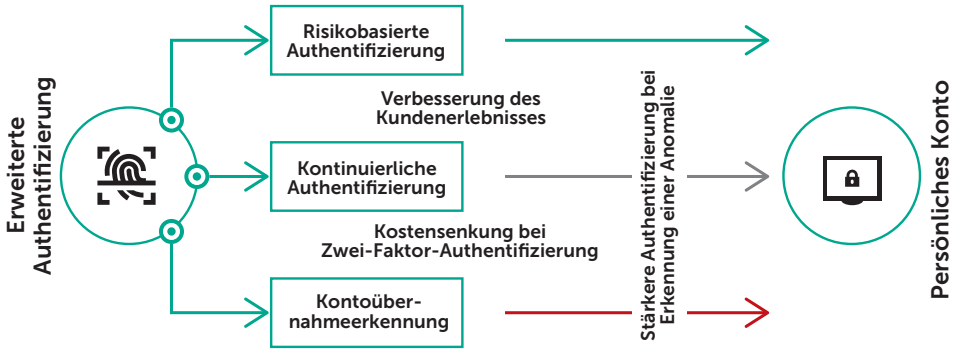
Der Weg in die digitale Welt ist nicht einfach nur ein Trend: Er ist eine Notwendigkeit. In Zeiten, in denen die meisten Kunden für alltägliche Aktivitäten Online- und mobile Kanäle nutzen, müssen Unternehmen hochwertige Services mit maximaler Funktionalität bereitstellen. Zur selben Zeit müssen sie das Gleichgewicht zwischen Online-Sicherheit und reibungsloser Kundenfreundlichkeit finden. Und genau hier kommt Kaspersky Fraud Prevention ins Spiel: Die Lösung unterstützt Sie beim Ausbau und der Weiterentwicklung Ihrer Online- und mobilen Kanäle, ohne dass hierdurch zusätzliche Stressfaktoren, Sicherheitsbedenken oder Online-Nutzungsprobleme entstehen.

Kaspersky Fraud Prevention funktioniert auf Grundlage eines komplexen Portfolios hochentwickelter Technologien wie z. B. Verhaltensanalysen und Biometrie, Geräte- und Umweltanalysen, die in der Kaspersky Fraud Prevention Cloud zusammengeführt werden. Bei der vorausschauenden Erkennung komplexer Betrugssysteme über Internet und mobile Kanäle kommt maschinelles Lernen zum Einsatz. So profitieren Betrugsüberwachungssysteme vom zusätzlichen Kontext hinsichtlich einer rechtzeitigen und präzisen Entscheidungsfindung sowie der intelligenten und flexiblen Nutzung einer beschleunigten Authentifizierung.

Die Lösung besteht aus zwei vollwertigen Produkten, die entweder getrennt voneinander zur Lösung relevanter geschäftlicher Probleme verwendet werden können oder gemeinsam deutlich die Sicherheitsstufe anheben und den Betrugsschutz und die Benutzerfreundlichkeit verbessern.

Advanced Authentication wurde zur Verbesserung der Benutzerfreundlichkeit, Kostenreduzierung bei der Zwei-Faktor-Authentifizierung und kontinuierlichen Ermittlung verdächtiger Aktivität entwickelt, was letztendlich geschäftliches Wachstum und ein höheres Sicherheitsniveau mit sich bringt.

Direkt ab dem Zeitpunkt der ersten Anmeldung analysiert Advanced Authentication kontinuierlich Ereignisse, damit Risiken ermittelt und entsprechende Empfehlungen ausgesprochen werden können.



Automated Fraud Analytics verwendet eine perfekt ausgewogene Kombination modernster Technologien mit globaler Threat Intelligence und menschlicher Expertise. Durch diese gebündelte Kompetenz können alle wichtigen Daten analysiert werden, damit rechtzeitig die richtigen Entscheidungen getroffen werden und auch komplexe Betrugsversuche erkannt werden. Aktivitäten, die möglicherweise betrügerisch sind, werden bereits im Vorfeld erkannt und die betroffenen Unternehmen gewarnt.

Im Verlauf einer Benutzersitzung werden Ereignisse, die Benutzer, ihre Geräte und die Umgebungen dieser Geräte betreffen, in Betrugsmanagementsysteme eingespeist, die mithilfe dieser Daten zeitgerecht korrekte Entscheidungen treffen. In der Kaspersky Fraud Prevention Cloud stehen generierte Vorfälle bereit, um Aufschlüsse über tatsächliche Betrugsfälle zu gewinnen und dem Problem wirklich auf den Grund zu gehen.

Kaspersky Fraud Prevention bietet nicht nur hochentwickelte Technologie und Know-how, sondern auch:

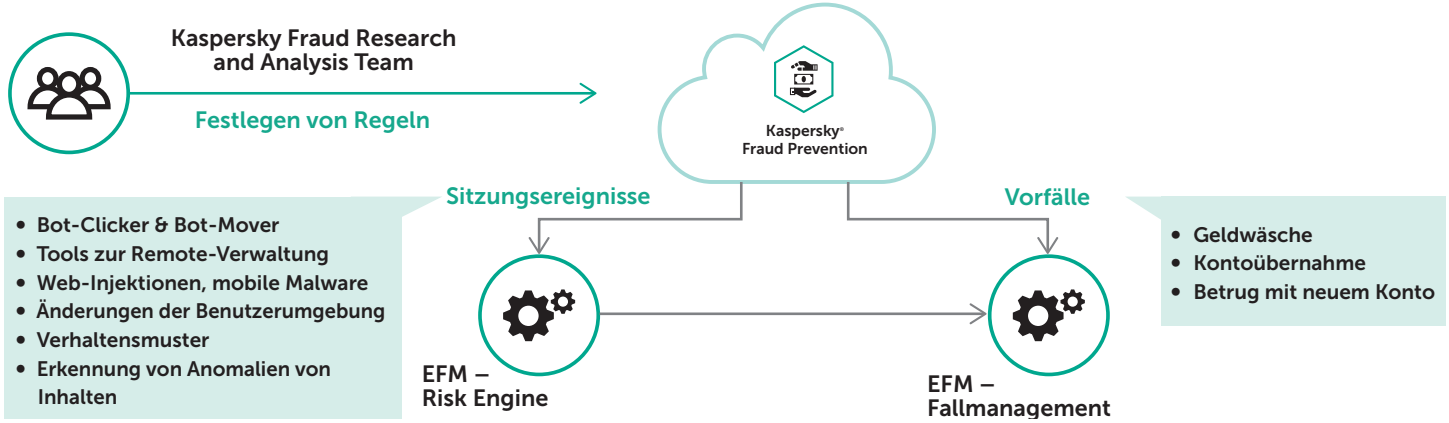
Maintenance Service Agreement – hervorragender Support für Ihren gesamten Sicherheitsbedarf, um Ihr Unternehmen mit erstklassiger Unterstützung durch unsere zertifizierten Techniker vor Ort zu schützen.

Implementation Services – spezielle Implementierungstechniker schaffen Verknüpfungen zwischen unseren Produkten und bereits vorhandenen Sicherheits- und Betrugsbekämpfungslösungen.

Fraud Prevention Consulting – Unternehmensberatung zum Aufbau der richtigen Betrugsbekämpfungsstrategie von einem Expertenteam mit unterschiedlichen Spezialkenntnissen und branchenübergreifendem Know-how.

Die wichtigsten Vorteile von Kaspersky Fraud Prevention:

- Wachstum der Online-Kanäle und der mobilen Kanäle ohne zusätzliche Belastung durch Sicherheitsbedenken und Probleme mit der Benutzerfreundlichkeit
- Kostenkontrolle bei der Betrugsbekämpfung und geringere Verluste durch Betrug
- Echtzeiterkennung von hochentwickelten Betrugsversuchen, noch bevor eine Transaktion erfolgt
- Verbesserung kommerzieller Betrugsüberwachungslösungen durch zusätzliche Daten



IoT-Sicherheit

Das Vertrauen Ihrer Kunden durch Sicherung ihrer Daten rechtfertigen

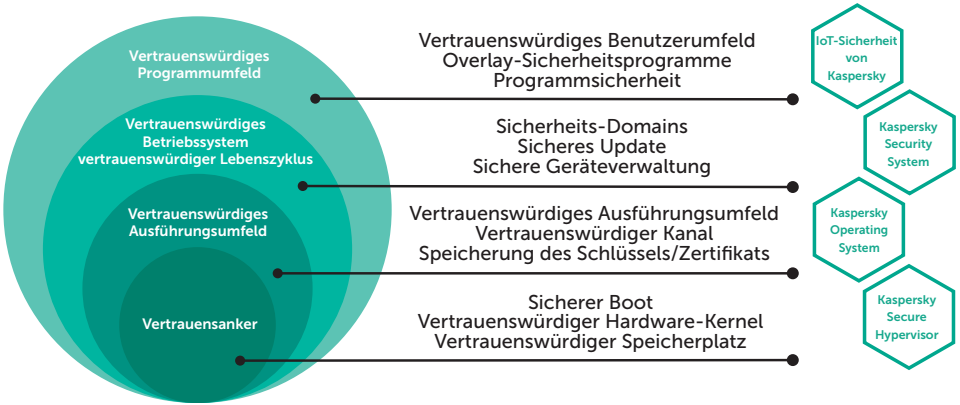
Das Internet der Dinge (Internet of Things, IoT) ist ein neues Paradigma, das die Welt verändert. Es könnte unsere Welt sicherer machen, unsere Gesundheit verbessern, uns Zeit und Geld sparen, Abfälle reduzieren und die Steuerung von Produktionsabläufen, ja, das Leben im Allgemeinen um eine neue Dimension erweitern.

Der Cybersicherheit wird traditionell mit der Sicherheit personenbezogener Daten in Verbindung gebracht. Im Zeitalter des IoT geht es jedoch vielmehr um die Sicherheit der Privatsphäre. Verletzungen der Privatsphäre von Nutzern wie z. B. die Fernüberwachung über intelligente Heimkameras, Multimedia-Geräte oder Babyphone, Eingriffe in die Funktionsfähigkeit von Haushaltsgeräten, unerwartete Abschaltungen und der Ausfall alltäglicher Serviceleistungen – all das ist für den Endbenutzer nicht akzeptabel.

Gleichzeitig bietet das Internet der Dinge Geräteherstellern (einschließlich Hardwarekomponenten und Software), Telekommunikationsdienstleistern und dem Systemintegrationsmarkt enorme Möglichkeiten. Sollten die Endbenutzer das Vertrauen in IoT-Lösungen verlieren, so könnte dies die Umsetzung dieser Möglichkeiten verhindern oder erheblich verlangsamen. Aus diesem Grund hat End-to-End-Sicherheit bei IoT-Lösungen für alle Beteiligten oberste Priorität.

So wie die Dinge stehen, können mit dem IoT verbundene Edge Devices und Telekommunikationsgeräte leicht gegen die Grundsätze der Cybersicherheit verstoßen. Unter Umständen kann die Hardware die Integrität der Firmware nicht kontrollieren, und die Geräte werden manchmal mit vorinstallierten Passwörtern ausgeliefert, einschließlich Administrator-Passwörter. Schwache Einstellungen für die Netzwerksicherheit oder die Verwendung alter und anfälliger Software können auch zu Problemen führen. Wenn dazu noch Prozesse für Software-Updates fehlen, können anfällige Geräte jahrelang ohne Updates betrieben werden, sodass es nur eine Frage der Zeit ist, wann das Gerät erfolgreich angegriffen wird.

Vertrauensgarantien auf Geräteebene



Grundlage für die Gewährleistung der sicheren Funktionsweise von IoT-Geräten ist das Prinzip der Vertrauenskette. Dies schließt Edge Devices und Elemente der Infrastruktur (Gateways) mit ein. Das Prinzip beginnt mit einem Vertrauensanker auf der Hardwareebene.

Die Technologie startet ein Betriebssystem per Trusted Boot, wobei auch die Integrität des OS-Image geprüft wird, bringt Kryptografie zum Einsatz und speichert wichtige Daten mithilfe hardwaregestützter Schutzmechanismen. Trusted Boot ist eine entscheidende Technologie für wichtige IoT-Infrastrukturgeräte wie z. B. Gateways. Hierbei wird das Betriebssystem von zuvor festgelegten Medien aus und erst, nachdem das Gerät bestimmte Integritätsprüfungen erfolgreich bestanden hat, gebootet.

Das nächste wichtige Element der Vertrauenskette ist ein sicheres Betriebssystem, das in der Lage ist, die ordnungsgemäße Ausführung von Software, die nicht als vertrauenswürdig gilt, sicherzustellen. Die jüngsten Entwicklungen in der Computertechnik machen es möglich, auf der Ebene des Betriebssystems eine Umgebung zu implementieren, die das Verhalten von Programmen einschränkt, die nicht als vertrauenswürdig angesehen werden.

Das IoT-Konzept umfasst eine Vielzahl von Geräten, Gadgets, Technologien, Software und Kommunikationsprotokollen. Diese heterogene Umgebung bringt jedoch viele Sicherheitsrisiken mit sich, die jeden Aspekt unseres Lebens mit dem IoT ernsthaft beeinträchtigen können. Kaspersky Lab hat eine Reihe von Produkten entwickelt, mit denen sich die damit verbundenen Risiken minimieren lassen:

- **Embedded Systems Security**
  Mit dieser Lösung zur Sicherheitsoptimierung für Low-End-Systeme mit begrenzter Speicherkapazität können Sie Ihre Embedded Devices und Computer, die Microsoft Windows als Betriebssystem haben, ohne kontinuierliche Wartung oder Internetverbindung absichern und schützen.
- **KasperskyOS**
  Das Betriebssystem KasperskyOS ist darauf ausgelegt, vielfältige und komplexe Embedded Systems durch eine starke Abtrennung und Durchsetzung von Richtlinien vor den Auswirkungen von schädlichem Code, Viren und Hackerangriffen zu schützen. KasperskyOS schafft eine Umgebung, in der eine Sicherheitslücke oder schlechter Code kein großes Problem mehr darstellt. Die Schutzkomponente Kaspersky Security System kontrolliert Interaktionen über das ganze System hinweg, sodass die Ausnutzung von Sicherheitslücken wirkungslos bleibt.
- **Kaspersky Security System**
  Kaspersky Security System ist eine Recheneinheit, die aufgrund von Sicherheitsrichtlinien Entscheidungen trifft, wobei gleichzeitig verschiedene Arten von Sicherheitsrichtlinien zum Einsatz kommen (rollenbasiert und Mandatory Access Control, temporale Logik, Kontrollstruktur, Type Enforcement usw.) und die spezifischen Anforderungen des Kunden berücksichtigt werden können. Je genauer die Richtlinien, desto mehr wächst die Kontrolle und Sicherheit des gesamten Systems.

  Kaspersky Security System kann zusammen mit KasperskyOS (die sicherste Konfiguration) als auch in einer Linux-basierten Lösung (sichere Aktionen in einem unsicheren System) eingesetzt werden.
- **Kaspersky Secure Hypervisor**
  Kaspersky Secure Hypervisor (KSH) läuft auf dem KasperskyOS-Mikrokernel. Mit KSH können potentiell nicht vertrauenswürdige virtuelle Gastbetriebssysteme voneinander getrennt werden, obwohl sie physisch auf der gleichen Hardware-Plattform ausgeführt werden, wobei die gesamte Kommunikation zwischen ihnen kontrolliert werden kann und vertrauenswürdig ist. Ein weiterer Vorteil von KSH besteht in der Möglichkeit, die Hardwarekosten zu senken.
- **Kaspersky Transportation Security Service**
  Integrierte „Sicherheit für Sicherheitssysteme" auf Grundlage von KasperskyOS – ein einziger sicherer Gateway in elektronische Steuergeräte (Electronic Control Units, ECUs) und verschiedene, auf den Bedarf heutiger und zukünftiger vernetzter Fahrzeuge zugeschnittene Security Assessment Services.
- **Secure Communication Unit**
  Bei der Secure Communication Unit (SCU) handelt es sich um eine Steuereinheit für Kommunikationsgateways, die innerhalb des Fahrzeugnetzwerks mit mehreren Subnetzen und/oder Gateway-Steuergeräten dieser Subnetze verbunden ist. Somit ist die SCU der einzige Gateway zur externen Kommunikation, wohingegen interne Geräte innerhalb einer Domäne oder sogar zwischen Domänen kommunizieren können, ohne SCU-Dienste zu nutzen. Die SCU läuft auf KasperskyOS und wird durch das Kaspersky Security System abgesichert. KasperskyOS steuert alle Interaktionen innerhalb der SCU auf der untersten Ebene und setzt die anhand der Sicherheitsrichtlinie getroffenen Entscheidungen des Kaspersky Security System durch. Es sind nur explizit genehmigte Interaktionen möglich.

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. Die Zeit ist gekommen, bewährte Technologien wie Gerätekontrolle und Default Deny zum Schutz an die Front zu schicken.

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.

Es ist an der Zeit, bewährte Technologien wie Gerätekontrolle und Default Deny wo erforderlich mit einem zusätzlichen Virenschutzmodul für kritische Systeme anzuwenden.

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.

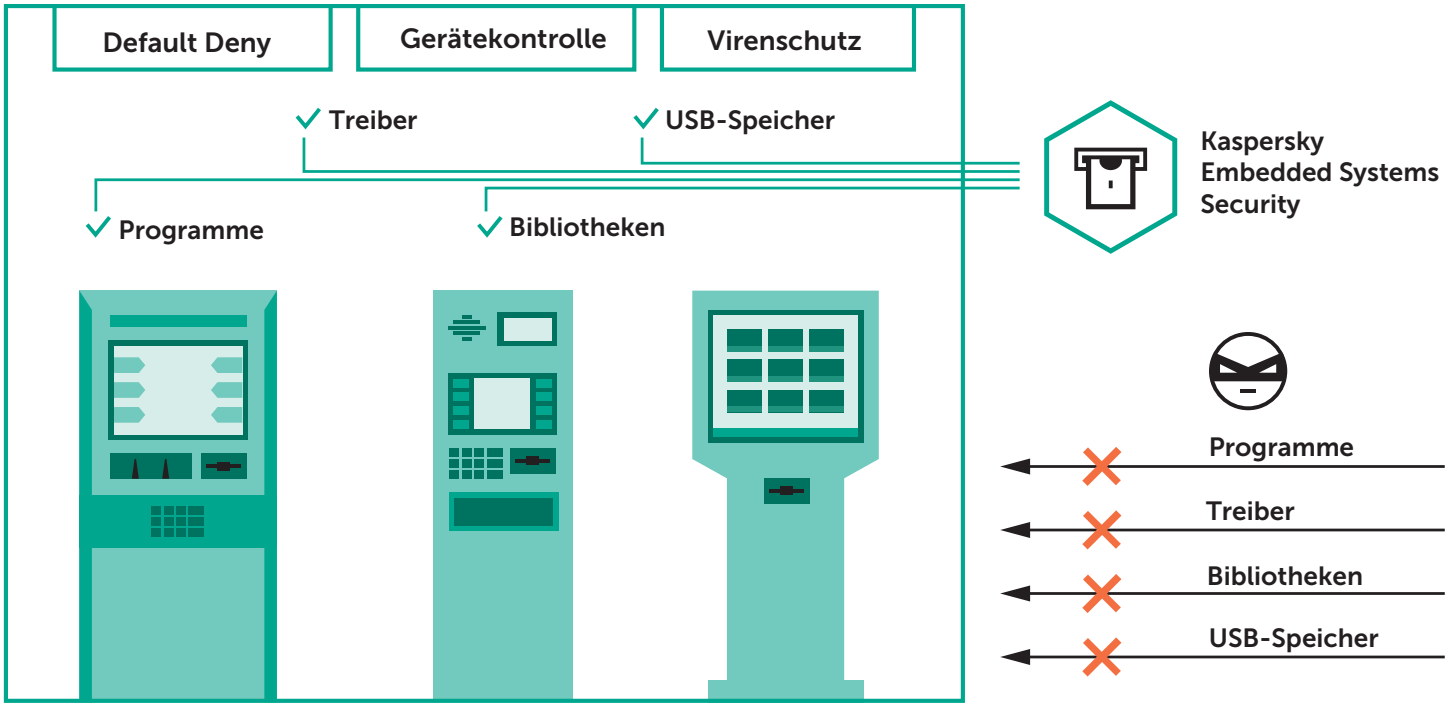
Kaspersky Embedded Systems Security bietet einen „Nur Default Deny"-Betriebsmodus, für den lediglich 256 MB RAM und nur 50 MB Speicherplatz auf der Festplatte notwendig sind – ideal für Systeme, die auf Windows XP basieren und mit Low-End-Hardware betrieben werden.

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.



Premium Support und Professional Services

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

Premium Support

Beim Eintreten eines Sicherheitsvorfalls ist es kritisch, wie lange es dauert, um die Ursache zu identifizieren und zu beseitigen. Das schnelle Erkennen und Lösen eines Problems kann den finanziellen Verlust für Unternehmen verhindern. Unser Premium Support ist so ausgelegt, dass genau dieses Ziel erreicht wird. Zugang zu unseren Experten rund um die Uhr, angemessene und informierte Priorisierung von Problemen mit garantierten Reaktionszeiten und privaten Patches – alles, was nötig ist, um Ihr Problem so bald wie möglich zu beheben.

Kaspersky Lab bietet eine Reihe von Programmen mit Premium Support, bei denen Ihre IT-Sicherheit jederzeit höchste Priorität genießt, damit Ihre Geschäfte auch weiterhin reibungslos ablaufen und bei Vorfällen die ganze Kraft unseres Know-hows darauf ausgerichtet wird, direkt den schnellsten und effektivsten Weg zur Wiederherstellung der vollen Performance zu finden.

Unsere Pläne für den Premium Support umfassen:

- Eigener Technical Account Manager
- Support rund um die Uhr über eine spezielle Telefonleitung
- SLAs für die Vorfallsreaktion
- Unmittelbare Warnhinweise bei neuen Bedrohungen

Professional Services

Cybersicherheit bedeutet eine erhebliche Investition. Setzen Sie sich deshalb mit Experten zusammen, die genau wissen, wie Sie Ihre Investition optimal nutzen, um die individuellen Anforderungen Ihres Unternehmens zu erfüllen.

Unsere Sicherheitsexperten arbeiten gemäß unserer Best Practices und helfen in der gesamten IT-Infrastruktur Ihres Unternehmens beim Deployment, der Konfiguration und der Aktualisierung von Kaspersky-Produkten.

Kaspersky Lab Professional Services stellen sicher, dass Ihre Reaktion auf Veränderungen oder Umstellungen reibungslos verläuft, wirksam ist und keine unnötigen Betriebsunterbrechungen verursacht.

Kaspersky Professional Services umfasst:

- Implementierung und Upgrade
- Konfiguration
- Integritätsprüfung („Health Check")
- Produktschulung

Über Kaspersky Lab

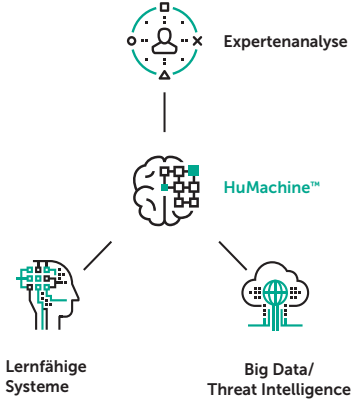
Kaspersky Lab ist ein global agierendes Cybersicherheitsunternehmen, das im Jahr 1997 gegründet wurde. Die tiefgreifende Threat Intelligence sowie Sicherheitsexpertise von Kaspersky Lab ist Basis für Sicherheitslösungen und -Services zum Schutz von Unternehmen, kritischen Infrastrukturen, staatlichen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

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

Für Ihre Notizen



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

#truecybersecurity
#HuMachine

www.kaspersky.de