PRAKTISCHER LEITFADEN

EINE SICHERE IT – IHR VERDIENST

So bringen Sie IT-Sicherheit und Geschäftsziele in Einklang

Erfolgreiches Business geht auf Nummer sicher!
kaspersky.de/business-security
#securebiz

KASPERSKY lab

INHALT

EINE SICHERE IT – IHR VERDIENST

NEUE EFFIZIENZEN VORANTREIBEN

In der schnelllebigen Geschäftswelt von heute haben Unternehmen, die neue Technologien rasch umsetzen, einen deutlichen Vorteil gegenüber ihren Konkurrenten. Durch die neuesten Entwicklungen in der IT und die kontinuierliche Verbesserung von Geschäftsprogrammen kann dafür gesorgt werden, dass Unternehmen jeder Größenordnung Folgendes erreichen können:

- Die Effizienz ihrer alltäglichen Geschäftsprozesse steigern
- Die Service-Levels verbessern
- Die Zeit bis zur Markteinführung verkürzen
- Eine engere Zusammenarbeit mit Lieferanten und Geschäftspartnern unterstützen
- Auf sich verändernde Anforderungen in ihren Zielmärkten reagieren

… und gleichzeitig die Kosten senken.

Dagegen werden Unternehmen, die das Potential neuer, innovativer businesskritischer Prozesse nicht rasch genug nutzen, möglicherweise feststellen, dass ihnen ihre Rivalen in Bezug auf Effizienz voraus sind. Dieser Rückstand könnte sich äußerst negativ auf die Gewinnspanne auswirken.

NEUE TECHNOLOGIEN DÜRFEN KEINE NEUEN RISIKEN MIT SICH BRINGEN

Unternehmen profitieren insbesondere von Technologien, die eine größere Mobilität ermöglichen, z. B. BYOD (Bring Your Own Device)-Initiativen, und von Server- und Desktop-Virtualisierungsprogrammen. Wie alle Veränderungen der Geschäftsprozesse ziehen neue Technologien jedoch auch neue Herausforderungen nach sich – einschließlich Sicherheitsrisiken, die dem Unternehmen potentiell einen großen Schaden zufügen können.

Für den Schutz aller Bestandteile des IT-Netzwerks im Unternehmen stehen fortschrittliche Sicherheitslösungen zur Verfügung. Um wirklich davon zu profitieren, muss sich das Unternehmen aber die notwendige Zeit nehmen, um die passende Lösung für jedes potentielle Sicherheitsrisiko auszuwählen. Überdies muss darauf geachtet werden, dass ausschließlich effiziente Sicherheitsprodukte ausgewählt werden, die einen umfassenden Schutz bieten, ohne die IT-Systeme und -Abteilungen unnötig zu belasten oder gar die Reaktionsfähigkeit des Unternehmens zu beeinträchtigen.

Wenn das Thema Sicherheit nicht bei jedem neuen Technologieprojekt in Ihrem Unternehmen auf der Tagesordnung zu finden ist, besteht die reale Gefahr, dass das Unternehmen später mit dem Verlust wertvoller Daten, dem „Durchsickern“ vertraulicher Kundendaten, der Unterbrechung businesskritischer Prozesse, Problemen bei der Einhaltung von Vorschriften, Geldbußen, Rufschädigung und vielen anderen Problemen zu kämpfen hat.

LERNEN SIE MAX KENNEN – DEN FURCHTLOSEN IT- UND SICHERHEITSSPEZIALISTEN

Als IT-Manager für ein Unternehmen mit 150 Mitarbeitern verwaltet Max in seiner Arbeitszeit jeden Aspekt der IT-Systeme und -Services des Unternehmens – auf physischer, virtueller und mobiler Ebene. Darüber hinaus ist er für die Sicherheit aller Server, Desktops und mobilen Geräte zuständig, inklusive vertraulicher Unternehmensdaten.

Weil er so viele Aufgaben koordinieren und zudem mit einem begrenzten Budget auskommen muss, ist Max immer auf der Suche nach IT-Lösungen, die den Support vereinfachen, alltägliche Aufgaben automatisch abarbeiten und die Kostenkontrolle unterstützen.

Die Vorgesetzten von Max verstehen die täglichen Herausforderungen, vor denen er steht, nicht bis ins Detail. Sie wissen nur, dass alles reibungslos funktionieren muss. Sie sind sich aber durchaus bewusst, dass der anhaltende Erfolg des Unternehmens zunehmend von der IT abhängt. Es ist von zentraler Bedeutung, dass Max neue Technologien und IT-Services einführen kann, die effektivere Geschäftsprozesse ermöglichen. Gleichzeitig muss er seine täglichen Aufgaben erfüllen und sicherstellen, dass die wertvollen Unternehmensdaten geschützt sind.

MAX SAGT

„Wie ich selbst leidvoll erfahren musste, können neue Technologien neue Sicherheitsrisiken mit sich bringen. Deshalb stehen bei mir zu Beginn eines neuen Projekts Sicherheitserwägungen auf der Tagesordnung. Nur so können wir die Risiken bewerten und entscheiden, ob unsere vorhandenen Sicherheitstechnologien ausreichen, sowie, falls nötig, unsere Sicherheitsrichtlinien anpassen."

FÜR DAS UNTERNEHMEN ARBEITEN – NICHT DAGEGEN

Für den anhaltenden Erfolg eines Unternehmens ist die geschäftliche Agilität wichtiger denn je. Heutzutage ändern sich viele der Faktoren, die sich direkt auf den ROI eines Unternehmens auswirken können, noch schneller als vor einigen Jahren. Zu diesen Faktoren zählen:

- Änderungen im Kundenverhalten und bei den Kundenanforderungen
- Änderungen beim Service-Level Ihrer Mitbewerber, die von Kunden gewünscht werden

Hersteller stehen unter Druck, neue Produkte schnell auf den Markt zu bringen, während Einzelhandels- und Dienstleistungsunternehmen permanent nach Möglichkeiten suchen, die Betriebskosten zu reduzieren, um wettbewerbsfähig zu bleiben.

Deshalb ist es unerlässlich, mit den neuen Technologien Schritt zu halten, mit deren Hilfe Ihr Unternehmen die Herausforderungen meistern kann. Die IT spielt zwar eine zentrale Rolle, wenn es darum geht, wichtige Prozesse zu ermöglichen und die Effizienz zu steigern, dennoch sollten Sie im Blick behalten, dass das IT-Netzwerk im Unternehmen dem Geschäft dienen soll und nicht umgekehrt. Jede Technologie, die sich negativ auf Ihre alltäglichen Geschäftsabläufe auswirkt oder die Einführung neuer, effizienter Prozesse verzögert, unterstützt Ihr Unternehmen nicht so effektiv, wie es sein sollte.

Dasselbe gilt für die IT-Sicherheit. Natürlich müssen Sie Ihre Systeme und die darin abgelegten vertraulichen Daten unbedingt schützen. Aber komplexe, schlecht integrierte Sicherheitsprodukte sind für moderne, agile, effiziente Unternehmen einfach nicht geeignet.

Die IT-Sicherheit soll sich um den Schutz kümmern, ohne die

geschäftliche Agilität zu beeinträchtigen und ohne:

- wichtige Prozesse zu verlangsamen
- die geschäftliche Agilität zu beschränken, um neue Technologien einzuführen, die neue Prozesse ermöglichen
- bei Wachstum nicht angemessen skalieren zu können

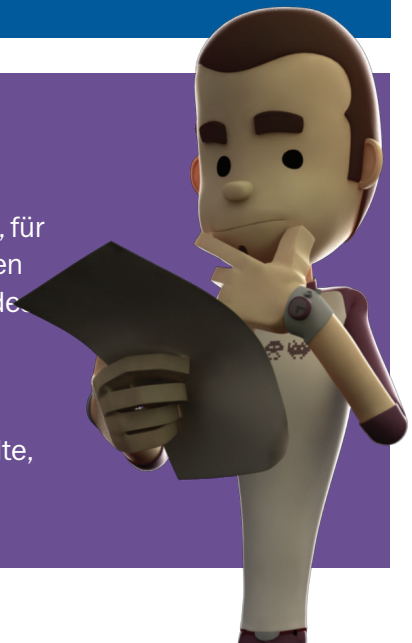
„Die starke Zunahme bei Sicherheitsprodukten für ein einziges Gerät ist nur noch schwer zu bewältigen und zu verwalten und verursacht hohe Kosten. Viele Unternehmen haben auf diesen Umstand reagiert, indem sie ein einziges Produkt anschaffen, das unterschiedliche Sicherheitsanforderungen handhaben kann. Sicherheitspakete/-Plattformen lassen sich leichter installieren als mehrere unterschiedliche Programme, und sie sind leichter zu verwalten, wenn sie über eine Konsole bedient werden können."

IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS
JANUAR 2013, IDC NR. IS01V, BAND: 1

MAX SAGT

„Früher habe ich viel Zeit investiert, um mit unflexiblen Sicherheitsprodukten zu arbeiten, für die wir unsere Geschäftsprozesse so anpassen mussten, dass sie mit den Beschränkungen des Produkts zurechtkamen.

Mit der Zeit kam ich zu dem Schluss, dass ein gutes Sicherheitsprodukt in der Lage sein sollte, unsere zentralen Geschäftsprozesse mit Schutzschichten zu umhüllen."



VERÄNDERUNGEN, DIE GÄNZLICH IHRER KONTROLLE ENTZOGEN SIND

Die IT kann bei den Veränderungen, welche die Effizienz und Gewinnspannen verbessern, eine positive Rolle spielen. Dennoch verändert sich die Geschäftsumgebung auf weniger wünschenswerte Weise. Menge und Raffinesse von Malware und gezielten Angriffen nehmen zu. Cyberkriminelle sind zunehmend besser organisiert und handeln professioneller, wenn sie versuchen, Geld zu stehlen, Zugriff auf wertvolle Informationen zu erhalten oder Ausfälle zu verursachen.

Die direkten Kosten für einen Angriff, einschließlich der von den Behörden verhängten Bußgelder, können erheblich sein. Die indirekten Kosten können jedoch noch höher ausfallen, für u. a. den Imageschaden, Schadensersatzansprüche von Kunden und Lieferanten, auf deren vertrauliche Daten unbefugt zugegriffen wurde und Verlust von geistigem Eigentum, das dem Unternehmen einen Wettbewerbsvorteil verschafft hat.

WICHTIGE ÜBERLEGUNGEN BEI DER AUSWAHL EINER EFFEKTIVEN SICHERHEITSLÖSUNG

ANTI-MALWARE-PRODUKTE ALS UNVERZICHTBARE ERSTE SCHUTZMAUER IN IHREM VERTEIDIGUNGSSYSTEM

Anti-Malware-Software ist auch weiterhin ein unverzichtbarer Bestandteil des IT-Verteidigungssystems eines Unternehmens. Gute Anti-Malware-Lösungen verlassen sich jedoch nicht allein auf den signaturbasierten Schutz.
Sie umfassen auch:

- Heuristische Analyse
- Cloud-basierte Echtzeit-Bereitstellung von Daten zu neuen und aufkommenden Bedrohungen

Für den signaturbasierten Schutz analysieren Sicherheitsanbieter jedes neue Malware-Programm, das sie entdecken. Sie stellen Updates für die Viren-Datenbanken der Endpoint-Geräte bereit. In der Zwischenzeit ist das IT-Netzwerk Ihres Unternehmens unter Umständen jedoch sehr anfällig. Selbst wenn zwischen der Veröffentlichung des neuen Malware-Programms und der Verfügbarkeit des Signatur-Updates nur wenige Stunden liegen, sind Ihre Systeme immer noch anfällig, es sei denn, Ihre Sicherheitssoftware umfasst weitere Schutztechnologien.

Die heuristische Analyse ermöglicht eine aktive Reaktion auf das Aufkommen neuer Malware. Auch wenn noch keine Malware-Signatur geladen werden konnte, kann die heuristische Analyse viele zuvor unbekannten Malware-Elemente oder neue Varianten einer älteren Malware-Bedrohung erkennen.

Das dritte unverzichtbare Element eines modernen Malware-Schutzes wird über die Cloud bereitgestellt. Durch den Einsatz Cloud-basierter Services, die Daten über neue Malware und andere Bedrohungen bereitstellen, können Sicherheitsanbieter die Fähigkeit des IT-Netzwerks im Unternehmen erheblich verbessern, die neuesten Malware-Angriffe abzuwehren.

SCHÜTZEN ANTI-MALWARE-PRODUKTE JEDOCH AUSREICHEND VOR NEUEN, KOMPLEXEN BEDROHUNGEN?

Anti-Malware-Produkte sind für Ihren Schutz zwar äußerst wichtig und die Lösungen, die signaturbasierte, heuristische und Cloud-basierte Technologien kombinieren, bieten heutzutage einen besseren Schutz als ihre Vorgänger. Dennoch ist es wirklich nicht klug, den Schutz Ihres Unternehmens und Ihres Rufs nur Anti-Malware-Produkten zu überlassen.

Leider genügen Anti-Malware-Produkte allein nicht, um die Sicherheit Ihrer Systeme und Daten zu gewährleisten, denn die Cyberkriminellen benutzen ebenfalls ausgefeilte Techniken, um die Sicherheit Ihres Unternehmens zu gefährden.

Um die heutigen Bedrohungen abzuwehren, müssen Unternehmen Sicherheitsprodukte einsetzen, die ein mehrschichtiges System an Sicherheitstechnologien bieten, einschließlich:

- Malware-Schutz
- Programmkontrolle mit dynamischen Whitelists
- Gerätekontrolle
- Web-Kontrolle
- Vulnerability Scanning
- Patch Management
- Datenverschlüsselung

… und dazu spezielle Sicherheitstechnologien, um mobile Geräte, virtuelle Umgebungen und mehr zu schützen.

„Traditionelle Endpoint-Sicherheit ist ein Synonym für Anti-Malware-Produkt. Es ist kein Geheimnis, dass sich signaturbasierte Anti-Malware-Technologien bei der heutigen modernen Malware nicht sonderlich bewährt haben. Deshalb geht die Tendenz bei der Unternehmens-IT weg von punktuell eingesetzten Anti-Malware-Technologien und hin zu einer mehrschichtigen Abwehr mit einem Maßnahmenportfolio, das nicht nur Anti-Malware-Produkte, sondern auch Host-basierte Firewall/IPS, Programmkontrolle, Geräte- und Medienkontrolle und Endpoint-Verschlüsselung umfasst.“

THE FORRESTER WAVE™: ENDPOINT SECURITY, Q1 2013 ENDPOINT SECURITY SUITES TAKE CENTER STAGE IN THE ENTERPRISE FORRESTER RESEARCH, INC 4. JANUAR 2013

MAX SAGT

„Sicherheitslücken schädigen nicht nur das Unternehmen. Sie können auch Bußgelder für die Geschäftsführung nach sich ziehen.

In vielen Regionen können Regulierungsbehörden eine Reihe von Strafen gegen Geschäftsführer verhängen, welche die Sicherheitsmaßnahmen vernachlässigt haben – u. a. Bußgelder und/oder Gefängnisstrafen.“

KONTROLLFUNKTIONEN: SCHUTZ FÜR IHR UNTERNEHMEN VOR DEN SICHERHEITSFEHLERN IHRER MITARBEITER

PROGRAMMKONTROLLE UND DYNAMISCHE WHITELISTS

Es gibt viele Möglichkeiten, wie nicht autorisierte Programme in Ihr Firmennetzwerk gelangen können. Dabei können einige dieser unerwünschten Programme ein Sicherheitsproblem darstellen:

- Benutzer laden Programme vielleicht absichtlich aus dem Internet herunter.
- Benutzer laden Programme möglicherweise von Wechseldatenträgern auf ihre Desktops.

Wenn Sie keine Gelegenheit hatten, diese Programme zu prüfen und zu genehmigen, wissen Sie natürlich nicht, ob diese frei von Malware sind. Zudem können Sie nicht sicher sein, ob das Vorhandensein dieser Programme Lizenzprobleme nach sich zieht.

Sicherheitsanbieter haben Funktionen für die Programmkontrolle entwickelt, mit denen Sie einfach kontrollieren können, welche Programme auf Ihrem Netzwerk gestartet werden können. Mit Tools für die Programmkontrolle können Sie Folgendes verwalten:

- welche Programme ausgeführt werden dürfen (Whitelist)
- welche Programme blockiert werden (Blacklist)
- wie sich autorisierte Programme beim Ausführen verhalten dürfen (Steuerung der Programmberechtigungen)

Bei den meisten Tools zur Programmkontrolle können Sie zwischen einer „Default Allow“- oder einer „Default Deny“-Richtlinie wählen:

- **Default Allow**: Wählen Sie diese Option, wenn Sie erlauben möchten, dass jedes Programm gestartet werden darf, sofern es nicht auf Ihrer Blacklist mit Programmen steht, die blockiert werden.
- **Default Deny**: Wählen Sie diese Option, um den Start aller Programme zu blockieren, sofern diese nicht auf Ihrer Whitelist der sicheren Programme stehen und ausgeführt werden dürfen.

Mit der Option „Default Deny“ können Sie besonders gut verhindern, dass Malware gestartet wird und dass Benutzer Programme ausführen, die nicht für Ihre Arbeit relevant sind. Die Richtlinie „Default Deny“ lässt sich jedoch viel einfacher einsetzen, wenn Ihr Sicherheitsanbieter Sie dabei unterstützt, die Sicherheit häufig verwendeter Programme zu bewerten – durch die Analyse der Programme in den eigenen Whitelisting-Labors des Anbieters.

„Für den Schutz vor äußerst gezielten und neuen Angriffen auf kleine Zielgruppen ist ein aktiver Ansatz erforderlich, der auf zuverlässigen Betriebsführungsprozessen basiert, wie Vulnerability Scanning, Patch Management und Programmkontrollfunktionen. Insbesondere die Programmkontrolle, bei der nur bekannte gutartige Programme ausgeführt werden dürfen, hat sich in anspruchsvollen Sicherheitsumgebungen als effektiv erwiesen und ist ganz besonders effektiv, wenn sie mit Unterstützung für vertrauenswürdige Änderungen kombiniert und mit Cloud-basierten Diensten zur Dateireputation ergänzt wird.“

MAGIC QUADRANT FOR ENDPOINT PROTECTION PLATFORMS
8. JANUAR 2014
GARTNER, INC.

GERÄTEKONTROLLE

Mithilfe von Wechseldatenträgern – u. a. USB-Flashlaufwerke, SD-Karten und externe Festplattenspeicher – können vertrauliche Daten gestohlen oder Malware in das Unternehmensnetzwerk geschleust werden. Ihre Verwendung muss daher streng kontrolliert werden.

Über Funktionen zur Gerätekontrolle können Sie leicht ermitteln, welche Geräte in Ihrem Firmennetzwerk verwendet werden dürfen und mit welchen nicht autorisierten Geräten Ihre Mitarbeiter oder Vertragspartner eine Verbindung zu Ihren Systemen herstellen. Überdies können Sie mit der Gerätekontrolle Folgendes tun:

- bestimmte Gerätetypen blockieren, z. B. Wechseldatenträger
- alle Geräte blockieren, die einen bestimmten BUS-Typ verwenden, z. B. alle USB-Geräte
- einzelne Geräte blockieren, entsprechend ihrer eindeutigen Kennungen
- Verschlüsselung erzwingen, wenn Sie Dateien auf einen Wechseldatenträger kopieren
- Gerätebeschränkungen für bestimmte Tageszeiten einrichten

USB-GERÄTE ALS WERKZEUG FÜR AUSGEKLÜGELTE ANGRIFFE

Einer der bekanntesten Angriffe auf einen Betreiber wichtiger Infrastrukturen soll mithilfe eines einfachen USB-Flashlaufwerks gestartet worden sein. Stuxnet, ein Cybersabotage-Wurm, wurde wahrscheinlich von einem USB-Gerät in die Systeme einer Kernkraftanlage geladen.

WEB-KONTROLLE

Wenn Sie Ihren Mitarbeitern unkontrollierten Zugriff auf das Internet gewähren, kann dies Folgen für die Sicherheit und Produktivität Ihres Unternehmens haben.

Selbst wenn Ihre Mitarbeiter im Rahmen ihrer alltäglichen Aufgaben auf legitime Webseiten zugreifen – können Sie wirklich sicher sein, dass diese Webseiten sicher sind? Es gibt viele Fälle, bei denen Cyberkriminelle echte Webseiten hacken, sodass arglose Besucher Opfer von Drive-by-Downloads werden: Dabei wird Malware automatisch auf das Gerät des Benutzers heruntergeladen. Das Malware-Programm erhält dadurch die Gelegenheit, sich im Firmen-IT-Netzwerk zu verbreiten.

Doch nicht nur die im Internet lauernden Sicherheitsrisiken sind ein Problem. Das Surfen im Internet kann auch extrem ablenken und sich auf die Produktivität Ihrer Mitarbeiter auswirken.

Einige Sicherheitslösungen umfassen flexible Web-Kontrollfunktionen, mit denen Sie Folgendes tun können:

- den Zugriff auf bestimmte Webseiten oder bestimmte Kategorien von Webseiten vollständig blockieren, z. B. Glücksspielseiten oder Seiten mit nicht jugendfreien Inhalten
- den Zugriff auf Webseiten blockieren, die illegale oder nicht autorisierte Downloads aktivieren, einschließlich nicht lizenzierter Programme
- den Zugriff auf Soziale Netzwerke beschränken, z. B. auf die Mittagszeit
- die neuesten Informationen nutzen, die in Echtzeit aus der Cloud bereitgestellt werden, um Benutzer vor infizierten oder gefährlichen Webseiten zu warnen und Drive-by-Infektionen zu vermeiden

VERHINDERN DER AUSNUTZUNG VON SCHWACHSTELLEN

Am häufigsten greifen Cyberkriminelle über Schwachstellen im Betriebssystem oder in Programmen auf Computer und Mobilgeräte zu. Diese Schwachstellen entstehen in der Regel aufgrund von Codefehlern im Programm oder im Betriebssystem. Sobald die Hacker-Community einen neuen Fehler ermittelt hat und einen Weg findet, diesen auszunutzen, verbreitet sich die Nachricht über die Schwachstelle schnell, und die Anzahl neuer Angriffe nimmt zu.

Für die meisten modernen Unternehmen, die mit einer Vielzahl von Softwareprogrammen und möglicherweise auch unterschiedlichen Versionen eines Betriebssystems arbeiten, kann es sich als schwierig erweisen, den Überblick über die neuesten Schwachstellen zu behalten und festzustellen, ob die Software-Entwickler Updates oder Patches für diese Schwachstellen bereitgestellt haben. Zudem ist es nicht einfach, die Bereitstellung der notwendigen Patches zu priorisieren und diese anschließend zu implementieren.

VULNERABILITY SCANNING

Vulnerability Scanning, die Schwachstellenanalyse, wird zwar normalerweise mit dem Systems Management und nicht mit Sicherheit in Zusammenhang gebracht, dennoch ist sie von zentraler Bedeutung für den Schutz des IT-Netzwerks Ihres Unternehmens vor Angriffen. Es ist daher äußerst wichtig, eine Sicherheits- oder Systems-Management-Lösung zu finden, die Ihr Netzwerk automatisch auf Schwachstellen untersucht.

PATCH MANAGEMENT

Die Schwachstellen des Betriebssystems und der Programme zu ermitteln, die im IT-Netzwerk Ihres Unternehmens vorhanden sind, kann dabei natürlich nur der erste Schritt sein. Sie müssen die neuesten Software-Patches und Updates anschließend priorisieren und implementieren. Dies kann zwar wieder als Aufgabe des Systems Managements angesehen werden, aber Sie können dadurch die Sicherheit des Unternehmens erheblich stärken. Zudem können Sie diese Aufgabe mithilfe einer guten Sicherheits- oder Systems-Management-Software automatisieren.

MAX SAGT

„Da die Märkte für IT-Sicherheits- und -Managementsoftware gereift sind, werden immer mehr vollständig integrierte Sicherheits- und Systems-Management-Lösungen angeboten. Die Zeiten, in denen man punktuelle Lösungen von mehreren Anbietern anschaffen und dann dafür sorgen musste, dass diese irgendwie zusammen funktionieren, sind zum Glück endlich vorbei!

Es lohnt sich aber zu überprüfen, wie zutreffend die Behauptungen der Anbieter in Bezug auf die Integrationsfähigkeit sind. Wenn ein Anbieter eine neue Funktion hinzugefügt hat, indem er beispielsweise einfach die Lösungen eines anderen Anbieters gekauft hat, kann dies Probleme nach sich ziehen. Passen Sie daher auf, dass Sie nicht auf den schönen Schein hereinfallen und die angebliche Integrationsfähigkeit eine ganze Fülle von operativen Problemen nach sich zieht.“

DATENVERSCHLÜSSELUNG

Wenn ein Mitarbeiter einen Laptop, ein USB-Flashlaufwerk oder eine externe Festplatte verliert, können vertrauliche Geschäftsdaten in die falschen Hände geraten. Das könnte Sie wiederum teuer zu stehen kommen. Wenn die Daten jedoch verschlüsselt wurden, führt der Verlust des Geräts nicht zwangsläufig zum Verlust vertraulicher Daten in lesbarem Format. Nach der Verschlüsselung können die Daten nur dann in ein lesbares Format dekodiert werden, wenn der erforderliche Verschlüsselungsalgorithmus verwendet wird.

Obwohl die Datenverschlüsselung schon seit vielen Jahren verfügbar ist, wird sie nicht von allen Unternehmen genutzt. Dieser Umstand ist zum Teil der mangelnden Benutzerfreundlichkeit einiger kommerziell erhältlicher Verschlüsselungsprodukte geschuldet. Bei vielen haben sich Konfiguration und Verwaltung als zu umständlich erwiesen, oder die Produkte haben sich negativ auf die IT-Leistung ausgewirkt.

In der Vergangenheit hat dies viele Unternehmen dazu verleitet, den Einsatz von Verschlüsselung – zugunsten von Performance und Produktivität – ganz aufzugeben. Sicherheitsanbieter haben jedoch auf die Nachfrage nach effizienteren Lösungen reagiert und benutzerfreundliche Verschlüsselungsprodukte auf den Markt gebracht.

NOCH MEHR RISIKEN DURCH MOBILITÄT

Durch mobile Geräte wurden ganz neue Möglichkeiten geschaffen, wie Unternehmen und externe Mitarbeiter interagieren und ihren Arbeitstag optimal nutzen können.

Mit Smartphones kann man viel mehr erledigen als nur Telefonate. Da sie leistungsstarke Computer sind, auf denen viele vertrauliche Unternehmensdaten gespeichert werden – inkl. Zugriffscodes und Kennwörter für Ihr Unternehmensnetzwerk – müssen Sie diese Geräte genauso schützen wie Ihre Desktops und Server.

Die Mobilität von Smartphones, Tablets und Laptops zieht auch noch weitere Sicherheitsrisiken nach sich. Alle diese Geräte befinden sich außerhalb Ihrer traditionellen Sicherheitszone. Sie können leicht verloren gehen oder gestohlen werden, was wiederum dazu führen kann, dass unbefugte Benutzer Zugriff auf Ihr Unternehmensnetzwerk erhalten.

BYOD-KOMPLIKATIONEN ELIMINIEREN

Initiativen für den Einsatz privater Geräte innerhalb des Unternehmens (Bring Your Own Device, BYOD) bieten viele Vorteile für Unternehmen und Mitarbeiter. Es können jedoch Risiken dadurch entstehen, dass auf den Geräten der Mitarbeiter vertrauliche Geschäftsdaten und persönliche Daten der Benutzer gespeichert werden.

Darüber hinaus kann sich die Verwaltung der unterschiedlichen Geräte, die auf Ihre Unternehmenssysteme zugreifen dürfen, als besonders schwierig erweisen, insbesondere, wenn die Mitarbeiter fast alle Arten von mobilen Geräten verwenden dürfen. Zudem wird es schwierig sicherzustellen, dass auf allen Geräten eine effektive Sicherheitssoftware installiert ist.

Deshalb ist es unverzichtbar, eine Lösung für mobile Sicherheit zu wählen, die eine Vielfalt von Funktionen für Mobile Device Management (MDM) umfasst.

SCHWACHSTELLEN VIRTUALISIERTER UMGEBUNGEN

Mit virtualisierten Server- und Desktopumgebungen können Unternehmen die Anschaffungskosten für Hardware unter Kontrolle halten und die Wartungs-, Energie- und Lizenzkosten reduzieren. Weil virtuelle Geräte schnell bereitgestellt werden können, kann die Virtualisierung zudem die geschäftliche Agilität unterstützen, indem neue IT-Services ohne unnötige Verzögerungen für Unternehmen bereitgestellt werden können.

Entgegen dem gängigen Mythos, dass virtualisierte Maschinen sicherer seien als physische Server und Desktops, müssen alle virtualisierten Maschinen geschützt werden, genau wie physische Hardware. Sicherheitstechnologien für den Schutz virtualisierter Umgebungen können sich jedoch von den Sicherheitsprodukten unterscheiden, die für den Schutz einer physischen IT-Infrastruktur genutzt werden.

Wenn eine traditionelle, agentenbasierte Sicherheitslösung auf allen virtualisierten Maschinen ausgeführt wird, werden die Systemressourcen deutlich weniger geschont, d. h. bei Ihrem Virtualisierungsprojekt wird ein deutlich geringerer ROI erzielt. Es ist stattdessen besser, eine Sicherheitslösung zu wählen, die für virtualisierte Umgebungen optimiert wurde. Dadurch entfällt die Notwendigkeit, identische Viren-Datenbanken und Sicherheitsagenten auf jeder virtualisierten Maschine auszuführen.

ERFAHREN SIE MEHR …

… über die Herausforderungen beim Schutz virtualisierter Umgebungen. Lesen Sie den neuesten Bericht von Kaspersky Lab:

Virtualization Security – ein praktischer Leitfaden
Mit Tipps für den Schutz Ihrer Systeme und vertraulichen Unternehmensdaten

SZENARIO EINER ENG MIT DEM SYSTEMS MANAGEMENT INTEGRIERTEN SICHERHEIT

Gute Funktionen für das Vulnerability Scanning und das Patch Management können sich positiv auf die Gesamtsicherheit Ihrer Systeme auswirken. Es gibt also überzeugende Argumente dafür, eine Sicherheitslösung zu wählen, die diese und weitere Systems-Management-Funktionen umfasst.

Viele Unternehmen führen separate Sicherheits- und Systems-Management-Softwarepakete aus – von verschiedenen Anbietern. Dies kann jedoch dazu führen, dass Sicherheit und Systems Management komplexer zu konfigurieren und zu kontrollieren sind und:

- die Belastung der IT-Verwaltung erhöht wird
- Lücken im Unternehmensschutz verursacht werden

Im Gegensatz dazu kann eine Lösung, die Sicherheits- und Systems-Management-Funktionen in einem Produkt von einem einzigen Anbieter kombiniert, beide Aufgaben vereinfachen.

Einige kombinierte Sicherheits- und Systems-Management-Lösungen verfügen auch über eine zentrale Verwaltungskonsole für alle Aufgaben. IT-Administratoren können davon erheblich profitieren:

- sie müssen nur eine Gruppe von Funktionen lernen
- sie müssen nicht zwischen verschiedenen Konsolen für Sicherheit und Systems Management wechseln
- es können einzelne Richtlinien implementiert werden, die sowohl Probleme der Sicherheit als auch des Systems Management betreffen

MAX SAGT

„Auf den ersten Blick erscheint die Benutzung von zwei oder drei Verwaltungskonsolen, um einzelne Sicherheits- und Management-Technologien verschiedener Anbieter zu verwalten, eine einfache Aufgabe für einen professionellen IT-Administrator.

In der Praxis ist dies jedoch außerordentlich zeitaufwändig und fehleranfällig, besonders wenn man unter dem Druck steht, schnell auf ein Sicherheitsproblem zu reagieren.“

SO KANN IHNEN KASPERSKY LAB HELFEN: INTEGRIERTE SICHERHEITS- UND SYSTEMS-MANAGEMENT-FUNKTIONEN

Neben seiner preisgekrönten Anti-Malware-Lösung und flexiblen Steuerungstechnologien, Datenverschlüsselung, mobiler Sicherheit und Sicherheit bei der Virtualisierung bietet Kaspersky Lab integrierte Systems-Management- und MDM (Mobile Device Management)-Technologien. Sie können also Ihre IT-Sicherheit und -Infrastruktur mit einem einzigen Produkt von einer einzigen Verwaltungskonsole aus verwalten.

„Die neueste Plattform Kaspersky Endpoint Security for Business (KESB) spiegelt die Fähigkeit des Unternehmens wider, problembasierte Angebote zu entwickeln, mit denen in dieser Kategorie Ressourcen-, Management- und Kostenstrukturen vereinfacht werden. IDC sieht in Kaspersky Lab ein führendes Unternehmen in der IDC MarketScape der westeuropäischen Endpoint-Sicherheitssoftware."

IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS
JANUAR 2013, IDC NR. IS01V, BAND: 1

Kaspersky Lab wird als ein führendes Unternehmen im Bereich des Gartner Magic Quadrant for Endpoint Protection Platforms anerkannt.

MAGIC QUADRANT FOR ENDPOINT PROTECTION PLATFORMS
8. JANUAR 2014
GARTNER, INC.

MODERNER MALWARE-SCHUTZ

Die neuesten Anti-Malware-Technologien von Kaspersky Lab bieten eine leistungsstarke Kombination aus:

- signaturbasiertem Schutz
- proaktiven Technologien
- Cloud-basierten Informationen zum Schutz vor neuer Malware

… für Mac-, Linux- und Windows-Plattformen sowie eine breite Palette an mobilen Geräten, einschließlich Android, iOS, Windows Phone, Windows Mobile, BlackBerry und Symbian.

Da die Urgent Detection System-Datenbank von Kaspersky Lab kontinuierlich mit Informationen über neu entdeckte Malware aktualisiert wird, können die fortschrittlichen Anti-Malware-Technologien von Kaspersky Lab Unternehmen auch vor den neuesten Bedrohungen und Angriffen schützen – sogar vor der Herausgabe der neuen Malware-Signatur.

Daneben überwacht der Aktivitätsmonitor von Kaspersky Lab das Verhalten von Programmen, die auf Ihren Endpoints ausgeführt werden. Wenn der Aktivitätsmonitor verdächtiges Verhalten erkennt, wird das Programm gesperrt, und schädliche Änderungen werden automatisch zurückgesetzt.

Kaspersky Lab entwickelt auch weiterhin Innovationen, u. a. neue Anti-Malware-Technologien, einschließlich dem automatischen Exploit-Schutz (AEP), der Systeme überwacht, um Verhaltensweisen zu ermitteln, die üblicherweise auf Malware schließen lassen, die Schwachstellen im Betriebssystem oder in Programmen auszunutzen versucht. AEP blockiert Exploits effektiv, um Systeme vor Zero-Day-Bedrohungen zu schützen.

FLEXIBLE KONTROLLTOOLS

PROGRAMMKONTROLLE

Die Tools zur Programmkontrolle von Kaspersky Lab ermöglichen eine fein abgestufte Kontrolle darüber, wie Programme in Ihrem Unternehmensnetzwerk ausgeführt werden. Mit ihnen können Sie einfach eine „Default Deny“- oder „Default Allow“-Richtlinie festlegen:

- Mit „Default Deny“ können Sie alle Programme, die nicht auf Ihrer Whitelist stehen, blockieren.
- Bei „Default Allow“ werden nur die Programme auf der Blacklist blockiert, alle anderen Programme dürfen ausgeführt werden.

DYNAMISCHE WHITELISTS

Kaspersky Lab ist der einzige Sicherheitsanbieter mit eigenem Whitelisting Lab, in dem die gängigsten Programme bewertet und auf Sicherheitsrisiken überprüft werden. Updates für die dynamische Programm-Whitelist von Kaspersky Lab werden automatisch aus dem Cloud-basierten Kaspersky Security Network heruntergeladen, um die Umsetzung einer „Default Deny“-Richtlinie zu erleichtern, indem die neuesten Informationen zu Programmen genutzt werden.

Einige Anbieter aktualisieren Ihre Programm-Whitelists nur unregelmäßig. Das dynamische Whitelisting von Kaspersky Lab bietet dagegen einen herausragenden Schutz.

GERÄTEKONTROLLE

Mit den Funktionen zur Gerätekontrolle von Kaspersky Lab können Sie die Verwendung von Wechseldatenträgern kontrollieren. Auf diese Weise können Sie das Unternehmen vor Sicherheitsrisiken schützen, die durch nicht genehmigte Geräte verursacht werden. Sie können einfach:

- Zugriffsberechtigungen für bestimmte Gerätetypen, einen bestimmten Gerätebus oder ein einzelnes Gerät festlegen
- Zeiträume festlegen, für die Ihre Gerätekontrollrichtlinie gilt, um beispielsweise den Zugriff von Geräten auf Ihr Unternehmensnetzwerk außerhalb der normalen Bürozeiten zu unterbinden

WEB-KONTROLLE

Mit Tools zur Web-Kontrolle lässt sich die Webbrowser-Nutzung getrennt für jeden einzelnen Mitarbeiter leichter überwachen und filtern. Dank Kaspersky Lab können Sie den Benutzerzugriff auf bestimmte Webseiten oder Kategorien von Webseiten einfach und schnell erlauben, verbieten, beschränken oder überprüfen – u. a. Browser-Games, Glücksspiel-Seiten oder Soziale Netzwerke.

Kaspersky Lab bewertet darüber hinaus die Reputation von Webseiten und gibt Warnungen aus – in Echtzeit, aus der Cloud –, damit gefährliche Webseiten automatisch gemieden und Drive-by-Infektionen verhindert werden können.

„Aufgrund der hervorragenden Stärke der Sicherheitsmechanismen und des attraktiven Preises gehen wir davon aus, dass Kaspersky Lab bei vielen Unternehmen, welche die Anschaffung eines Endpoint-Sicherheitsprodukts in Betracht ziehen, in die engere Wahl kommt.“

THE FORRESTER WAVE™: ENDPOINT SECURITY, Q1 2013
ENDPOINT SECURITY SUITES TAKE CENTER STAGE IN THE ENTERPRISE
FORRESTER RESEARCH, INC
4. JANUAR 2013

VULNERABILITY SCANNING UND PATCH MANAGEMENT

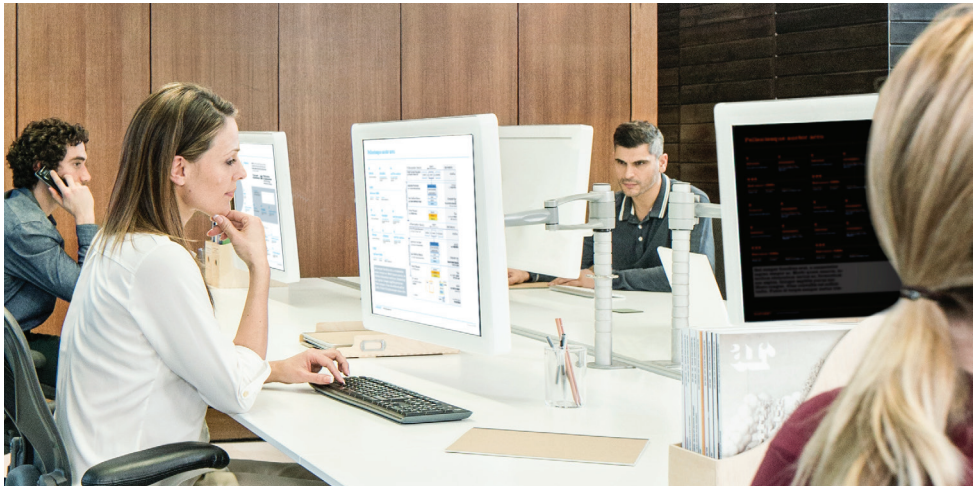
Kaspersky Systems Management umfasst das automatische Vulnerability Scanning sowie eine Patch-Management-Funktion, damit Sie die Stabilität und Sicherheit Ihres Unternehmensnetzwerkes erhalten können.

VULNERABILITY SCANNING

Mit den Technologien von Kaspersky Lab werden Ihre Endpoints gescannt, um Sicherheitsschwachstellen zu finden, die durch ungepatchte Betriebssysteme und Programme entstehen. Neben der Schwachstellen-Datenbank von Kaspersky Lab nutzt der Scanner auch noch die Datenbanken von Secunia und Microsoft.

AUTOMATISCHES PATCH MANAGEMENT

Alle während eines Scans festgestellten Schwachstellen erhalten einen Farbcode, um Ihnen die Priorisierung bei der Patch-Bereitstellung zu erleichtern. Mithilfe der Technologien von Kaspersky Lab können dringende Patches automatisch über Ihr Netzwerk bereitgestellt werden, und Sie können weniger dringende Software-Updates für Termine außerhalb der Bürozeiten planen.



BENUTZERFREUNDLICHE DATEN-VERSCHLÜSSELUNG

Die Verschlüsselungstools von Kaspersky Lab bieten:

- Full-Disk-Verschlüsselung (FDE) – setzt bei den physischen Sektoren des Laufwerks an und verschlüsselt alle Dateien gleichzeitig
- File-Level-Verschlüsselung (FLE) – verschlüsselt einzelne Dateien oder Ordner, um den sicheren Austausch von Daten zwischen Mitarbeitern und Trusted-Partnern zu ermöglichen

Der AES-Verschlüsselungsalgorithmus mit einer Schlüssellänge von 256 Bit bietet zwar eine starke Verschlüsselung, dennoch sind alle Verschlüsselungs- und Entschlüsselungsprozesse für Ihre Mitarbeiter vollständig transparent. Stattdessen richten Ihre IT-Administratoren einfache Richtlinien ein, mit denen gesteuert wird, welche Dateien und Laufwerke automatisch verschlüsselt werden. Zudem haben die Verschlüsselungs- und Entschlüsselungsverfahren keine signifikanten Auswirkungen auf die IT-Leistung.

Zur Verschlüsselung auf mobilen Geräten bietet Ihnen Kaspersky Lab die Möglichkeit, die Verschlüsselungsfunktionen zu verwalten, die auf vielen gängigen Mobilplattformen vorhanden sind.

SICHERHEIT FÜR MOBILE GERÄTE UND MOBILE DEVICE MANAGEMENT

Kaspersky Lab war das erste Unternehmen, das Antiviren-Lösungen für mobile Geräte angeboten hat. Heute ist das Unternehmen ein führender Anbieter sowohl von modernen Anti-Malware-Agenten als auch effizienten MDM (Mobile Device Management)-Funktionen in einer integrierten Lösung.

Die Sicherheitstechnologien von Kaspersky Lab für mobile Geräte schützen eine Vielzahl von mobilen Plattformen – einschließlich Android, iOS, Windows Phone, Windows Mobile, BlackBerry und Symbian – vor den neuesten Malware-Bedrohungen. Da Kaspersky Lab den signaturbasierten Schutz, aktive Schutzmaßnahmen und Cloud-basierte Technologien kombiniert, werden mobile Geräte durch eine mehrschichtige Anti-Malware-Lösung geschützt.

KONTROLLTOOLS

Durch die Programmkontrolle kann zudem leichter festgelegt werden, welche Programme auf allen mobilen Geräten ausgeführt werden dürfen. Man kann einfach mit einer „Default Deny"-Richtlinie dafür sorgen, dass nur die Programme auf der Whitelist ausgeführt werden oder eine „Default Allow"-Richtlinie festlegen, mit der nur Programme auf der Blacklist blockiert werden.

Mit Tools zur Web-Kontrolle können Sie schädliche Webseiten oder Webseiten, die nicht der Sicherheitsrichtlinie oder Internet-Nutzungsrichtlinie Ihres Unternehmens entsprechen, blockieren.

TRENNUNG VON UNTERNEHMENSDATEN UND PERSÖNLICHEN DATEN: INITIATIVE FÜR EIN SICHERERES BYOD

Mithilfe der Containerisierung von Kaspersky Lab können Unternehmensdaten und persönliche Daten auf dem Mobilgerät eines Benutzers auf einfache Weise getrennt werden. Die Unternehmensprogramme werden dabei in einem speziellen Container aufbewahrt, und Sie können somit deren Verschlüsselung einzeln aktivieren. Wenn ein Mitarbeiter das Unternehmen verlässt, können Sie per Fernzugriff alle Unternehmensdaten auf dem mobilen Gerät löschen.

UMGANG MIT VERLORENEN ODER GESTOHLENEN MOBILEN GERÄTEN

Wenn ein mobiles Gerät verloren geht oder gestohlen wird, können Sie mithilfe der Remote-Zugriffsfunktionen von Kaspersky Lab Folgendes tun:

- das mobile Gerät sperren
- die Unternehmensdaten oder alle Daten auf dem Gerät löschen
- die ungefähre Position des Geräts ermitteln

Selbst wenn der Gerätedieb die SIM-Karte des Geräts bereits ausgetauscht hat, sendet Ihnen die SIM-Kontrollfunktion von Kaspersky Lab die neue Telefonnummer des Mobilgeräts zu. Damit haben Sie wieder die Möglichkeit, die Sperr-, Lokalisier- und Löschfunktionen per Fernzugriff auszuführen.

EINFACHERE VERWALTUNG VON MOBILGERÄTEN

Mit den umfangreichen MDM (Mobile Device Management)-Funktionen von Kaspersky Lab lässt sich das Deployment von deren mobilen Sicherheitsagenten und anderen Programmen vereinfachen: entweder over the air (OTA) oder über Tethering. Überdies werden Microsoft Exchange ActiveSync und Apple MDM Server unterstützt.

AUSWAHL VON SICHERHEITSTECHNOLOGIEN FÜR VIRTUALISIERTE UMGEBUNGEN

Mit seinen Sicherheitslösungen für eine breite Palette virtualisierter Umgebungen – einschließlich VMware, Citrix und Microsoft – überlässt Ihnen Kaspersky Security for Virtualization die Entscheidung zwischen zwei Ansätzen für die sichere Virtualisierung, die entwickelt wurden, um die Auswirkungen auf die Konsolidierungsraten zu minimieren und Ihren ROI zu steigern.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Wenn Sie über eine VMware-basierte Umgebung verfügen, arbeitet Kaspersky Security for Virtualization | Agentless über VMware vShield, damit Sie jede virtualisierte Maschine auf einem virtualisierten Host schützen können. Hierfür wird eine virtualisierte Maschine installiert, die für Sicherheit zuständig ist (Security Virtual Appliance oder SVA).

Neben dem Malware-Schutz auf Dateiebene und Netzwerkebene – über die Network-Attack-Blocker-Technologie von Kaspersky Lab nutzt Kaspersky Security for Virtualization | Agentless auch Echtzeit-Bedrohungsinformationen aus dem Kaspersky Security Network.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

Mit einer eigenen Security Virtual Appliance auf dem Host und einem kleinen Software-Agenten – dem Light Agent – auf jeder virtualisierten Gastmaschine bietet Kaspersky Security for Virtualization | Light Agent ein höheres Sicherheitsniveau als agentenlose Virtualisierungslösungen. Trotzdem benötigt diese Lösung wesentlich weniger Systemleistung und Speicherkapazität als ein traditionelles, agentenbasiertes Sicherheitsprodukt – dank Auslagerung der Anti-Malware-Aufgaben und der Malware-Datenbank an die Security Virtual Appliance.

Neben dem fortschrittlichen Malware-Schutz und dem Schutz auf Netzwerkebene umfasst Kaspersky Security for Virtualization | Light Agent auch Werkzeuge für die Programm-, Geräte- und Web-Kontrolle.

HOHE KONSOLIDIERUNGSRATEN – HOHE VERFÜGBARKEIT

Ob Sie sich nun für Kaspersky Security for Virtualization | Agentless oder Kaspersky Security for Virtualization | Light Agent entscheiden – Sie müssen keine Maschine neu starten oder den Hostserver in den Wartungsmodus versetzen, wenn Sie Ihre Sicherheitslösung von Kaspersky Lab einrichten.

Diese ist perfekt für Rechenzentren und Unternehmen geeignet, die eine Leistung mit „fünf Neunen“ (99,999 %) bei der Betriebszeit erbringen müssen.

KOMBINATION AUS SICHERHEITS- UND SYSTEMS-MANAGEMENT-FUNKTIONEN

VERWALTUNG VON HARDWARE, SOFTWARE UND LIZENZEN

Kaspersky Lab stellt Ihnen detaillierte Kenntnisse über Ihre IT-Ressourcen bereit: durch die automatische Erkennung aller Hard- und Software-Elemente in Ihrem Firmen-IT-Netzwerk und deren Protokollierung im Hard- und Software-Bestand. Dadurch können Sie:

- den Sicherheitsstatus Ihrer Systeme überwachen
- die notwendigen Sicherheitseinstellungen vornehmen
- Verstöße gegen Lizenzbedingungen ermitteln

DEPLOYMENT VON BETRIEBSSYSTEMEN

Kaspersky Lab unterstützt Sie beim optimierten Deployment von Betriebssystemen. Hierzu werden automatische Funktionen bereitgestellt, mit denen Computer-Images erstellt und geklont und in einem separaten Verzeichnis abgelegt werden können, sodass diese bei einem Deployment verfügbar sind.

APPLICATION PROVISIONING

Mit Kaspersky Lab wird die Bereitstellung von Programmen erleichtert. Sie werden dabei unterstützt, Software per Befehl oder zeitplangesteuert bereitzustellen.

REMOTE-DEPLOYMENT VON SOFTWARE UND TROUBLESHOOTING PER FERNZUGRIFF

Wenn Sie neue Software in einer entfernten Zweigstelle installieren müssen, ermöglicht Kaspersky Lab Ihnen den Einsatz einer lokalen Workstation als Update-Agent für den gesamten Remote-Standort. Darüber hinaus wird die Fehlerbehebung durch den Fernzugriff erheblich vereinfacht.

NETZWERKZUGRIFFSKONTROLLE (NAC)

Mit Technologien, die automatisch alle Geräte in Ihrem Unternehmensnetzwerk ermitteln, erleichtert Kaspersky Lab die folgenden Aufgaben:

- Kontrollieren, welche Geräte für den Zugriff auf das Netzwerk berechtigt sind
- Überprüfen, dass jedes Gerät die Sicherheitsrichtlinien des Unternehmens erfüllt
- Blockieren des Netzwerkzugriffs für Geräte, die nicht die erforderliche Sicherheitssoftware ausführen

EINE EINHEITLICHE VERWALTUNGSKONSOLE

Die Sicherheitstechnologien und Systems-Management-Funktionen von Kaspersky Lab können von einer Verwaltungskonsole aus konfiguriert und kontrolliert werden, womit der IT-Administrator eine Übersicht über eine einzige Benutzeroberfläche erhält.

Es ist nicht mehr nötig, mehrere verschiedene und womöglich nicht kompatible Konsolen zu betreiben. Kaspersky Security Center reduziert die Komplexität und erspart Ihrer IT-Abteilung einen erheblichen Zeitaufwand.

Durch die einheitliche Konsole werden zahlreiche verschiedene Verwaltungs- und Sicherheitsaufgaben über physische, mobile und virtualisierte Umgebungen vereinfacht. Sie profitieren von Folgendem:

- besserer Überblick über jeden Endpoint im IT-Netzwerk Ihres Unternehmens
- eine einfache Schnittstelle für die Sicherheits-, MDM- und Systems-Management-Funktionen
- detaillierte Kontrolle über die Benutzeraktivitäten, einschließlich deren Nutzung von Programmen, Geräten und dem Internet

ÜBERBLICK ÜBER BEWÄHRTE INNOVATIONEN UND LEISTUNGEN VON KASPERSKY LAB

Zu den vielen Preisen, Auszeichnungen und Anerkennungen für Kaspersky Lab zählt der Preis „Produkt des Jahres 2013“ vom unabhängigen Testlabor AV-Comparatives, der verliehen wurde, nachdem unsere Internet-Sicherheitslösung durchgehend die besten Ergebnisse im Jahr 2013 erzielt hatte.

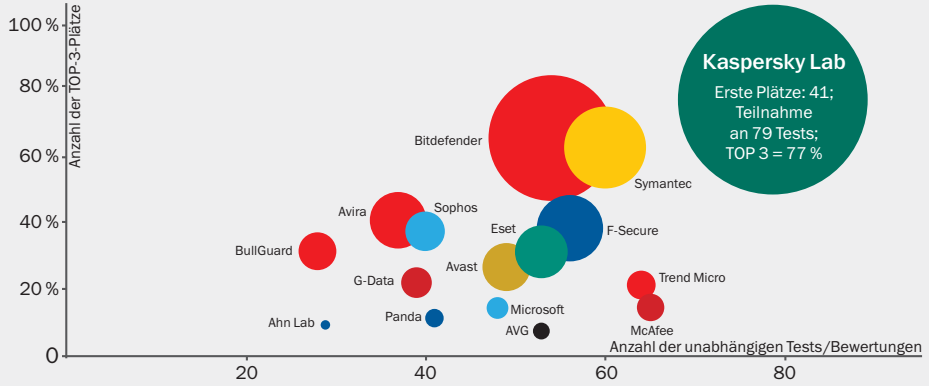
Das Testprogramm von AV-Comparatives gilt als das umfassendste in der Branche. Der Preis als „Produkt des Jahres“ wird auf der Grundlage des Gesamtrankings in einem vollen Testjahr vergeben. Kaspersky Internet Security wurde ausgewählt, weil das Produkt bei allen durchgeführten Tests solide in Führung lag. Kaspersky Lab hat bereits im Jahr 2011 den Titel „Produkt des Jahres“ von AV-Comparatives errungen und war auch im Jahr 2012 ganz oben mit dabei.

Da Kaspersky Endpoint Security for Business dieselben zentralen Malware-Schutz-Technologien nutzt wie Kaspersky Internet Security kann Ihr Unternehmen vom preisgekrönten Schutz von Kaspersky Lab profitieren. Zu den weiteren Preisen und Leistungen zählen:

- Auszeichnung „Information Security Vendor of the Year“ – SC Magazine Awards Europe 2013
- Auszeichnung „Information Security Team of the Year“ – SC Magazine Awards Europe 2013
- Gewinner des Excellence Award – SC Magazine Awards 2013
- Höchste Auszeichnung für Kaspersky Endpoint Security for Windows im Test „Virenschutz für Unternehmen“, April-Juni 2013, von Dennis Technology Labs
- Die größte Anzahl von Gold- und Platin-Auszeichnungen – in allen Testkategorien – vom Drittanbieter Anti Malware Test Lab seit 2004.
- Mehr als 50 x „Bestanden“ bei den strikten Tests von VB100 seit 2000
- Auszeichnung „Checkmark Platinum Product“ von West Coast Labs

MEHR PLÄTZE UNTER DEN TOP 3 ALS ANDERE ANBIETER

Im Jahr 2013 haben die Produkte von Kaspersky Lab an 79 unabhängigen Tests und Bewertungen teilgenommen. Unsere Produkte waren 41 Mal auf Platz 1 und 61 Mal unter den Top 3.



Anmerkungen:
- Laut dem Gesamtergebnis eines im Jahr 2013 durchgeführten unabhängigen Tests von Unternehmens-, Verbraucher- und mobilen Produkten
- Das Gesamtergebnis umfasst Tests, die von den folgenden unabhängigen Testlaboren und Zeitschriften durchgeführt wurden:
  - Testlabore: Anti-Malware.ru, AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, TollyGroup, VB100
  - Zeitschriften: CHIP Online, ComputerBild, Micro Hebdo, PC Magazine, PCWorld, PC Welt
- Im oben abgebildeten Diagramm zeigt die Größe jedes Kreises die Anzahl der erreichten ersten Plätze.

STRATEGISCHE TIPPS VON MAX: SO WIRD EINE SICHERE IT IHR VERDIENST

„Aufgrund des unaufhaltsamen Anstiegs von Malware und anderen Bedrohungen sowie deren zunehmender Raffinesse muss das Thema Sicherheit in der IT-Strategie jedes Unternehmens eine wichtige Rolle spielen.“

- Es ist an der Zeit, Ihre alltägliche IT-Routine zu unterbrechen und etwas Zeit in die Bewertung Ihrer vorhandenen IT-Sicherheitsmaßnahmen zu investieren. Beurteilen Sie, ob diese Maßnahmen ausreichen, um die heutigen Anforderungen zu meistern.
- Wählen Sie eine IT-Sicherheitslösung, die möglichst flexibel und skalierbar ist und vermeiden Sie sämtliche Produkte, welche die Agilität Ihres Unternehmens beschränken.
- Denken Sie daran, dass es bei der IT-Sicherheit bei Weitem nicht nur um Malware-Schutz geht. Suchen Sie nach Sicherheitslösungen, die zusätzlichen Schutz bieten, einschließlich Programmkontrolle, Gerätekontrolle, Web-Kontrolle, Datenverschlüsselung und mehr.
- Die Nutzung von mobilen Geräten nimmt weiter zu. Vergessen Sie deshalb nicht, dass auf Smartphones und Tablets große Mengen an vertraulichen Geschäftsdaten gespeichert werden können. Stellen Sie sicher, dass auf allen mobilen Geräten, die auf Ihr Unternehmensnetzwerk und Ihre Geschäftsdaten zugreifen, eine entsprechende Sicherheitssoftware ausgeführt wird. Nutzen Sie Mobile Device Management (MDM), um die mobilen Geräte in Ihrem Netzwerk zu überwachen.
- Vor dem Start einer BYOD (Bring Your Own Device)-Initiative sollten Sie bewerten, wie sich dies auf die Unternehmenssicherheit auswirkt. Ziehen Sie Sicherheitstechnologien in Betracht, die Ihnen erlauben, Unternehmensdaten und persönliche Daten des Benutzers auf deren mobilen Geräten voneinander zu trennen.
- Virtualisierte Umgebungen sind nicht sicherer als Umgebungen mit physischen Servern und Desktops – auch sie müssen geschützt werden. Treffen Sie die Entscheidung für ein Sicherheitsprodukt für Ihre virtualisierte Infrastruktur jedoch mit Bedacht. Die falsche Sicherheitstechnologie könnte sich negativ auf die Konsolidierungsraten auswirken.
- Schwachstellen in der Software sind das gängige Einfallstor für Malware und Cyberkriminelle zu Ihren Computern und Netzwerken. Stellen Sie deshalb sicher, dass Ihre Systems-Management-Software Funktionen für das Vulnerability Scanning und Patch Management umfasst. Obwohl es sich dabei um Systems-Management-Funktionen handelt, können sie sich erheblich auf Ihre Sicherheit auswirken.
- Wenn Sie sich für ein Produkt entscheiden, das Sicherheits- und Systems-Management-Funktionen vereint, kann die Abwicklung der Aufgaben deutlich vereinfacht werden, und Sie können integrierte Richtlinien festlegen, wodurch Sie viel Zeit einsparen können.
- Benutzerfreundlichkeit bedeutet bei IT-Sicherheits- und auch bei Systems-Management-Software mehr als nur praktische Funktionen. Wenn Ihre Sicherheits- und Systems-Management-Software komplex und schwer zu verwalten ist, besteht ein viel größeres Risiko, dass Fehler und Sicherheitslücken auftreten.

„Die Leute von Kaspersky Lab konzentrieren sich auf das, was sie gut können: Endpoint-Sicherheit. Mit der hohen Punktzahl für Funktionen und strategische Kriterien wird die interne Entwicklung im Unternehmen anerkannt, durch die möglichst weitgehend sichergestellt wird, dass die verschiedenen Komponenten für Workstations, Laptops, E-Mail, gemeinschaftlich genutzte Server und Internet-Gateways dieselbe Code-Basis für einfache Updates und Kontinuität im Falle eines Produktfehlers nutzen.”

IDC MARKETSCAPE: WESTERN EUROPEAN ENTERPRISE ENDPOINT SECURITY 2012 VENDOR ANALYSIS
JANUAR 2013, IDC NR. IS01V, BAND: 1

ÜBER KASPERSKY LAB

Kaspersky Lab ist der weltweit größte Privatanbieter von Lösungen für den Schutz von Endpoints. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer.* In seiner 16-jährigen Firmengeschichte hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet großen Unternehmen, KMUs und Einzelverbrauchern wirksame digitale Lösungen für die Datensicherheit. Kaspersky Lab ist derzeit in nahezu 200 Ländern und Regionen weltweit tätig und sorgt für den Schutz von mehr als 300 Millionen Anwendern weltweit.

Weitere Informationen erhalten Sie unter
http://www.kaspersky.com/de/business-security.

* Das Unternehmen belegte im Rahmen des IDC-Rating „Worldwide Endpoint Security Revenue by Vendor 2012" den vierten Rang. Die Rangfolge wurde im IDC-Bericht „Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC Nr. 242618, August 2013) veröffentlicht. In dem Bericht wurden Softwarehersteller auf Grundlage ihrer Erlöse aus dem Verkauf von Sicherheitslösungen für Endpoints im Jahr 2012 eingestuft.