Patchen für das Rechenzentrum

Tägliche Nachrichten über Anfälligkeiten und andere Bedrohungen sowie die Angst vor dem Unbekannten oder Opfer dieser Bedrohungen zu werden, halten Unternehmen in Atem. Sie tun alles, was in Ihrer Macht steht, um die Software auf den Systemen Ihrer Benutzer auf dem neuesten Stand und in sicherem Zustand zu halten. Aber wie steht es um die Server in Ihren Rechenzentren? In der heutigen Zeit, in der Hacker auf bereits geschriebenen Exploit-Code zugreifen können, brauchen Unternehmen ein wirksames Mittel, um ihre Server im Rechenzentrum zu schützen, ohne die IT-Ressourcen zu erschöpfen.

Patchmanagement muss Teil Ihrer Sicherheitspraktiken sein, damit Ihre Server stets abgesichert sind, Ihre Daten geschützt und verfügbar bleiben und der Ruf Ihres Unternehmens keinen Schaden nimmt. Sie müssen die neuesten Sicherheitspatches bereitstellen und gleichzeitig Zeit für die wesentlichen Unternehmensziele aufwenden.

Sie benötigen eine präzise Kontrolle und Berichterstattung über den gesamten Patchprozess: kontinuierliche Patcherkennung, Inventarisierung und Bereitstellung aller verfügbaren Patches in Ihrer Umgebung, und zwar nach einem auf Ihr Unternehmen zugeschnittenen Zeitplan.

Viele Unternehmen haben jedoch Schwierigkeiten, ihre Serversoftware stets mit den neuesten Softwareupdates für Betriebssysteme und Anwendungen von Drittanbietern, wie z. B. Microsoft Windows® und VMware vSphere® Hypervisor-Systeme, auf dem neuesten Stand zu halten. Das Problem ist, dass Rechenzentren mehr und andersartige Probleme für das Patchmanagement verursachen als Clientsysteme.

Erkennung und Problembehebung für das gesamte Rechenzentrum

Um ein hohes Maß an Patchgenauigkeit in Ihrer Umgebung zu erreichen, müssen Sie in der Lage sein, Systemscans für fehlende Patches leicht zu finden und Patches in Ihrer gesamten Umgebung richtlinienkonform bereitzustellen. Ohne eine klare Sicht auf Ihre Umgebung und die detaillierten Informationen, denen Sie entnehmen, welche Systeme am anfälligsten sind, ist es unmöglich, die Risiken für Ihr Unternehmen zu verstehen. Aufgrund der vielfältigen Konfigurationen in modernen Rechenzentren ist dies jedoch keine einfache Aufgabe.

Zeit- und Budgetbedenken im Zusammenhang mit einer virtuellen Rechenzentrumsumgebung, das Warten darauf, dass virtuelle Maschinen (VMs) hochgefahren, gepatcht und dann wieder heruntergefahren werden, haben zur Folge, dass manche virtuelle Umgebungen ignorieren und damit unnötige Risiken eingehen. Wenn man sich ausschließlich auf physische Server konzentriert, ist das Unternehmen exponiert und läuft Gefahr, bei einem Audit durchzufallen. Sie müssen in der Lage sein, Anfälligkeiten zu finden, nach fehlenden Patches zu scannen und diese Patches ohne Mühe auf physischen Servern und virtuellen Systemen bereitzustellen – ohne Unterbrechung von Server-Workloads oder des Geschäftsbetriebs. Und was die Compliance betrifft, dürfen Offlinesysteme nicht ignoriert werden. Sie müssen die Patch-Compliance sicherstellen und Softwareupdates bereitstellen, unabhängig davon, ob sich ein System im Netzwerk befindet oder nicht.

Schnellere Installation von Patches

Wie lange dauern derzeit die Softwareupdateprozesse in Ihrem Rechenzentrum? Monate oder Wochen? Wenn Sie Ihre Gefährdung verringern wollen, müssen Sie dies auf Tage und Stunden reduzieren.

In der Vergangenheit traten 50 % der Exploits innerhalb von zwei bis vier Wochen nach dem Release auf. Eine selbst auferlegte, 14-tägige Patch-SLA wird Ihnen einen Vorsprung vor der Mehrzahl der Exploits verschaffen. Manuelle Prozesse, Verfahren und mehrere Tools, die nicht Ihre gesamte Umgebung unterstützen können, erhöhen jedoch die Komplexität des Managements, ebenso wie die Zeit, die für die Erkennung, Definition und Bereitstellung von Softwareupdatepaketen und die Anwendung dieser kritischen Patches benötigt wird.

Unabhängig davon, ob Ihre Systeme online oder offline sind, müssen Sie Zeit sparen und Ihre knappen Ressourcen auf Aktivitäten lenken, die sich sofort und in hohem Maße bezahlt machen.

Es gibt viele Möglichkeiten, die Ihnen helfen, diese Zeit und dieses Risiko zu reduzieren. Beispielsweise sparen Patch-Vorlagen Zeit und reduzieren Ihr Risiko bei jedem neuen Server. Die Möglichkeit, alle Ihre Offline-VMs schnell zu finden und dann Offline-VMs und Vorlagen zu patchen, kann bis zu einer Stunde pro System sparen. Wenn Sie Offline-Images in einem konstanten Zustand der Einsatzbereitschaft halten, können Sie eine virtuelle Maschine bereitstellen,

ohne sich Gedanken darüber machen zu müssen, ob sie auf dem neuesten Stand ist.

Die wirkungsvollste Art, Zeit zu sparen, ist die Automatisierung jedes Teils des Server-Patchen-Prozesses. Denken Sie darüber nach, wie Sie derzeit mit Anfälligkeits-bewertungen von Anbietern umgehen. Das Auffinden aller Patches im Zusammenhang mit den Common Vulnerabilities and Exposures (CVEs) und das automatische Erstellen von Patchgruppen von Updates wäre eine enorme Zeitersparnis.

Schließlich müssen Sie die Compliance mit der Berichtspflicht vereinfachen, indem Sie die Masse von Information in Ihrer Umgebung reduzieren und bei entsprechendem Bedarf auf Daten zugreifen. Wenn Sie Führungskräften, Direktoren und Anwendungseigentümern die richtigen Daten an die Hand geben, sorgen Sie für Transparenz zur Unterstützung von Audits und stellen aktuelle Informationen über Ihre Sicherheitsaufstellung für eine effektive Entscheidungsfindung bereit.

Eine Patchmanagement-Checkliste

Die Automatisierung Ihres Patchmanagementprozesses von der Erkennung über die Bewertung bis hin zur Bereitstellung auf Ihren Workstations, physischen und virtuellen Servern, online und offline, trägt dazu bei, die Lieferzeit kritischer Sicherheitspatches zu verkürzen. Die folgende Tabelle gibt Aufschluss darüber, wonach Sie suchen müssen, um die richtige Patch-Lösung zu finden.

Ivanti kann helfen

Mit robustem und einfachem Patchen, das alle Ihre Anforderungen erfüllt, kann Ivanti zum Schutz Ihres Rechenzentrums beitragen. So sparen Sie Zeit und Geld und können sich weiterhin auf die Unterstützung von Kerngeschäftsinitiativen konzentrieren. Die Ivanti Tools sind in wenigen Minuten einsatzbereit und unterstützen Sie auf der Basis der von Ihnen definierten Richtlinien bei der automatischen Erkennung, Bewertung und Korrektur Ihrer Systeme im gesamten Rechenzentrum. Unsere Tools vereinfachen das Patchen über Ihre physischen und virtuellen Systeme hinweg. Finden Sie Workstations im Online- und Offline-Zustand, scannen Sie nach fehlenden Patches und stellen Sie diese bereit. Patchen Sie anschließend alles, angefangen beim Betriebssystem, über Anwendungen bis hin zu virtuellen Maschinen, virtuellen Vorlagen, ja sogar den ESXi-Hypervisor, dank der umfassenden VMware-Integration unseres Produkts.

Funktionalität	Beschreibung
Administration	Zentraler, rollenbasierter Verwaltungspunkt
Automatisierte Erkennung, Inventarisierung und automatisiertes Patchen	Schutz für Client-Workstations, physische Server, virtuelle Server, Hypervisoren und Vorlagen
Betriebssystem-Updates	Windows- und Linux-Betriebssysteme
Patchen von Anwendungen	Drittanbieter- und individuell angepasste Anwendungen
Automatisierung der Patchlistenerstellung über CVE	Importieren von Schwachstellenbewertungslisten beliebiger Anbieter
Patchinhalte	Zugriff auf einen extensiven Patchkatalog
Patchbereitstellung	Mit und ohne Agent und mit cloudbasiertem Agent
Rollback-Unterstützung	Fähigkeit, Snapshots vor dem Patchen zu erstellen
Automatisierungs-Enabler	APIs für Automatisierung und Orchestrierung
Kollaboration	Statusfreigabe und Überprüfung der Patch-Compliance mit anderen
Berichte	Echtzeit-Dashboards und anpassbare Berichte

Mehr erfahren www.ivanti.de +49 (0)699417570 contact@ivanti.de