KASPERSKY lab

BEST PRACTICES

Systems Management

www.kaspersky.de

LEITFADEN ZU BEST PRACTICES BEIM SYSTEMS MANAGEMENT

Mehr Sicherheit und einfachere Verwaltung durch zentrale IT-Verwaltungstools.

Nicht gepatchte Schwachstellen in gängigen Programmen sind eine der größten Bedrohungen für die IT-Sicherheit in Unternehmen. Dieses Risiko wird noch durch die ständig steigende IT-Komplexität erhöht. Wenn Sie keinen Überblick über Ihre Ressourcen haben, wie können Sie diese dann schützen? In diesem Best-Practices-Leitfaden erfahren Sie, wie es geht ...

Die zunehmende Vielfalt an Plattformen, Geräten, Software und anderen Programmen macht IT-Managern das Leben schwer, erhöht die Komplexität und führt zu einer zusätzlichen Belastung der vorhandenen Ressourcen. Aber nicht nur Geräte und Software werden immer vielfältiger: Kaspersky Lab entdeckt täglich 350.000 neue Bedrohungen, von denen viele speziell darauf ausgelegt sind, Schwachstellen in beliebten Unternehmensprogrammen auszunutzen. So verschaffen sich Cyberkriminelle Zugriff auf vertrauliche Daten, stehlen Geld oder Daten, oder blockieren Ihre Systeme, bis ein Lösegeld gezahlt wird.

Dieses hohe Ausmaß an Komplexität unterminiert die Sicherheit, die betriebliche Effizienz und das Wachstumspotenzial. Es fördert die Fehleranfälligkeit und beschränkt die Möglichkeiten zum Umgang mit Neuerungen. Ein effektives Systems Management kann viel ausmachen, wenn es darum geht, bewährte Ansätze (Best Practices) zu fördern, durch die die IT-Ressourcen optimal genutzt und zugleich eine mehrstufige Sicherheitsstrategie unterstützt wird, die dem im ständigen Wandel begriffenen Bedrohungspanorama gewachsen ist. Hier erfahren Sie, wie dies möglich ist.

1. ZENTRALISIERUNG, AUTOMATISIERUNG, KONTROLLE

Es gibt einige grundlegende Schritte, die jedes Unternehmen ergreifen kann, um eine optimale Leistungsfähigkeit der IT-Abteilung zu gewährleisten, die Kosten zu reduzieren, die Service-Levels zu verbessern und flexibler zu werden:

- Standardisierung der Desktop-/Laptop-Strategie und Beschränkung der Anzahl an Images auf ein Minimum
- Verwaltung der Einstellungen und Konfigurationen für PCs, Laptops und mobile Endgeräte von einer zentralen Stelle aus
- Einführung und Unterhalt umfassender Sicherheitstools
- Automatisierung von Hardware- und Software-Beständen, Softwarebereitstellung, Vulnerability Scanning, Patch Management und anderen Routineaufgaben
- Troubleshooting und Software-Installation per Fernzugriff, auch an Remote-Standorten
- Implementieren einer rollenbasierten Zugriffskontrolle mit Anpassung der zentralen Konsolenansicht nach Rollen und Berechtigungen
- Unternehmensintegration mit SIEM-Systemen zur Minimierung von Administrationsaufgaben und -Tools bei vereinfachtem Reporting

Die Automatisierung wichtiger Routineaufgaben – sei es im Bereich der Sicherheit oder des Troubleshooting – ermöglicht es IT-Administratoren, nicht mehr immer nur Gefahrenherde zu löschen, sondern vielmehr strategisch zu planen, sodass die IT-Richtlinien den betriebswirtschaftlichen Anforderungen entsprechen und diese unterstützen. Automatisierung reduziert auch die bei der Ausführung manueller Prozesse in komplexen Systemen notorische Fehleranfälligkeit.

2. EFFEKTIVE KONTROLLE UND UMSETZUNG BEIM PROVISIONING ÜBER IMAGES

Jahr für Jahr werden neue Hardware und Programme sowie regelmäßige Updates für Software, Betriebssysteme, Patches und Programmupdates bereitgestellt. Das ist zeitaufwändig, teuer und mit wachsendem Bestand zunehmend komplex.

Die Vorbereitung und Verwaltung eines „Golden Image" – des voll optimierten Master-Images (oder Klons) eines vollständigen Desktops – spart viel Zeit und Ressourcen. Diese perfekte Systemkonfiguration wird in einem speziellen Verzeichnis im Netzwerk gespeichert und kann nach Bedarf bereitgestellt werden. In Unternehmen, die auf ein neues Betriebssystem umsteigen, können die Steuerung, das Bestandsverzeichnis und das Deployment solcher Images automatisiert werden. Der wahre Nutzen besteht dabei in der Möglichkeit, das Deployment auch außerhalb der Bürozeiten mithilfe der Wake-on-LAN-Technologie durchzuführen. Dies bedeutet Zeiteinsparungen und weniger Unterbrechungen für die Endbenutzer.

Durch ein effektives Deployment über Images wird gewährleistet, dass die Betriebssysteme mit optimalen Sicherheitseinstellungen installiert werden. Vergessen Sie dabei aber nicht die Sicherheit der Images selbst – sorgen Sie für Sicherung und Kontrolle des Zugriffs auf alle Images durch:

- Starke Passwörter
- Schutz durch Zertifikate zur Client-Authentifizierung
- Zugangskontrollen zum Schutz des „Referenzcomputers", mit dem das Betriebssystem für das so genannte „Golden Image" erfasst wird. Auf diese Weise wird schädliche Software nicht versehentlich in das Image aufgenommen.
- Speichern des Images an einem sicheren Ort, an dem es nicht kompromittiert werden kann
- Pflege von Sicherheitspatches und -Updates auf dem Referenzsystem, damit alle neu implementierten Systeme optimal gesichert sind

Effektives Image-Management im Hinblick auf die Standardisierung des gewählten Betriebssystems auf allen Geräten im Netzwerk Auswahl einer Lösung, die eine Automatisierung und zentrale Verwaltung von Images ermöglicht Noch etwas praktischer wird es, wenn Sie sich für eine Lösung entscheiden, mit der die Daten der Endbenutzer automatisch gespeichert werden.

Zusätzliche Kontrolle und Flexibilität bieten Lösungen, bei denen die BS-Images nach der Erstellung bearbeitet werden können. UEFI-Unterstützung, die Fähigkeit, mit Windows PE ein Boot-Flashlaufwerk zu erstellen und die Option, ein BS-Image aus einem Distributionspaket zu importieren, sorgen für verbesserte Bedienbarkeit und noch mehr Effizienz.

3. OPTIMIERUNG DER INSTALLATION UND DES DEPLOYMENTS VON SOFTWARE

Softwareupdates. Softwareupdates betreffen sowohl die Installation neuer Software als auch die Updates vorhandener Software. Ein manuelles Update jedes einzelnen Computers im Unternehmen würde Ihnen keine Zeit für andere Aufgaben lassen. Das Software-Deployment kann so automatisiert und optimiert werden, dass es sich minimal auf das Netzwerk auswirkt und für die Endbenutzer vollkommen transparent ist. Tipps zu Best Practices:

- Halten Sie Ihre Deployment-Optionen möglichst offen. Wählen Sie dazu eine Lösung, die nicht nur standardmäßige MSI-Pakete unterstützt, sondern auch andere ausführbare Dateitypen wie exe, bat oder cmd.
- Seien Sie flexibel im Hinblick auf das Deployment: Optionen, mit denen sowohl bedarfsorientierte als auch planmäßige Deployments möglich sind, geben Ihnen mehr Flexibilität. Planmäßige Deployments sind besonders dann sehr nützlich, wenn es sich um große Pakete handelt – das Deployment kann dann außerhalb der Bürozeiten stattfinden, wenn das Netzwerk kaum belastet ist. Kaspersky Systems Management ermöglicht die automatische Installation von mehr als 100 beliebten Programmen, die über das Kaspersky Security Network identifiziert werden. Diese können bei Bedarf nach Geschäftsschluss installiert werden.
- Wählen Sie eine Lösung, mit der Remote-Deployments von einer einzigen Konsole aus möglich sind. Dank Multicast-Technologie führt dies zu weniger Datenverkehr mit Zweigstellen.
- Möglichkeit der Modifizierung von Installationspaketen und somit erhöhte Flexibilität – Sie können Installationsparameter selbst festlegen, um die Kompatibilität mit Ihren Richtlinien zu gewährleisten.
- Entscheiden Sie sich für eine Lösung mit Troubleshooting per Fernzugriff: Das Troubleshooting per Fernzugriff spart Zeit und Mühe, und Sie können die Probleme schnell und direkt lösen. Eine weitere Sicherheitsebene für Remote-Sitzungen wird durch Benutzerberechtigungen und Sitzungsprotokolle/Sitzungs-Audits gewährleistet.

Durch Automatisierung und Optimierung von Software-Deployment und -Updates können Sie sicherstellen, dass Best Practice-Verfahren in Ihrem Unternehmen zum Standard werden. In Szenarien mit mehreren Standorten oder Systemen lässt sich durch die Steuerung des Deployments von Software die Komplexität und Fehleranfälligkeit reduzieren, die normalerweise mit repetitiven manuellen Prozessen einhergeht.

4. UMFASSENDE KONTROLLE ÜBER IHRE RESSOURCEN

Ein wichtiger Bestandteil einer effektiven IT-Sicherheit besteht darin, einen guten Überblick über alle in Ihrem Netzwerk verwendeten Geräte und Programme zu haben. Auf diese Weise erkennen Sie, an welchen Stellen Sie eingreifen müssen.

Zu den Best Practices gehört ein absolut transparenter Einblick in die gesamte Hardware und Software in Ihrem Netzwerk. Dabei spielt auch die automatische Geräteerkennung eine wichtige Rolle, mit deren Hilfe Sie sicherstellen können, dass alle Richtlinien eingehalten werden. Weitere Schritte umfassen u. a. Folgendes:

- **Software-Bestandsaufnahme**: Automatisieren Sie die Bestandsaufnahme, um sich umfassende Transparenz und Kontrolle zu verschaffen. Mithilfe dieser Liste können Administratoren die Softwarenutzung kontrollieren, Endbenutzer in Kenntnis setzen, wenn sie verbotene oder nicht lizenzierte Software ausführen, und bei Bedarf auch unerwünschte Programme ganz sperren. Management und Kontrolle von Softwarelizenzen im gesamten Unternehmen ist eine der einfachsten Maßnahmen, um Ausgaben für unnötige Software zu vermeiden.

- **Verfolgen von Hardware-Beständen und Geräten**: Ermöglicht Ihnen eine umfassende Ansicht aller im Netzwerk verwendeten Geräte. Sie können die Erkennung neuer Hardwarekomponenten und die Benachrichtigung darüber automatisieren, um das Verzeichnis auf dem aktuellen Stand zu halten, alle Änderungen zu überwachen und nicht mehr verwendete Geräte auszurangieren. Die Netzwerkzugriffskontrolle (NAC) bedeutet, dass Gastgeräte auf sichere Weise im Netzwerk hinzugefügt und blockiert werden können, wenn sie die Sicherheitsanforderungen nicht erfüllen oder anderen Richtlinien unterliegen.

- **Lizenzplanung**: Nach erfolgter Bestandsaufnahme kann die Lizenznutzung nach den Anforderungen der jeweiligen Abteilung einfacher kontrolliert werden. Beispielsweise könnte sich herausstellen, dass Benutzer in der Buchhaltung über unnötige Lizenzen für eine Grafikdesign-Software verfügen, die Sie anderweitig bereitstellen oder ganz auslaufen lassen können. Dank eines umfassenden Überblicks über alle Lizenzen bleiben Sie beim Lizenzmanagement außerdem immer auf dem neuesten Stand.

- **Reporting**: Zentralisierte Berichte liefern umfassende Informationen über alle in Ihrem Netzwerk verwendeten Software- und Hardwarekomponenten, einschließlich ihrer Nutzung in der Vergangenheit. Dank der Erkenntnisse aus diesen Berichten wird für Gruppen auf allen Ebenen eine effektive Nutzungskontrolle ermöglicht.

Die Lizenzkontrolle ist bisweilen eine zeitaufwändige, oftmals komplexe Aufgabe. Ihre Automatisierung spart nicht nur Zeit, sondern gewährleistet auch, dass das Unternehmen wichtige Best Practices befolgt: Einhaltung von Richtlinien, kostengünstige Software- und Hardwareverwaltung und umfassende Transparenz aller Aktivitäten im Netzwerk. Viele Erfolge mit wenig Aufwand.

5. FORTSCHRITTLICHES VULNERABILITY ASSESSMENT UND PATCH MANAGEMENT

Die Verwaltung und Verteilung von Software-Updates bei gleichzeitiger ständiger Überprüfung auf potenzielle Schwachstellen ist eine der wichtigsten, anspruchsvollsten und ressourcenintensivsten Aufgaben der IT-Abteilung.

Angesichts der sich ständig wandelnden Bedrohungen, mit denen Cyberkriminelle Systeme immer wieder nach Schwachstellen durchkämmen, ist es für IT-Administratoren von entscheidender Bedeutung, Lücken zu erkennen und zu schließen, bevor sie ausgenutzt werden.

Erzielt wird dies durch Vulnerability Assessment. Dabei werden Geräte und Software im Netzwerk auf Schwachstellen gescannt, die möglicherweise ausgenutzt werden könnten. Ist eine solche Lücke erst einmal erkannt, kann sie mithilfe des Patch Managements geschlossen werden, indem auf allen Rechnern im Netzwerk die nötigen Updates installiert bzw. die betroffenen Reparaturen vorgenommen werden.

Mit einer Kombination aus effektivem Patch Management und Vulnerability Assessment sind Sie Cyberkriminellen immer einen Schritt voraus. Hier erfahren Sie, wie:

- **Immer auf dem neuesten Stand sein**: Veraltete Software, ob auf Servern oder Workstations, bedeutet immer ein Risiko für das Unternehmen. Automatisierte Scanabläufe ermöglichen eine rasche Erkennung und Priorisierung von Schwachstellen.

Das Kaspersky Systems Management bietet eine automatische Bereitstellung von Patches und Updates innerhalb kürzester Zeit für Software von Microsoft und anderen Anbietern. Dank Statusinformationen zur Patch-Installation erhalten Administratoren noch größere Kontrolle. Weniger wichtige Problemlösungen können auf Zeiten nach Geschäftsschluss verschoben werden. Durch Wake-on-LAN-Befehle funktioniert dies sogar bei ausgeschalteten Computern. Die Multicast-Übermittlungstechnik ermöglicht die lokale Verteilung von Patches und Updates in Zweigstellen und reduziert so die Anforderungen an die Bandbreite.

Durch die Automatisierung der Bereitstellung von Softwareaktualisierungen und der damit einhergehenden Verwaltungsaufgaben können Sie durch die Bereitstellung, Überprüfung und Entfernung von Patches bedingte Betriebsunterbrechungen minimieren.

- **Berichte**: Anhand von Berichten zu Scans erhalten Sie weitere Einblicke in die IT-Sicherheit des Unternehmens. Untersuchen und melden Sie potentielle Schwachstellen, verfolgen Sie alle Änderungen und verschaffen Sie sich einen detaillierten Einblick in den Patch-Status aller Geräte und Systeme im Netzwerk.

Durch gezielte Angriffe, ausgeklügelte nachhaltige Bedrohungen, automatisierte Angriffe und Zero-Day-Schwachstellen wird die Zeitspanne zwischen der Entdeckung einer Schwachstelle und deren Ausnutzung durch ein Exploit verkürzt. Wenn Administratoren regelmäßige Assessments und die Anwendung von Patches automatisieren und planen, können sie die entsprechenden Prozesse ohne Einbußen bei der Effektivität rationalisieren.

6. ZENTRALES MANAGEMENT UND ROLLENBASIERTE ZUGRIFFSKONTROLLE

Durch Zentralisierung und Automatisierung von grundlegenden Sicherheits-, Konfigurations- und Verwaltungsabläufen, z. B. Vulnerability Assessment, Patch- und Update-Bereitstellung, Bestandsverwaltung und Anwendungs-Rollouts, sparen IT-Administration nicht nur Zeit, sie tragen auch zur Optimierung der Sicherheit bei.

Eine einzige integrierte Verwaltungskonsole, das Kaspersky Security Center, ermöglicht die Verwaltung für Desktops, Mobilgeräte sowie alle anderen physischen und virtualisierten Endpoints im gesamten Netzwerk über eine einzige Benutzeroberfläche. In komplexen Unternehmensnetzwerken sorgt die rollenbasierte Zugriffskontrolle (RBAC) dafür, dass Konsolenansichten und -funktionen je nach Rolle und Berechtigungen des Administrators angepasst werden können. Ein bestimmter Administrator ist beispielsweise in der Lage, alle Bereiche des IT-Sicherheitsmanagements auf der Konsole anzuzeigen, aber nur die Funktionen für Vulnerability Assessment und Patch Management zu bearbeiten.

7. SIEM-INTEGRATION FÜR UNTERNEHMENSUMGEBUNGEN

Viele Organisationen, vor allem größere Unternehmen, verwenden Security Information and Event Management (SIEM)-Systeme, um Protokolle und andere sicherheitsbezogene Daten für Analysen zu erfassen. Sicherheitssysteme, die Berichte für führende SIEM-Systeme erstellen können, erleichtern die Arbeit und die Tool-Anforderungen für den Administrator und vereinfachen gleichzeitig den Reporting-Prozess im Unternehmen.

Kaspersky Systems Management kann in IBM QRadar und HP ArcSight integriert werden und bietet so Funktionen zur Ereignisübermittlung.

ZU GUTER LETZT

Schwachstellen in Software-Programmen werden immer mehr zum Schwerpunkt für gut geplante, gezielte Angriffe auf Unternehmen aller Größen. Ein effektives Programm- und Patch Management in Verbindung mit Vulnerability Assessment und anderen Funktionen des Systems Management ermöglichen einen integrierten Ansatz für die IT-Sicherheit in Unternehmen.

Kaspersky Systems Management ist eine verwaltete Komponente des Kaspersky Security Center. Zur Automatisierung von IT-Routineaufgaben wird jede Funktion über diese zentrale Konsole unter Verwendung einheitlicher, intuitiver Befehle und Benutzeroberflächen verwaltet. So erzielen Sie eine optimale Sicherheit für Ihr Unternehmen.


Twitter.com/
Kaspersky_DACH


Facebook.com/
Kaspersky.Lab.DACH


Youtube.com/
KasperskyLabCE

Kaspersky Lab ZAO, Moskau,
Russland
www.kaspersky.de

Informationen zur
Internetsicherheit:
www.viruslist.de

Informationen zu Partnern in
Ihrer Nähe finden Sie hier:
www.kaspersky.com/buyoffline

KASPERSKY lab