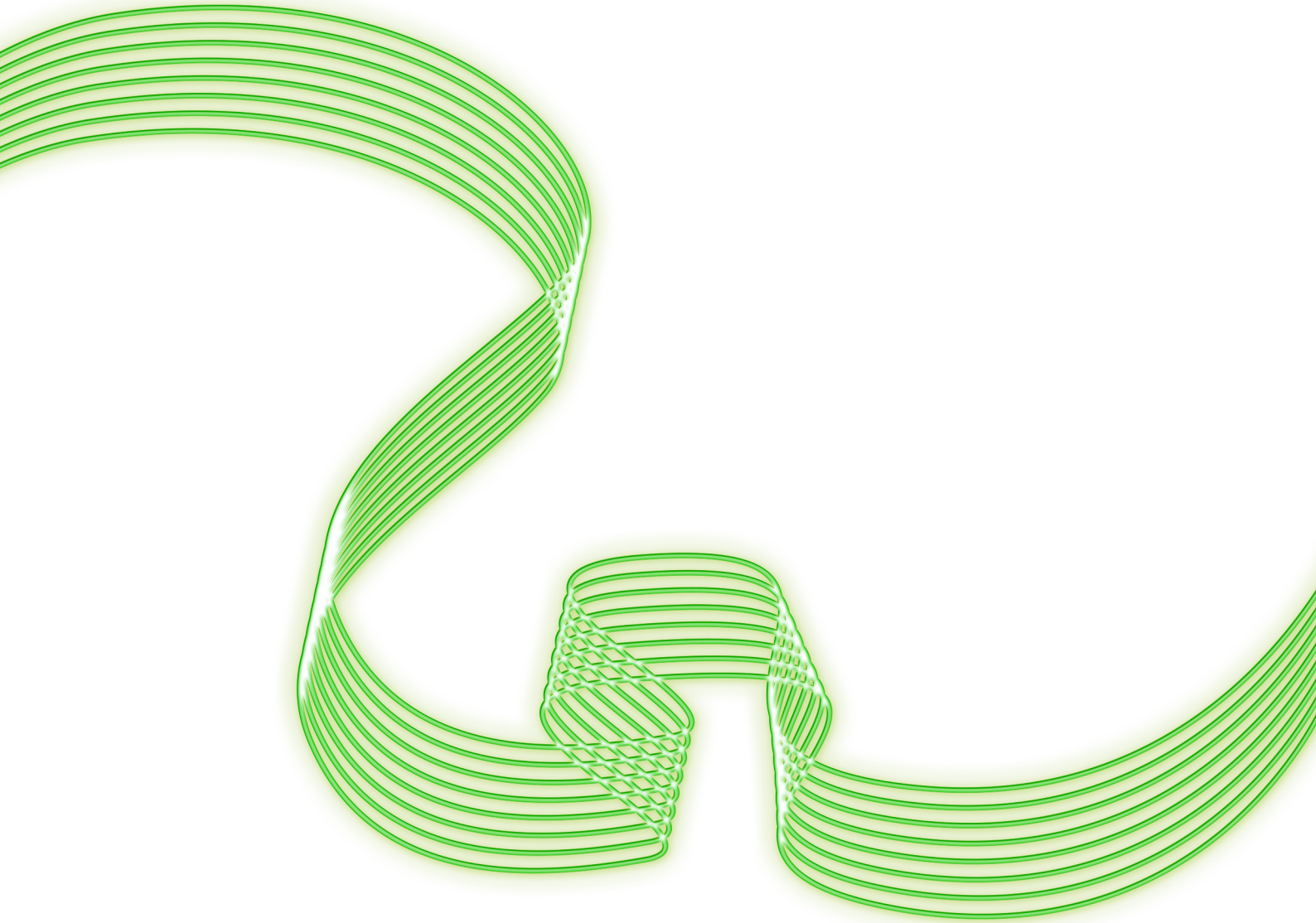

AUFWAND VERRINGERN – SICHERHEIT ERHÖHEN

Wie können Sie angesichts der steigenden Komplexität der Firmen-IT gleichzeitig die Effizienz und die Unternehmenssicherheit steigern?

With Kaspersky, now you can.
www.kaspersky.de/business

Be Ready for What's Next

KASPERSKY lab

Inhaltsverzeichnis

1.0	Zusammenfassung	3
2.0	Argumente für effiziente Systems-Management-Lösungen	4
3.0	Systems Management – die größten Herausforderungen	7
4.0	Systems Management – die Lösungen	10
5.0	Kaspersky Systems Management	13
6.0	Fazit	16

Zusammenfassung

1.0

1.1 KOMPLEXE IT KOMMT UNTERNEHMEN TEUER ZU STEHEN

Aufgrund der zunehmenden Komplexität unternehmenseigener IT-Umgebungen wird die Aufgabe ihrer Verwaltung immer aufwendiger und nimmt immer mehr Zeit in Anspruch. Diese wachsende Komplexität bringt zahlreiche Herausforderungen für Unternehmen mit sich:

- **Erhöhte Kosten** – Der Zeit- und Arbeitsaufwand für alltägliche Systems-Management-Aufgaben steigt.

- **Überlastete Ressourcen** – Mit der Einführung jedes neuen Geräts und jeder neuen Anwendung in das Unternehmensnetzwerk wächst die Liste der regelmäßigen IT-Verwaltungsaufgaben.

- **Weniger Flexibilität** – Angesichts der zahlreichen routinemäßigen IT-Verwaltungsaufgaben bleibt den IT-Mitarbeitern weniger Zeit, das Unternehmen bei der Einführung neuer Services zu unterstützen, die zu einem entscheidenden Wettbewerbsvorteil werden könnten.

- **Sicherheitslücken** – Manuelle Prozesse sowie die Notwendigkeit, separate Verwaltungskonsolen für unterschiedliche Aufgaben zu verwenden, schaffen ideale Voraussetzungen für Betriebsfehler – und solche Fehler können zu ernsthaften Sicherheitslücken führen.

- **Mangelnde Transparenz** – Die Komplexität der meisten unternehmensinternen IT-Umgebungen macht es für IT-Mitarbeiter schwierig, sich einen Überblick über die gesamte Hardware und Software des Netzwerks zu verschaffen. Dieser Punkt ist besonders wichtig. Ohne ein präzises Bild der IT-Infrastruktur in ihrer Gesamtheit fehlt Unternehmen die Grundlage für:
  - die Kontrolle darüber, wie ihre IT-Bestände verwendet werden – sei es zwecks größerer Effizienz oder zur Einhaltung von Richtlinien oder gesetzlichen Auflagen
  - die Verwaltung ihrer IT-Umgebung zur Aufrechterhaltung der Service-Levels und der Produktivität
  - den Schutz aller Systeme und vertraulichen Daten vor Schadsoftware und Angriffen

1.2 ABBAU VON KOMPLEXITÄT FÜR MEHR EFFIZIENZ UND VERSTÄRKTE SICHERHEIT

Die neuesten IT-Systems-Management-Lösungen vereinfachen und automatisieren zahlreiche routinemäßige IT-Verwaltungsaufgaben. Dies bietet folgende Vorteile:

- **Reduzierung des Workloads der IT-Mitarbeiter**, sodass diese mehr Zeit in strategische IT-Projekte investieren können, um die betriebliche Effizienz und Wettbewerbsfähigkeit zu steigern
- **Kostenmanagement und -reduzierung**
- **Beseitigung häufiger Fehlerquellen bei der IT-Verwaltung**
- **Ermöglichung zuverlässigerer System- und Datensicherheit**

Zu den besten Lösungen gehören Produkte mit einer einheitlichen Verwaltungsoberfläche, die es IT-Mitarbeitern ermöglicht, ein breites Spektrum von Systems-Management-Aufgaben von einer einzigen Konsole aus zu überwachen und zu verwalten.

Argumente für effiziente Systems-Management-Lösungen

2.0

2.1 DIE WACHSENDE BEDEUTUNG DER IT

Angesichts der Tatsache, dass die IT immer mehr unternehmenskritische Prozesse unterstützt (was für Unternehmen jeder Größenordnung gilt), ist die effiziente Verwaltung aller Elemente des Unternehmensnetzwerks unumgänglich und bietet folgende Vorteile:

- Durchführung aller für moderne Unternehmen erforderlichen wichtigen Geschäftsprozesse
- Aufrechterhaltung hoher Service-Levels für die Mitarbeiter und Kunden des Unternehmens
- Freisetzung vorhandener IT-Ressourcen für neue strategische IT-Projekte
- Management und Minimierung der Kosten

Die IT spielt eine immer wichtigere Rolle bei der Einführung neuer Services und der Verbesserung bestehender Prozesse. Infolgedessen sind IT-Abteilungen jedoch gezwungen, eine immer größere Anzahl von Geräten und eine immer breitere Palette unterschiedlicher Endpoints zu verwalten.

2.2 DIE WACHSENDEN BEDROHUNGEN FÜR IHR UNTERNEHMEN

Gleichzeitig nimmt die Anzahl der gegen Unternehmenssysteme – und die Sicherheit wertvoller Daten – gerichteten Bedrohungen exponentiell zu. Leider werden diese Bedrohungen auch immer komplexer, wenn es darum geht, die Sicherheit von Unternehmen zu unterwandern. So steigt nicht nur die Menge der Sicherheitsbedrohungen, sondern auch deren Effektivität.

Die heutigen Angriffe von Cyberkriminellen und Schadsoftware sind bei dem Versuch, die Sicherheitslücken auszunutzen, unaufhaltsam. Die Ziele solcher Angriffe:

- Geld von Unternehmen zu stehlen
- den Ruf oder die Marktposition von Unternehmen zielgerichtet zu schädigen, z. B durch:
  - einen Denial-of-Service (DoS)-Angriff, der die webbasierten Services von Unternehmen zeitweilig ausschaltet
  - den Diebstahl vertraulicher Daten, einschließlich wertvollen geistigen Eigentums
- persönliche Daten über die Kunden und Angestellten eines Unternehmens zu sammeln – zum Identitätsdiebstahl und zum Stehlen von Geld einzelner Personen

2.3 WARUM KOMPLEXITÄT VERMIEDEN WERDEN SOLLTE

Komplexität in all ihren Formen kann sich sehr geschäftsschädigend auswirken. Im Folgenden finden Sie einige Beispiele dazu, wie Komplexität die IT beeinträchtigt:

- Komplexe IT-Systems-Management-Prozesse:
  - verbrauchen wichtige Supportressourcen
  - verschwenden Geld
  - lassen dem Unternehmen weniger Zeit, um sich strategischen IT-Projekten zu widmen

- Komplexe Prozesse in der IT-Sicherheitsverwaltung erhöhen das Risiko kostspieliger Fehler, die Unternehmen anfällig für Schadsoftware und zielgerichtete Angriffe machen können.

Da IT-Umgebungen immer komplexer werden – mit einer größeren Anzahl von Geräten und Zugriffspunkten – müssen Unternehmen aktiv nach Möglichkeiten suchen, die Auswirkungen dieser Komplexität einzudämmen. Es müssen Methoden erarbeitet werden, die:

- viele der täglich anfallenden IT-Verwaltungsaufgaben vereinfachen und automatisieren
- die Notwendigkeit von Expertenschulungen für reguläre IT-Verwaltungsaufgaben minimieren
- sicherstellen, dass das Unternehmensnetzwerk trotz ständig wechselnder IT-Sicherheitsbedrohungen geschützt bleibt

2.4 ÜBERLASTUNG DURCH TÄGLICH ANFALLENDE SYSTEMS-MANAGEMENT-AUFGABEN

An einem normalen Arbeitstag führen IT-Administratoren viele oder alle der folgenden Aufgaben aus:

- Einrichten neuer Workstations, Laptops und Server
- Bereitstellen neuer Software-Anwendungen für verschiedene Bereiche des Unternehmensnetzwerks
- Sicherstellen, dass Software-Lizenzverpflichtungen erfüllt werden und keine unlizenzierte Software ausgeführt wird
- Anwenden von Richtlinien hinsichtlich des Zugriffs von Geräten auf das Unternehmensnetzwerk
- Überprüfen, ob Anwendungen im Netzwerk ausgeführt werden dürfen oder nicht
- Erkennen von Sicherheitslücken in Betriebssystemen und Anwendungen
- Bewerten des Schweregrads von Schwachstellen und Festlegen von Prioritäten hinsichtlich Wiederherstellungsmaßnahmen
- Implementieren der neuesten Patches und Updates zur Eliminierung von Sicherheitslücken
- Unterstützen mobiler und Remote-Benutzer beim Zugriff auf Unternehmenssysteme
- Kontrollieren der Einschränkungen beim Zugriff von Gästegeräten auf das Unternehmensnetzwerk

2.5 ZUSÄTZLICHE SCHWIERIGKEITEN FÜR DAS IT-TEAM

Eine solch lange Liste an Herausforderungen für die IT-Verwaltung stellt eine erhebliche Belastung für IT-Abteilungen dar. Dabei sind allerdings auch noch weitere Faktoren zu berücksichtigen:

- Tragbare Geräte wie Wechseldatenträger sind potenzielle „Lecks“ für Unternehmensdaten.
- Benutzer laden ohne Lizenz Software und Anwendungen herunter, die Schadsoftware enthalten können.
- Bring-Your-Own-Device (BYOD)-Initiativen schaffen neue betriebliche Herausforderungen und Sicherheitsprobleme für das Unternehmen.

… und all das zu einer Zeit, in der Schadsoftware immer raffinierter wird und Cyberkriminelle neue und höchst lukrative Möglichkeiten entwickeln, um Unternehmenssysteme und -daten anzugreifen.

2.6 DIE POTENZIELLEN VORTEILE VERBESSERTER SYSTEMS-MANAGEMENT-LÖSUNGEN

Trotz all dieser Schwierigkeiten haben IT-Abteilungen die Aufgabe, die Unternehmensanforderungen hinsichtlich stabiler IT-Services zu erfüllen, um den Anforderungen von Mitarbeitern, mobilem Personal, Kunden und Anbietern gerecht zu werden. Gleichzeitig müssen sie jedoch auch ein Höchstmaß an Sicherheit für alle Systeme und Daten gewährleisten.
Darüber hinaus unterliegen diese Aufgaben in den meisten Unternehmen strengen Budgetvorgaben.

Um IT-Teams bei diesem Balance-Akt zwischen Servicebereitstellung und Budgetkontrolle zu unterstützen, haben Anbieter versucht, umfassendere Systems-Management-Lösungen zu entwickeln, die Folgendes bieten:

- Vereinfachung und Automatisierung der:
  - Bereitstellung von Betriebssystemen
  - Bereitstellung von Anwendungssoftware
- Fehlerbehebung per Fernzugriff
- Erstellung automatischer Bestandslisten über Hardware und Software, um:
  - dem Unternehmen vollständige Transparenz hinsichtlich aller Bereiche seiner IT-Umgebung zu bieten
  - die Überwachung und Kontrolle von Softwarelizenzen zu vereinfachen
- Automatisches Aufdecken von Schwachstellen in der Software und Priorisierung der Patch-Bereitstellung
- Durchführung geplanter regelmäßiger Sicherheitsscans
- Verhindern der Nutzung illegaler oder unerwünschter Software
- Festlegung und Verwaltung von Zugriffsrichtlinien für Unternehmensressourcen

Systems Management – die größten Herausforderungen

3.0

3.1 TRANSPARENZ

Warum Transparenz von entscheidender Bedeutung ist

Wann immer ein neuer Geschäftsprozess eingeführt oder ein neues IT-Projekt umgesetzt wird, ist dies meist mit der Einführung neuer Hardware und Software im Unternehmensnetzwerk verbunden. Mit jedem Jahr, in dem neue Geräte und Anwendungen eingeführt werden, steigt die Wahrscheinlichkeit, dass Unternehmen feststellen, wie wenig Überblick sie darüber haben, welche Hardware und Software in ihrem Netzwerk ausgeführt wird.

Doch wie können Unternehmen ohne detaillierte Transparenz bei Servern, Laptops, Routern, Switches und Wechseldatenträgern sowie bei Betriebssystemen und Anwendungen ihr Netzwerk effektiv verwalten und schützen?

- Hardware-Transparenz unterstützt IT-Teams bei folgenden Aufgaben:
  - Implementierung von Kontrollfunktionen, um vertrauliche Daten vor dem Download auf nicht autorisierte Wechseldatenträger zu schützen
  - Überwachung der Einführungsversuche neuer, nicht autorisierter Geräte
  - Identifizierung und Außerbetriebnahme alter, nicht unterstützter Geräte

- Software-Transparenz unterstützt IT-Teams bei folgenden Aufgaben:
  - Verwaltung der Art und Weise, wie bei Betriebssystemen und Anwendungen Fehler behoben und Updates durchgeführt werden, sodass Systeme und Software störungsfrei ausgeführt und Sicherheitslücken eliminiert werden
  - Unterbinden der Nutzung nicht autorisierter Anwendungen, die Schadsoftware enthalten können
  - Unterstützung von Compliance-Zielen – durch Erkennung und Eliminierung illegaler, raubkopierter Software, die möglicherweise von Mitarbeitern heruntergeladen wurde
  - Verwaltung des Unternehmensbestands an Softwarelizenzen, sodass keine unnötigen Kosten durch nicht genutzte bzw. nicht benötigte Lizenzen entstehen
  - Identifizierung alter Anwendungen, die nicht mehr vom Hersteller unterstützt werden

Mobilität erhöht Transparenzprobleme

Angesichts der zunehmenden Anzahl an mobilen Geräten ist es für Unternehmen wichtiger denn je, vollständige Transparenz hinsichtlich aller auf das Netzwerk zugreifenden Geräte zu erlangen. Diese Fülle an mobilen Geräten schließt auch Bring-Your-Own-Device (BYOD)-Initiativen ein, im Rahmen derer Mitarbeiter über ihre eigenen Smartphones, Tablets und anderen Geräte Zugriff auf das Unternehmensnetzwerk erhalten.

3.2 SOFTWAREBEREITSTELLUNG

Die Vorteile der Automatisierung

Die manuelle Installation und Konfiguration von Betriebssystemen und Anwendungen auf jedem Server, Desktop und Laptop ist äußerst zeitaufwendig, besonders dann, wenn die Umsetzung auch externe Büros und Niederlassungen betrifft.

In der Vergangenheit traten bei einer längerfristigen manuellen Einführung von Software in der Regel Probleme auf, weil unterschiedliche Benutzer Zugriff auf unterschiedliche Software hatten (einige Benutzer führten bereits die neueste Software aus, andere warteten noch auf die Aktualisierung ihrer Computer).
Die Automatisierung der Bereitstellung von Betriebssystemen kann dabei helfen, Konsistenz zu gewährleisten und gleichzeitig Zeit und Geld zu sparen.

3.3 SCHWACHSTELLEN

So entstehen Schwachstellen

Software ist nur in den seltensten Fällen fehlerfrei: Der Quellcode fast aller im Handel erhältlichen Software-Anwendungen und Betriebssysteme enthält Fehler.

Einige dieser Fehler erschweren lediglich die Nutzung und können umgangen werden. Viele Softwarefehler bieten allerdings neue, umfangreiche Möglichkeiten für Schadsoftware und Cyberkriminelle, Zugriff auf Unternehmenssysteme und -daten zu erhalten, um vertrauliche Daten und Geld zu stehlen, den Ruf des Unternehmens zu schädigen oder Daten bzw. Systeme zu blockieren, bis die Unternehmen ein „Lösegeld“ an den Blockierer gezahlt haben.

Daher ist es kein Wunder, dass die Eliminierung dieser Schwachstellen, sowohl in Betriebssystem als auch in Anwendungen, zu einem wesentlichen Teil der täglichen IT-Verwaltungsaufgaben geworden ist.

Zielgerichtete Angriffe

Die Ausnutzung von Schwachstellen ist schon lange nicht mehr das Resultat willkürlicher Angriffe. In den vergangenen Jahren hat sich ein Wandel von der unausgegorenen, willkürlichen Vorgehensweise vollzogen, bei der Kriminelle Angriffe mit breiter Basis starteten – in der Hoffnung, zufällig auf ein Unternehmen oder eine Organisation zu stoßen, deren IT-Infrastruktur Schwachstellen aufweist. Heutzutage suchen sich organisierte Cyberkriminelle zielgerichtet bestimmte Unternehmen aus. Bevor sie ihren Angriff starten, haben die Kriminellen bereits die speziellen Schwächen oder Schwachstellen in der IT-Infrastruktur des anvisierten Unternehmens identifiziert.

In einigen Fällen erstellen Hacker sogar Listen der Schwachstellen, die innerhalb der IT-Umgebung bestimmter Unternehmen auftreten, und verkaufen diese Listen mitsamt dem Unternehmensnamen an andere Kriminelle.

Die häufigste Art des Angriffs

Da alle Unternehmen zahlreiche Anwendungen für ihre täglichen Geschäftsprozesse verwenden, ist es nicht verwunderlich, dass Schadsoftware- und Cyberangriffe auf Unternehmensnetzwerke am häufigsten über die Schwachstellen in Betriebssystemen und Anwendungen erfolgen. Daher ist es äußerst wichtig, dass IT-Teams alle Betriebssysteme und Anwendungen überwachen und durch die neuesten Patches auf dem aktuellen Stand halten.

3.4 BEREITSTELLUNG VON PATCHES

Beobachten der Verfügbarkeit von Patches

Wenn eine Schwachstelle erkannt wurde, besteht eine der größten Herausforderungen darin, die Zeit zwischen der Veröffentlichung eines neuen Patches und dessen Bereitstellung in der IT-Infrastruktur des Unternehmens so gering wie möglich zu halten.

In der Vergangenheit mussten IT-Administratoren Zeit für die Beobachtung der Nachrichtenmedien der IT-Branche aufwenden, um von neuen Sicherheitslücken innerhalb von Betriebssystemen und Anwendungen zu erfahren. Gleichzeitig mussten sie mit den Anbietern in Kontakt bleiben, um Informationen zur Verfügbarkeit neuer Patches zu erhalten. Dies kann sehr zeitaufwendig sein und lässt Raum für die Möglichkeit, dass das IT-Team eines Unternehmens Informationen zu wichtigen Patches verpasst.

Problem-Patches

Die Veröffentlichung eines neuen Patch stellt noch lange nicht die Lösung für das Problem dar. In manchen Fällen kann ein Patch die Funktionsweise einer Anwendung oder eines Betriebssystems beeinträchtigen, in extremen Fällen sogar ein gesamtes System betriebsunfähig machen.

So stehen Unternehmen vor dem Dilemma, sich zwischen der Anwendung des Patches – auch wenn dies die nahtlose Ausführung von wichtigen Geschäftsprozessen beeinträchtigt – und der weiteren Nutzung der Anwendung ohne die Vorteile des letzten Sicherheitspatches entscheiden zu müssen.

IT-Administratoren testen neue Patches oft auf einem separaten Computer mit Testhardware, um festzustellen, ob der Patch die Ausführung einer Anwendung stark einschränkt.

3.5 ZUGRIFFSKONTROLLE

Entscheiden, wer Zugriff auf das Netzwerk erhält

Bei den meisten Unternehmen befinden sich oft Gastgeräte im Unternehmensnetzwerk. Wenn Partner oder Kunden das Unternehmen besuchen, bringen Sie für gewöhnlich ihre Laptops und Tablets mit. Somit muss das Unternehmen Richtlinien und Kontrollen festlegen, anhand derer den Gastgeräten der Zugriff auf das Unternehmensnetzwerk gestattet wird.

Auch wenn das Unternehmen eine BYOD-Strategie verfolgt, müssen die notwendigen Netzwerkszugriffskontrollen umgesetzt werden.

Mobil- und Gastgeräte müssen identifiziert und auf Schadsoftware überprüft werden. Außerdem darf diesen Geräten nur dann Zugriff auf Unternehmenssysteme gewährt werden, wenn sichergestellt wurde, dass das Gerät mit der geeigneten Sicherheitssoftware und den passenden Sicherheitseinstellungen konfiguriert wurde.

Systems Management – die Lösungen

4.0

4.1 ERLANGEN EINES TRANSPARENTEN ÜBERBLICKS ÜBER DAS UNTERNEHMENSNETZWERK

Einige Systems-Management-Lösungen können ganze Unternehmensnetzwerke scannen, alle Komponenten identifizieren und eine detaillierte Bestandsaufnahme der gesamten Hardware und Software erstellen:

Hardware-Bestandsaufnahme

Durch Auflistung aller:

- Server
- Desktops
- Laptops
- Wechseldatenträger usw.

… können IT-Mitarbeiter den Status und den Verlauf jedes Hardware-Elements verfolgen. Wenn es der Administrator als notwendig erachtet, können ungenutzte Geräte in ein Archiv übertragen werden.

Software-Bestandsaufnahme

Durch das Auflisten von Informationen über die gesamte Software, die auf dem Unternehmensnetzwerk verfügbar ist, unterstützt die Software-Bestandsaufnahme die Lizenzkontrolle, die Identifizierung ungepatcher Software und vieles mehr.

Stärkung des IT-Teams

Der transparente Überblick über die Hardware- und Software-Bestandsaufnahme befähigt das IT-Team, Folgendes zu tun:

- Priorisieren von Verwaltungs- und Sicherheitsaufgaben
- Beseitigen von Sicherheitslücken
- Umsetzen eines strategischen Ansatzes, um von den Unternehmensinvestitionen in die IT-Infrastruktur optimal zu profitieren.

Sämtliche „vergessene“ Anwendungen (einschließlich Software, die nicht aktiv verwendet wird, aber immer noch auf einer Workstation oder einem Server vorhanden ist) könnten die Schwachstelle für einen Angriff auf das Unternehmensnetzwerk darstellen. Mit dem transparenten Überblick über die gesamte Software innerhalb des IT-Unternehmensnetzwerks ist es dem IT-Team möglich, ungenutzte Anwendungen zu identifizieren und sie entweder zu entfernen oder sicherzustellen, dass sie auf dem neuesten Stand gehalten werden – so wie jede andere Anwendung.

4.2 AUTOMATISIERUNG DER BETRIEBSSYSTEM- UND ANWENDUNGSBEREITSTELLUNG

Die Automatisierung der Bereitstellung von Betriebssystemen und Anwendungssoftware bietet viele Vorteile, einschließlich:

- Verringerung des Workloads für IT-Support-Mitarbeiter
- Reduzierung der Kosten für Upgrades und Neuinstallationen
- weniger Zeitaufwand für die Umsetzung einer Initiative
- Sicherstellung von Konsistenz, damit alle Benutzer innerhalb kurzer Zeit Upgrades erhalten
- Beseitigung von Fehlern, die zu Inkonsistenzen innerhalb der Konfigurationen führen

Anstatt auf jedem einzelnen Computer die notwendige Software zu installieren, bereitet der IT-Administrator einen Master-Computer vor und kopiert das Image dieses Computers, sodass die verbleibenden Nodes geklont werden können. So beinhalten sie dasselbe „Golden Image“ aller Betriebssysteme und der gesamten Anwendungssoftware.

4.3 BESEITIGUNG VON SOFTWARE-SCHWACHSTELLEN

Wenn es um die Beseitigung von Schwachstellen und die Verwaltung der Patch- und Update-Bereitstellung geht, ist ein präventiver Sicherheitsansatz unumgänglich. Zuerst ist es notwendig, ein Audit Ihrer IT-Infrastruktur durchzuführen, damit jede Schwachstelle im Betriebssystem und in den Anwendungen sämtlicher Computer identifiziert werden kann. Anschließend sollten Sie die Bereitstellung von Patches priorisieren, damit die Schwachstellen mit dem größten Risiko zuerst beseitigt werden.

Nachdem Sie festgestellt haben, welche Software aktualisiert werden muss und warum, müssen Sie Folgendes in Erfahrung bringen:

- die Art der Schwachstelle
- die Gefahrenwertung der Schwachstelle – niedrig, mittel, hoch oder kritisch
- welche Software-Versionen betroffen sind
- welche Workstations, Server oder anderen Geräte betroffen sind
- wann die Schwachstelle erkannt wurde
- ob ein Patch vom Hersteller verfügbar ist

Angesichts Ihrer zahlreichen weiteren Aufgaben ist es wichtig, dass alle diese Informationen in einem eindeutigen, genauen Bericht dargestellt werden, der Ihnen die Entscheidung bezüglich des nächsten Schritts erleichtert. Zusätzlich können Sie dank der Echtzeit-Transparenz Ihrer gesamten IT-Umgebung sicherstellen, dass die Software für Ihr gesamtes Netzwerk aktualisiert wird.

Mit diesen Informationen können Sie die Strategie zur Patch-Bereitstellung planen:

- Da die Schwachstellen auf der Grundlage ihres Schweregrads bewertet werden, ist es einfacher, sich sofort den Elementen mit hohem Risiko zuzuwenden. So können weniger dringende Updates außerhalb der normalen Arbeitszeiten implementiert werden, wenn die Netzwerkressourcen weniger beansprucht werden.

- Für besonders vertrauliche Anwendungen sollten Sie regelmäßige Updates und Patches ausführen.

4.4 KONTROLLE DES ZUGRIFFS AUF DAS UNTERNEHMENSNETZWERK

Da Besucher Mobilgeräte und Laptops und Mitarbeiter eigene Geräte mit in das Unternehmen bringen, umfassen effektive Systems-Management-Lösungen flexible Tools, die es den IT-Mitarbeitern ermöglichen, Richtlinien hinsichtlich folgender Punkte festzulegen:

- Welche Geräte sind für den Zugriff auf das Netzwerk berechtigt?
- Worauf genau können einzelne Geräte oder Gerätegruppen im Netzwerk zugreifen? (Besucher des Unternehmens benötigen z. B. möglicherweise nur Internetzugriff und keinen Zugriff auf Unternehmenssysteme)

4.5 REDUZIERUNG DER UNÜBERSICHTLICHKEIT MEHRERER VERWALTUNGSKONSOLEN

Da Unternehmen viele verschiedene IT-Verwaltungsaufgaben zu bewältigen haben, führen die meisten Unternehmen einzelne Anwendungen für fast jeden einzelnen IT-Verwaltungsprozess aus, den sie benötigen. Diese Vorgehensweise ist sowohl umständlich als auch ineffizient:

- Das IT-Team muss Zeit aufwenden, um sich mit den verschiedenen Verwaltungskonsolen der Anwendungen vertraut zu machen.

- Wenn der IT-Support-Mitarbeiter im Laufe des Arbeitstages von einer Verwaltungskonsole zur nächsten wechselt, muss er sich auch mental auf die Konventionen, Schlüsselsequenzen und Terminologie einstellen, die auf die bestimmte Konsole zutreffen, die er gerade verwendet. Dieser wiederholte Wechsel zwischen den verschiedenen Konsolen – jede Konsole hat dabei ein anderes Design und eine andere Oberfläche und verwendet unterschiedliche Konventionen – kann zu Betriebsfehlern führen … und diese Fehler können wiederum die Effizienz und vor allem die Sicherheit beeinträchtigen.

Im Gegensatz hierzu bieten Lösungen, die den IT-Mitarbeitern die Verwendung einer zentralen Konsole für die Überwachung und Verwaltung ermöglichen, unter anderem folgende entscheidende Vorteile:

- Hardware-Bestandsaufnahme
- Software-Bestandsaufnahme
- Bereitstellung von Betriebssystemen und Anwendungen
- Vulnerability Scanning – zur Identifizierung von Sicherheitslücken innerhalb von Betriebssystemen und Anwendungen
- Patch-Bereitstellung – zur Beseitigung von Sicherheitslücken
- Zugriffssteuerung

Eine zentrale Konsole kann den Zeitaufwand für die Durchführung von Routineaufgaben bei der IT-Verwaltung sowie das Auftreten von Fehlern erheblich verringern.

Kaspersky Systems Management

5.0

5.1 BESSERER ÜBERBLICK ÜBER IHR GESAMTES NETZWERK

Hardware-Bestandsaufnahme

Kaspersky Systems Management führt nicht nur automatisch eine Bestandsaufnahme der gesamten Hardware in der IT-Umgebung Ihres Unternehmens durch, sondern erkennt zudem automatisch jedes neue Gerät, das in Ihrem Netzwerk erscheint.

Der IT-Administrator wird über E-Mail, Ereignisse und Berichte über ein neues Gerät informiert. Somit profitiert das IT-Team von den Vorteilen des transparenten Überblicks über die gesamte Hardware.

Software-Bestandsaufnahme und Lizenzkontrolle

Eine automatische Bestandsaufnahme der gesamten Software auf dem Netzwerk trägt dazu bei, dass Administratoren über die Verwendung illegaler und ungewünschter Software informiert werden. So können der Start von Anwendungen automatisch blockiert und Benutzer darauf hingewiesen werden, dass sie gegen die Unternehmensrichtlinien verstoßen haben.

Da die Software-Bestandsaufnahme Informationen zu den erworbenen Lizenzen (für jede Anwendung) enthält, können die IT-Mitarbeiter die Nutzung von Anwendungen verfolgen, um:

- die Verwendung unlizenzierter Software zu verhindern
- Lizenzen vor ihrem Ablauf zu erneuern
- Möglichkeiten zur Verringerung der Anzahl an Softwarelizenzen zu ermitteln

Mit Kaspersky Systems Management ist es einfacher, zu verstehen:

- welche Software das Unternehmen besitzt
- welchen Anteil davon das Unternehmen verwendet
- welchen Anteil davon das Unternehmen benötigt

Flexibles Reporting

Die Administratoren können eine Reihe von Berichten erstellen, dank denen Sie eine noch größere Kontrolle über die Software erlangen, die auf dem Netzwerk verwendet wird. Darüber hinaus informieren zentralisierte Berichte die Administratoren über den Verwendungsverlauf jeder Anwendung, sodass die IT-Mitarbeiter die Nutzung von Software überwachen und kontrollieren können.

5.2 BEREITSTELLUNG VON BETRIEBSSYSTEMEN

Automatisierte Bereitstellung

Kaspersky Systems Management automatisiert die Erstellung und das Klonen von Computer-Images, um Zeit zu sparen und die Bereitstellung von Betriebssystem-Images zu optimieren.

- Alle von Ihnen erstellten Images werden in einer speziellen Bestandsaufnahme erfasst, auf welche die Client-Computer während des Bereitstellungsprozesses zugreifen.

- Die Bereitstellung von Images auf Client-Workstations kann entweder über PXE (Preboot eXecution Environment)-Server, die zuvor in Ihrem Netzwerk eingesetzt wurden, oder mit den eigenen Funktionen von Kaspersky Systems Management ausgeführt werden.

5.3 BEREITSTELLUNG VON ANWENDUNGEN

Cloud-basierte Updates

Mit Kaspersky Systems Management können Sie zwischen manueller und planmäßiger Bereitstellung von Anwendungen wählen, wobei ein Hintergrund-Installationsmodus unterstützt wird.

Neben standardmäßigen MSI-Paketen unterstützt Kaspersky Systems Management auch die Bereitstellung durch andere Programmdateien, einschließlich EXE, BAT und CMD.

Unter Verwendung des Cloud-basierten Kaspersky Security Network verfolgt Kaspersky Systems Management automatisch die neuesten verfügbaren Updates für viele der am häufigsten verwendeten Anwendungen, sodass Sie die aktuellste Version der Anwendungen verteilen können, die Sie bereitstellen möchten.

Remote-Funktionen

Bei Zweigstellen kann der Administrator einen Computer zum Update-Agent für die gesamte Zweigstelle bestimmen. Das Installationspaket wird auf den Update-Agent der Zweigstelle geladen und anschließend von diesem Update-Agent auf alle anderen Workstations der Zweigstelle verteilt. Diese Vorgehensweise kann den Netzwerk-Traffic erheblich reduzieren. Außerdem sorgt die Multicast Technology für weitere Einsparungen im Hinblick auf den Netzwerk-Traffic.

Mit Kaspersky Systems Management kann auch eine Remote-Verbindung zum Desktop eines beliebigen Client-Computers hergestellt werden. Diese Funktion ist während der Software-Bereitstellung besonders hilfreich.

5.4 VULNERABILITY ASSESSMENT

Mit Kaspersky Systems Management können Client-Workstations auf Schwachstellen im Windows-Betriebssystem und in den auf der Workstation ausgeführten Anwendungen überprüft werden. Vulnerability Scannings können für die Microsoft-Datenbank, Secunia und für die Schwachstellen-Datenbank von Kaspersky Lab durchgeführt werden.

Die Schwachstellen-Datenbank von Kaspersky Lab ist ein einzigartiges Element der Vulnerability-Assessment-Technologie. Basierend auf fortwährender Forschung des Kaspersky-Lab-Expertenteams wird die Datenbank unter Verwendung von Echtzeit-Schwachstellen und Malware-Informationen erstellt, die vom Cloud-basierten Kaspersky Security Network zusammengetragen werden.

5.5 PATCH MANAGEMENT

Automatisch oder auf Abruf

Patches können auf Abruf oder automatisch bereitgestellt werden. Somit kann der gesamte Ablauf – von der Schwachstellen-Erkennung bis zur Patch-Bereitstellung – zur Entlastung der IT-Mitarbeiter automatisiert werden.

Bei der Verteilung von Microsoft-Updates und -Hotfixes kann Kaspersky Systems Management als ein Windows Update (WSUS)-Server eingesetzt werden. Kaspersky Systems Management synchronisiert Daten regelmäßig mit Updates und Hotfixes (mithilfe von Microsoft Windows Update-Servern) und verteilt sie anschließend automatisch über die Windows Update-Services auf Client-Computern im gesamten Netzwerk – ohne Ihr IT-Team mit zusätzlichen Aufgaben zu belasten.

Bei Nicht-Microsoft-Software werden die Informationen über neue Software-Patches in Kaspersky Systems Management von den eigenen Kaspersky-Servern geladen. Falls ein spezielles Update nicht verfügbar ist, kann es manuell hinzugefügt und anschließend automatisch verteilt werden.

Reduzierung des Netzwerk-Traffics

Um den Netzwerk-Traffic zu reduzieren, kann die Patch-Bereitstellung auf Zeiten nach Geschäftsschluss verschoben werden, wobei ein Update-Agent die Bereitstellung der Patches in Zweigstellen unter Verwendung der Multicast-Technologie übernehmen kann.

Detailliertes Reporting (einschließlich Informationen darüber, welche Workstations am verwundbarsten sind und warum) unterstützt die IT-Administratoren bei der Planung und verschafft ihnen einen Überblick über den Status aller Softwarelösungen im gesamten Unternehmensnetzwerk.

5.6 NETZWERKZUGRIFFSKONTROLLE (NAC)

Mit Kaspersky Systems Management sind Administratoren in der Lage, Zugriffsrichtlinien zu erstellen und einzelne Geräte oder Gerätegruppen zu klassifizieren, um Zugriff auf das Unternehmensnetzwerk zu gestatten oder zu verweigern. Beispiel:

- Unternehmenseigene oder persönliche Mitarbeitergeräte können:
  - automatisch Zugriff auf das Netzwerk erhalten – unter der Voraussetzung, dass die Geräte über die aktuellsten Updates und Sicherheitspatches verfügen.
  - mit den notwendigen Softwarelösungen, Updates und Patches aktualisiert werden, bevor ein Zugriff auf das Netzwerk gestattet wird.

- Neue Geräte werden automatisch als „Gästegeräte“ erkannt und auf das Gastportal zur Autorisierung weitergeleitet, bevor ihnen der Zugriff auf das Internet oder das Unternehmensnetzwerk gestattet wird.

- Mithilfe von Sicherheitsrichtlinien werden sämtliche Zugriffe über infizierte Geräte oder Geräte mit verbotener Software blockiert.

Fazit

6.0

6.1 DIE HERAUSFORDERUNGEN

Die komplexen IT-Netzwerke stellen für die meisten Unternehmen große Herausforderungen für Betrieb und Sicherheit dar:

- Die Vielfalt der Endpoints und Geräte im Unternehmensnetzwerk nimmt weiterhin zu.
- Die Bandbreite und Anzahl der routinemäßigen Systems-Management-Aufgaben ist signifikant gestiegen.
- IT-Mitarbeitern fällt es schwer, den Überblick über ihr Netzwerk zu behalten.
- Das Beheben von Schwachstellen im Betriebssystem und in den Anwendungen kann schwierig und zeitaufwendig sein.
- Die Einführung von Mobilgeräten und BYOD führt zu:
  – einer Steigerung des Workloads durch Systems-Management-Aufgaben
  – neuen Sicherheitsproblemen

Außerdem:

- werden Schadsoftware und Cyberkriminelle immer ausgeklügelter und raffinierter.
- laden einige Benutzer gewohnheitsmäßig Software herunter, unabhängig davon, ob sie Schadsoftware enthält oder illegal ist.
- muss der Zugriff auf das Unternehmensnetzwerk streng kontrolliert werden – insbesondere bei Gastgeräten.

6.2 DIE LÖSUNGEN

Viele Hersteller haben Produkte entwickelt, die den IT-Mitarbeitern bei der Verwaltung ihrer IT-Infrastruktur helfen. Doch nicht alle Produkte decken die gesamte Bandbreite der Aufgaben ab, mit denen sich IT-Administratoren Tag für Tag auseinandersetzen müssen. In vielen Fällen führte dies bei den Unternehmen zur Verwendung mehrerer Produkte, die jeweils eine eigene Verwaltungskonsole aufweisen. Diese Abhängigkeit von mehreren Produkten steigert die Komplexität und kann zu Sicherheitslücken führen.

6.3 DIE KASPERSKY-LAB-LÖSUNG

Mit Kaspersky Systems Management sind IT-Teams in der Lage, ihren Arbeitstag und das Unternehmensbudget optimal zu nutzen. Die Lösung von Kaspersky Lab ist benutzerfreundlich und:

- vereinfacht und automatisiert einen Großteil der täglichen Systems-Management-Aufgaben.
- bietet einen Überblick über die gesamte Hardware und Software im Unternehmensnetzwerk.
- ermöglicht Remote-Bereitstellung von Software und Remote-Troubleshooting.

… und darüber hinaus werden alle Systems-Management-Funktionen über eine einheitliche Verwaltungskonsole gesteuert.

Kaspersky Systems Management ist in folgenden Produkten enthalten:

- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business

… sowie als eigenständige Targeted-Security-Lösung erhältlich.

Über Kaspersky Lab
Kaspersky Lab ist der weltweit größte Hersteller von Endpoint-Security-Lösungen in privater Hand. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer. In seiner 15-jährigen Firmengeschichte hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet Einzelverbrauchern ebenso wie Unternehmen jeder Größenordnung wirksame Lösungen für die Datensicherheit. Derzeit ist das Unternehmen weltweit in fast 200 Ländern und Regionen tätig und sorgt bei über 300 Millionen Benutzern für den Schutz des Datenbestands.

Weitere Informationen erhalten Sie unter: www.kaspersky.de/business

j2laa/Stand: November 2013