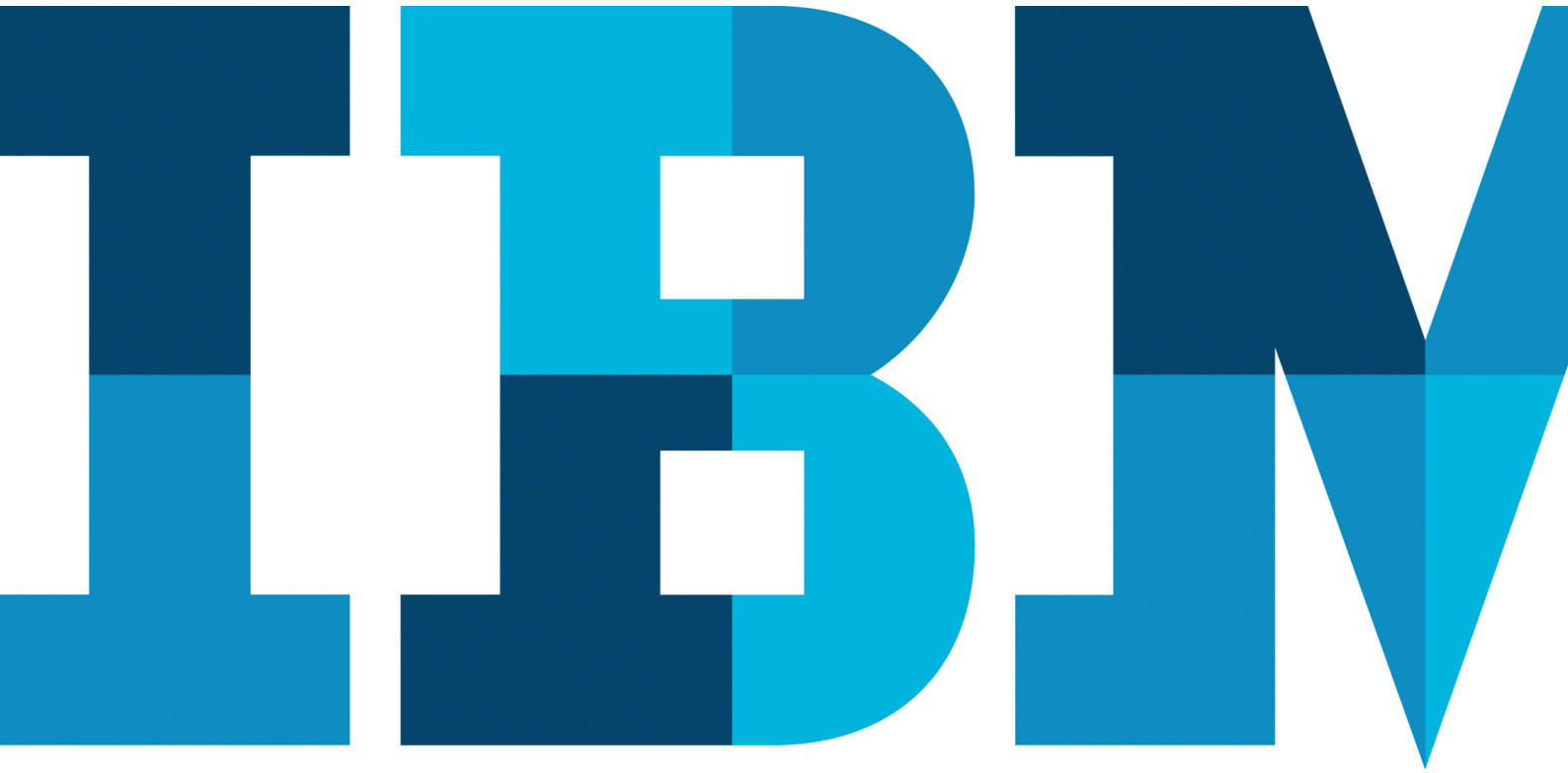
IBM Software
White Paper zum Thema Thought-Leadership

Februar 2011

Die Neuerfindung des Patch-Managements

IBM Tivoli Endpoint Manager verändert das Patchkonzept



Inhalt

Einführung

Malware befindet sich in einem Wettlauf gegen die Zeit. Es gilt, anfällige Computersysteme zu infizieren, bevor Softwareanbieter Patches zum Schutz der Systeme ihrer Kunden veröffentlichen und diese installiert werden. Wenn Malware den Wettlauf gewinnt, verlieren Unternehmen an Produktivität und riskieren den Verlust sensibler Daten, mögliche Schadensersatzklagen und behördliche Ordnungsstrafen. Das Ausmaß des Problems ist besorgniserregend: Der fortlaufende Kampf zwischen Hackern und Softwareunternehmen kostet die US-Wirtschaft schätzungsweise 266 Milliarden US-Dollar pro Jahr. Dies basiert auf Zahlen des Cyber Secure Institute, einer Interessensgruppe mit Sitz in Washington D.C.[1]

Als Reaktion auf diese Bedrohung geben immer mehr Softwareanbieter immer mehr Patches heraus, um den unzähligen Malwareangriffen etwas entgegensetzen zu können. Leider sind die meisten Unternehmen nicht gut genug ausgerüstet, um diese Flut an Patches zeit- und kosteneffizient zu implementieren. Aufgrund von organisatorischen Prozessen brauchen die meisten IT-Abteilungen Wochen oder gar Monate für die Implementierung von Patches in der gesamten IT-Umgebung. Einigen Schätzungen zufolge kann es sogar ganze vier Monate dauern, bis ein Unternehmen eine Patch-Compliance von 90 bis 95 Prozent erreicht. Bis es soweit ist wurden bereits zahllose weitere Patches herausgegeben. Das bedeutet, dass Unternehmen ständig einem hohen Risiko ausgesetzt sind und keine Compliance erreichen – eine Situation, die im Laufe der Zeit nur noch schlimmer wird.

Patch-Management war aufgrund seiner hohen Komplexität schon immer eine schwierige Angelegenheit. Ungeachtet der Risiken installieren manche Unternehmen aufgrund des dafür erforderlichen Zeit- und Arbeitsaufwands sowie einer möglichen Unterbrechung des Geschäftsbetriebs Patches nur sehr widerwillig. In einem Unternehmen mit einer heterogenen Hardware- und Softwareumgebung können die Aktualisierung der Flut an Patches und deren schnelle Implementierung IT-Mitarbeiter und IT-Budgets vor eine schwere Belastungsprobe stellen. Hier ist eine kosteneffiziente, auf Richtlinien basierende Lösung für das Patch-Management erforderlich, die schnell implementiert werden kann und Folgendes leistet:

- Eignet sich für alle Endgeräte in Unternehmen beliebiger Größe, einschließlich der größten
- Unterstützt mehrere Anbieter, Betriebssysteme, Anwendungen und Plattformen
- Funktioniert auch über langsame Verbindungen und unterstützt Einheiten außerhalb des firmeneigenen Netzwerks
- Minimiert die Belastung der IT-Mitarbeiter
- Wird in Echtzeit ausgeführt; Patches werden innerhalb von Stunden unternehmensweit implementiert

IBM Tivoli Endpoint Manager basierend auf BigFix-Technologie fasst die einzelnen Elemente des Patch-Managements in einer intelligenten, vereinfachten Lösung zusammen, die den Prozess für die Untersuchung, Beurteilung, Korrektur, Bestätigung, Umsetzung und Berichterstellung im Patchprozess beschleunigt und optimiert.

Das Mysterium Patch-Management

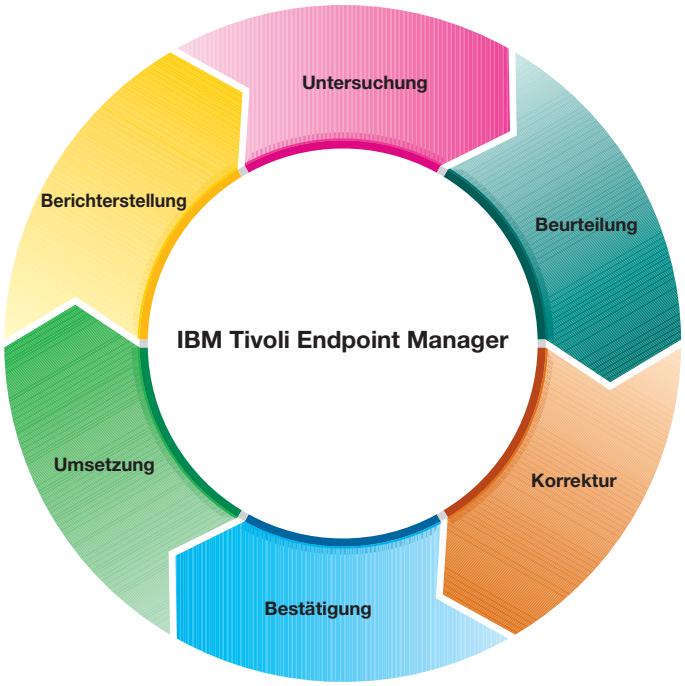
Patch-Management scheint so einfach zu sein, stellt Unternehmen jedoch vor eine der komplexesten und schwierigsten Aufgaben überhaupt. Bei effektivem Patch-Management geht es um mehr als nur darum, einen Systemadministrator zu beschäftigen, der Patches herausgibt oder sich auf Patchmechanismen von Softwareanbietern verlässt und hofft, dass die Patches dann erfolgreich angewendet werden (dies aber nie genau weiß). Das Mysterium Patch-Management wirft Fragen auf, die für Unternehmen möglicherweise schwierig oder gar unmöglich zu beantworten sind. Beispiel:

- Wie sollte ein Unternehmen kritische, außerhalb der Routinezyklen erscheinende Patches implementieren, die extrem dringlich sind?
- Wie können Systemadministratoren in einer Umgebung mit Hunderttausenden von Endgeräten mit den verschiedensten Betriebssystemen und Anwendungen den Überblick über Patches behalten?
- Wie sollen Systemadministratoren den Status standortunabhängiger Laptops und anderer mobiler Einheiten überwachen?
- Wie lange dauert der Patchprozess insgesamt und wie sollen Systemadministratoren bestätigen (und nachweisen), dass auf jedem Endgerät in der Infrastruktur ordnungsgemäß Patches installiert wurden und dass dies auch so bleibt?
- Wie können Systemadministratoren Patches schnell testen, bevor sie implementiert werden, und bei Problemen schnell rückgängig machen?
- Wie können Patches implementiert werden, ohne dass die Endbenutzer und deren Produktivität beeinträchtigt werden?

Aus Umfragen geht hervor, dass Patch-Management für Unternehmen eine der wichtigsten Prioritäten im Sicherheitsbereich darstellt. Diese Fragen zeigen jedoch auch auf, an welche Grenzen Unternehmen bei der Implementierung effektiver Verfahren für das Patch-Management stoßen. Neben einem Mangel an Transparenz und Mitarbeitern, möglichen Auswirkungen auf die Geschäftstätigkeit, Begrenzungen der Netzbandbreite, fehlendem Verwaltungskomfort, langen Korrekturzeiten, Problemen bei der Skalierbarkeit und der Abdeckung von verschiedenen Plattformen, Anwendungen anderer Hersteller und standortunabhängigen Endgeräten gibt es zahlreiche Hindernisse.

Glücklicherweise können diese Hindernisse überwunden werden. Tivoli Endpoint Manager überwindet diese Hindernisse mittels einer umfassenden Lösung, die speziell für dezentrale, heterogene Umgebungen entwickelt wurde. Mit dieser Lösung können Unternehmen den Status bezüglich Patch-Compliance endlich in Echtzeit und global über eine einzige Konsole analysieren, ändern, umsetzen und dokumentieren.

Prozess für das Patch-Management



Mit Tivoli Endpoint Manager wird das Patch-Management zu einem vollständig vereinheitlichten, geschlossenen Prozess, mit dem die Sicherheit verbessert und Einsparungen erzielt werden können.

Veränderung des Patch-Management-Konzepts

Es gibt zwar kein offizielles bewährtes Verfahren für das Patch-Management, das allgemeine Konzept umfasst jedoch einen geschlossenen Prozess mit sechs grundlegenden Schritten: Untersuchung, Beurteilung, Korrektur, Bestätigung, Umsetzung und Berichterstellung. Früher wurden viele dieser Schritte im Rahmen einzelner, nicht integrierter Technologien implementiert und es war praktisch unmöglich, einen geschlossenen Echtzeitprozess für das Patch-Management zu erstellen. Tivoli Endpoint Manager stellt all diese Schritte innerhalb eines vereinheitlichten, vollständig integrierten Prozesses bereit, der dazu beitragen kann, die Sicherheit zu verbessern und dabei Geld, Zeit und Ressourcen zu sparen.

Nachfolgend ein Vorher/Nachher-Vergleich zur Veränderung der Regeln des Patch-Managements durch diese Lösung.

Schritt 1: Untersuchung

Vorher: Der erste Schritt des Patch-Management-Prozesses ist die Identifizierung der verfügbaren Patches. Dies umfasst die Untersuchung der Patchverfügbarkeit über E-Mail-Nachrichten von Softwareanbietern, Popup-Benachrichtigungen von Anwendungen, Websites, Blogs und viele andere Quellen. Dieser Prozess muss für Hunderte von Patches der verschiedensten Anbieter von Betriebssystemen, Anwendungen und Malwareschutzlösungen wöchentlich oder gar täglich wiederholt werden. Eine Alternative – sich auf die automatischen Updates von Softwareanbietern zu verlassen – kann zu Fehlern mit schlimmen Folgen führen. Die automatische Anwendung von Patches ohne Test kann für Unternehmen ein hohes Risiko bedeuten. Das Unternehmen hat nämlich keine Kontrolle über den Zeitaufwand oder die Berichterstellung; und sich darauf zu verlassen, dass die Benutzer die Updates implementieren, ist risikoreich und wenig zuverlässig.

Besser ist es, wenn ein Patch-Management-Anbieter einen konsolidierten Datenstrom der häufigsten Patches bereitstellt, damit das Unternehmen nur die einzelnen Patchsendungen bewerten, diese auf Kompatibilität mit der Betriebsumgebung testen und dann im Rahmen stark differenzierbarer Richtlinien für bestimmte Maschinenprofile (bestimmte Patches können nur für die Endgeräte implementiert werden, für die sie erforderlich sind) implementieren muss. Das Problem dieses Konzepts ist im Falle einer manuellen Umsetzung der hohe Zeit- und Ressourcenaufwand, den viele Unternehmen möglicherweise nicht aufbieten können.

Nachher: IBM übernimmt Download, Test, Zusammenstellung und Verteilung von Patches für Betriebssysteme, Malwareschutzlösungen und Anwendungen aller Anbieter für den Kunden. Dadurch entfallen erhebliche Kosten im Bereich der Analyse und Akquise von Patches. Wenn ein unterstützter Anbieter ein neues Patch veröffentlicht, erhält IBM das Patch, führt eine vorläufige Analyse durch und erstellt Patchrichtlinien (IBM Fixlet-Nachrichten), die in das Update Richtlinieninformationen wie Patchabhängigkeiten, zutreffende Systeme und Prioritätsstufe einschließen. Die Fixlets werden dann automatisch an die Patchserver von Tivoli Endpoint Manager-Kunden gesendet. Die Lösung stellt zudem einen Prozess zur Verfügung, mit dem Kunden das Produkt so konfigurieren können, dass es die Patches direkt von den Websites der jeweiligen Anbieter herunterlädt oder den Patchinhalt lokal speichert. Darüber hinaus können Kunden mit einer über einen Assistenten gesteuerten Schnittstelle ihre eigenen an ihre ganz speziellen Bedürfnisse angepassten Fixlets erstellen. Dieser Prozess funktioniert bei praktisch allen Updates, auch bei Patches für interne Anwendungen.

Schritt 2: Beurteilung

Vorher: Für jedes identifizierte Patch muss die IT-Organisation die Anwendbarkeit und Priorität des Updates bestimmen und dabei identifizieren, auf welchen Endgeräten im Unternehmen Patches implementiert werden müssen. Im Falle von Sicherheitsupdates sind diese kritischen Informationen direkt gleichzusetzen mit Risiken, da geschäftliche Risiken mit der Anzahl ungepatchter Endgeräte zunehmen. Viele Unternehmen haben keinen Zugriff auf die vollständigen, aktuellen Asset- und Konfigurationsdaten, die notwendig sind, um den Umfang und die Auswirkungen von Patches im gesamten Unternehmen zu bestimmen. Es gibt Tools, mit denen diese Daten erfasst werden können, viele brauchen jedoch Tage oder gar Wochen, um diese Informationen zu sammeln und zu sortieren. Dafür muss nämlich jedes Endgerät im Netzwerk durchsucht werden (wobei viele standortunabhängige Endgeräte selten mit dem Netzwerk verbunden sind) – ein Prozess, der Tage dauern kann. Die erfassten Informationen müssen den Systemadministratoren zum Zeitpunkt des Patch-Releases unverzüglich zur Verfügung stehen, da viele Patches zeitkritisch sind und der Prozess der Risikobewertung und Patchpriorisierung so schnell wie möglich erfolgen muss.

Nachher: Bei Verwendung von Tivoli Endpoint Manager wird ein einziger intelligenter Software-Agent auf allen verwalteten Endgeräten installiert, der den Status des Endgeräts, einschließlich Patch-Levels, fortlaufend überwacht und einem Management-Server meldet. Der Agent vergleicht darüber hinaus die Compliance von Endgeräten mit definierten Richtlinien, wie z. B. mit verbindlichen Patch-Levels und Standardkonfigurationen. Diese Informationen sind insbesondere bei Patches für Notfälle kritisch, wenn ein Softwareanbieter ein besonders wichtiges, außerhalb des normalen Zyklus erscheinendes Patch herausgibt und Unternehmen Ausmaß und Risiko der entsprechenden Schwachstelle(n) schnellstmöglich quantifizieren müssen. In einem Beispiel installierte ein Kunde mit Tivoli Endpoint Manager auf 5.100 Endgeräten Agenten und fand dabei heraus, dass auf über 1.500 (30 Prozent) der Endgeräte des Unternehmens mindestens ein wichtiges Patch fehlte. Insgesamt fehlten auf allen Endgeräten im Unternehmen 20.033 „wichtige“ Patches – also durchschnittlich 13 Patches pro Endgerät. Sobald die Gesamtzahl Patches den Endgeräten, die sie benötigen, zugeordnet und die Priorität anhand des möglichen Einflusses auf das Geschäft des Unternehmens, festgelegt wurde, kann die IT-Organisation zum Schritt Korrektur übergehen.

Schritt 3: Korrektur

Vorher: Nachdem ein Patch bewertet und festgelegt wurde, dass es unternehmensweit verteilt werden soll, muss das Patch paketiert und getestet werden, damit sichergestellt ist, dass es nicht zu einem Konflikt mit anderen Patches und auf den Zielendgeräten installierter Software anderer Hersteller kommt. Darüber hinaus müssen Voraussetzungen und Abhängigkeiten von Patches, wie beispielsweise Mindest-Service-Pack-Levels, festgelegt werden. Dies erfolgt normalerweise durch Anwendung und Test des Updates auf einer bestimmten Anzahl von Endgeräten vor der allgemeinen Freigabe – ein Prozess, der unter Verwendung manueller Tools Tage oder gar Wochen dauern kann. Wenn die Tests darauf hinweisen, dass das Patch bedenkenlos unternehmensweit implementiert werden kann, wird es auf den betroffenen Endgeräten implementiert. Dies erfolgt normalerweise in mehreren zeitlich abgetrennten Tranchen, wodurch die Zeit bis zum vollständigen Patcherfolg weiter verlängert wird. Lange Korrekturzeiten sind auf die mangelnde Zuverlässigkeit der Patchqualität und der Verteilungsmechanismen zurückzuführen, da in beiden Fällen die Patchimplementierung nur selten auf Anhieb gelingt. Die meisten Unternehmen sind daher gezwungen, langsam vorzugehen, falls ein Patch zu einem unvorhergesehenen Problem führt, und um sicherzustellen, dass die Netzwerkverbindungen durch den Patchverteilungsprozess nicht überlastet werden. Aus diesem Grund ist es oft nicht einfach, eine Korrektur schnell und effektiv im gesamten Unternehmen durchzuführen.

Ein weiteres schwerwiegendes Problem ist die Tatsache, dass viele Tools für das Patch-Management aufgrund von Abhängigkeiten von Microsoft-Tools wie Windows Server Update Services (WSUS) nur unter Microsoft® Windows® funktionieren. Für viele Tools sind darüber hinaus fundiertes Fachwissen im Bereich Plattformen und hoch qualifizierte Mitarbeiter erforderlich, die diese bedienen. Viele dieser Tools funktionieren erst, wenn Endgeräte mit einem Hochgeschwindigkeitsnetz verbunden werden. Das heißt, standortunabhängige Laptops und andere mobile Endgeräte fallen für lange Zeit aus dem Updatezyklus heraus. Viele Tools bieten nicht die hochdifferenzierbaren, auf Richtlinien basierenden Kontrollen, die Administratoren benötigen, um Patches effektiv auf allen betroffenen Endgeräten im Unternehmen zu implementieren. Einstellungsmöglichkeiten, wie z. B. das Zeitfenster für die Patchinstallation, die Frage, ob ein Benutzer anwesend sein muss oder nicht, ob ein Neustart notwendig ist, die Verteilungsmethode (einschließlich Bandbreite und CPU-Regulierungen), Optionen für Systemtyp und Benutzerbenachrichtigung, müssen verfügbare Optionen des automatisierten Updateprozesse sein.

Nachher: Wenn IBM neue Patch-Fixlets über Tivoli Endpoint Manager veröffentlicht, können Unternehmen den Umfang des Updates feststellen, indem sie innerhalb von Minuten einen Bericht erstellen, aus dem die Endgeräte hervorgehen, für die das Update erforderlich ist. Die Patch-Fixlets umfassen Anweisungen für die Verteilung, einschließlich Anforderungen an Betriebssystem, Version und Vorbedingungen. Es entfällt die Notwendigkeit, Patches durch die IT „paketieren“ und umfassend testen zu müssen. Administratoren können innerhalb von wenigen Minuten bestimmen, wann das Patch herausgegeben werden soll, welche Benachrichtigung Endbenutzern ggf. angezeigt werden soll, ob man es Benutzern gestatten soll, eine Patchimplementierung zu verschieben, und wenn ja, für wie lange, und ob Neustarts erzwungen (oder verschoben) werden sollen oder nicht. Innerhalb von Minuten erhält der Endgeräteagent die neue Richtlinie und analysiert seinen Wirt sofort, um zu bestimmen, ob das Patch anwendbar ist. Ist dies der Fall, lädt der Agent das Patch herunter und implementiert es, wobei Erfolg oder Misserfolg ebenfalls innerhalb von Minuten gemeldet wird. Dieses Konzept kann, in Verbindung mit der Tivoli Endpoint Manager-Relay-Struktur und der Möglichkeit des Verbindungsaufbaus mit Geräten, die lediglich mit dem öffentlichen Internet verbunden sind, die Netzwerkbelastung erheblich reduzieren und die Anzahl auf Anhieb erfolgreicher Patches auf über 95 Prozent verbessern.

Die Lösung bietet darüber hinaus einen extrem sicheren Mechanismus, der kryptographische Identitäten nutzt und damit sicherstellt, dass nur autorisierte Administratoren Richtlinien erstellen und verteilen können. Da keine Active Directory-Abhängigkeiten vorliegen, müssen Administratoren von Tivoli Endpoint Manager nicht gleichzeitig Administratoren von Active Directory-Domänen sein. Die Lösung speichert Auditberichte, in denen protokolliert wird, wer angeordnet hat, welche Richtlinien auf welche Endgeräte angewendet werden sollen, und setzt von Administratoren, die den Korrekturprozess starten, kein spezielles Fachwissen im Bereich Betriebssysteme voraus. Jeder Administrator von Tivoli Endpoint Manager mit ein paar Stunden Basisschulung kann unter den Betriebssystemen Windows, Linux®, UNIX® und Mac OS® Patches sicher und schnell implementieren, ohne über domänenspezifisches Fachwissen verfügen zu müssen.

Schritt 4: Bestätigung

Vorher: Nach der geplanten Implementierung von Patches muss die erfolgreiche Installation bestätigt werden, damit die IT-Abteilung weiß, wann der Patchzyklus abgeschlossen ist, und die Erstellung von Complianceberichten beginnen kann. Diese Daten müssen an ein zentrales Berichtssystem übertragen werden, das Mitarbeiter über den Prozess, einschließlich der aufgetretenen Ausnahmen, in Echtzeit informiert. Viele Technologien für das Patch-Management führen diesen Prozess jedoch nicht effektiv durch, sodass eine erneute Überprüfung aller Endgeräte Wochen und die Behebung von Ausnahmen sogar noch länger dauern kann. Diese Zeitverzögerung führt zu erheblichen Unsicherheiten im Zusammenhang mit dem Risiko- und Compliancestatus des Unternehmens.

Viele Produkte sehen keine Bestätigung nach der Patchimplementierung vor oder es dauert Tage oder gar Wochen, um einen unternehmensweiten Bericht zu erstellen. Noch schlimmer ist aber, dass einige Tools fälschlicherweise berichten, dass Patches implementiert wurden, wenn eigentlich nur die entsprechenden Dateien heruntergeladen wurden, das Patch jedoch gar nicht installiert wurde. Bei all diesen Verzögerungen und Unsicherheiten bleiben einige Endgeräte häufig ungeschützt und stellen somit eine erhebliche Schwachstelle im Sicherheitskonzept dar.

Nachher: Sobald ein Patch implementiert wurde, bewertet der Tivoli Endpoint Manager-Agent automatisch und fortlaufend den Endgerätstatus, um die erfolgreiche Installation zu gewährleisten und den Management-Server in Echtzeit unverzüglich (oder bei mobilen Einheiten bei nächster Gelegenheit) zu aktualisieren. Dieser Schritt ist wichtig, wenn es um die Erfüllung von Complianceanforderungen geht, die einen verbindlichen Nachweis einer fortlaufenden Patchinstallation erfordern. Mit dieser Lösung können Administratoren die Patchimplementierung über eine zentralisierte Managementkonsole in Echtzeit überwachen und erhalten innerhalb von Minuten nach Start des Patchprozesses eine Bestätigung der Patchinstallation. Durch das Abschließen der Patchimplementierung können Unternehmen Patch-Compliance intelligenter, schneller und zuverlässiger sicherstellen.

Schritt 5: Umsetzung

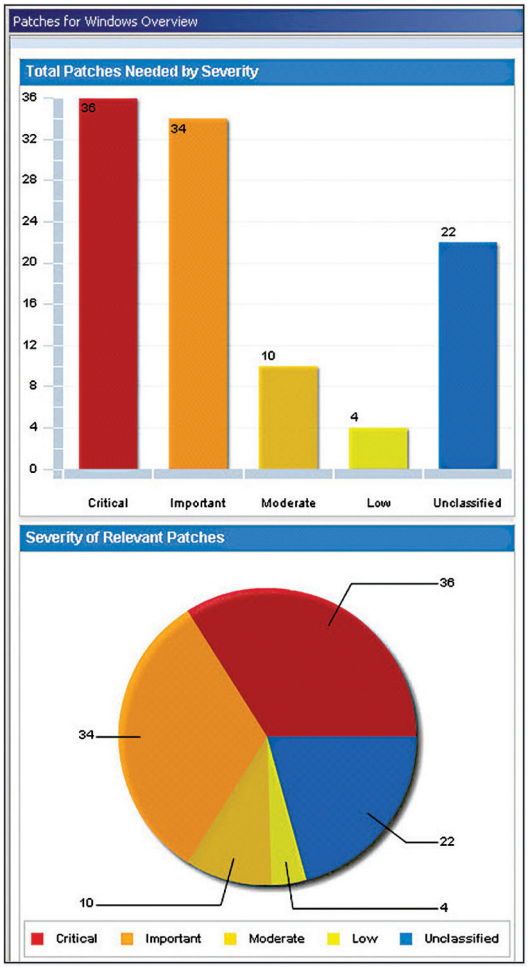
Vorher: Nach der Erstimplementierung bleiben viele Updates nicht immer „erhalten“. Benutzer deinstallieren entweder absichtlich oder versehentlich Patches, neue Anwendungen oder Patches können vorhandene Updates beschädigen, Malware kann Patches bewusst löschen oder durch das Update hervorgerufene Probleme können einen Rollback erforderlich machen. Technologien für das Patch-Management müssen Maschinen fortlaufend überwachen, um eine Einhaltung von Patchrichtlinien sicherzustellen und Funktionen für schnelle, auf Richtlinien basierende Rollbacks im Falle eines größeren Patchproblems bereitzustellen. Wenn ein Patch einer Sicherheitsrichtlinie entgegen gelöscht wird, muss es unverzüglich erneut installiert werden, und wenn ein Patch nach der Implementierung ein schwerwiegendes Problem verursacht, müssen Unternehmen in der Lage sein, schnell einen Gesamtrollback durchzuführen. Ohne die richtigen Tools ist dieser Schritt allerdings praktisch unmöglich.

Nachher: Der intelligente Tivoli Endpoint Manager-Agent setzt fortlaufend die Einhaltung von Patchrichtlinien durch und stellt damit sicher, dass Endgeräte immer auf dem neuesten Stand bleiben. Wenn ein Patch aus irgendeinem Grund deinstalliert wird, kann die Richtlinie festlegen, dass der Agent das Patch bei Bedarf automatisch erneut auf dem Endgerät implementieren soll. Sollte es Probleme mit einem Patch geben, können Administratoren von Tivoli Endpoint Manager schnell und einfach einen Rollback für die Endgeräte durchführen – entweder insgesamt oder nur für einzelne Endgeräte. Über dieselbe zentralisierte Konsole wird die Compliance des jeweiligen Endgeräts in Echtzeit gemeldet, sodass IT-Administratoren den Status aller verwalteten Endgeräte im Unternehmen problemlos überwachen können. Administratoren haben volle Kontrolle über ihre Endgeräte und können das Vielfache des Arbeitsvolumens im Vergleich zu anderen Produkten stemmen, welche umfassende manuelle Eingriffe erfordern und erhebliche Zeitverzögerungen für den Berichtsprozess mit sich bringen.

Schritt 6: Berichterstellung

Vorher: Berichterstellung ist ein wichtiger Bestandteil des Patch-Management-Prozesses. Compliance- und Unternehmensrichtlinien erfordern extrem detaillierte, aktuelle Dashboards und Berichte, die die Risikoposition des Unternehmens und den Patch-Management-Status für verschiedene Nutzer (einschließlich Complianceprüfern, Führungskräften, Management und selbst Endbenutzern) aufzeigen. Ohne Gesamtlösung gibt es keine klar umrissene Möglichkeit zur Meldung des unternehmensweiten Patchstatus.

Nachher: Mit den integrierten Funktionen für die Webberichterstellung von Tivoli Endpoint Manager können Endbenutzer, Administratoren, Führungskräfte, Management und andere bis auf die Minute aktuelle Dashboards und Berichte anzeigen, aus denen hervorgeht, welche Patches implementiert wurden, wann sie implementiert wurden und wer sie auf welchen Endgeräten implementiert hat. Spezielle mehrstufige Dashboards zeigen den Patch-Management-Fortschritt in Echtzeit an.



Dashboardberichte in Tivoli Endpoint Manager zeigen den Patch-Management-Fortschritt in Echtzeit an.

Wie es funktioniert

Traditionelle Konzepte für das Patch-Management, die mit manuellen Prozessen und mühsamen scan- und umfragebasierenden Mechanismen arbeiten, sind nicht mehr schnell oder kosteneffizient genug, um geschäftlichen Anforderungen und gesetzlichen Bestimmungen gerecht zu werden, und stellen Unternehmen vor inakzeptable Risiken und Kosten. Viele Unternehmen, die versuchen, „gebührenfreie“ oder kostengünstige Tools wie WSUS einzusetzen, merken schnell, dass diese Lösungen nicht den Anforderungen von Unternehmen gewachsen sind. Sie sind auf einen einzigen Anbieter begrenzt, bieten keine organisatorische Kontrolle darüber, welche Patches wo und wann implementiert werden, führen zu Betriebsunterbrechungen für den Endbenutzer und bieten häufig nur mangelhafte Berichterstellung, die den Echtzeitstatus nicht wiedergibt. WSUS ist ein gutes Beispiel für ein Einzelprodukt, das zur Durchführung nur eines Schrittes des vorstehend beschriebenen Patch-Management-Prozesses verwendet wird. Dennoch setzt man das Produkt ein, da es als „gebührenfrei“ betrachtet wird.

Microsoft hat regelmäßige Patch-Release-Zyklen eingeführt, die als „Patch-Dienstage“ bekannt sind und die unglücklicherweise auch „Hacker-Mittwoche“ hervorbrachten, an denen Onlinekriminelle beste Möglichkeiten zur Infizierung von Endgeräten, auf denen keine Patches implementiert wurden, haben, ohne weitere neue Schwachstellen ausfindig machen zu müssen. Endgeräte, die nicht unmittelbar durch Implementierung eines Patches geschützt werden, bieten eine Gelegenheit für Kriminelle und stellen ein Risiko für das gesamte Unternehmen dar. Darüber hinaus müssen Unternehmen Updates für die verschiedensten Produkte und Hardwaregerätetypen verschiedener Anbieter verwalten – nicht nur für Windows.

Tivoli Endpoint Manager ist marktführend hinsichtlich Einsatzbereich, Geschwindigkeit, Automatisierung und Wirtschaftlichkeit, ferner stellt die Lösung umfassende Patches für Betriebssysteme und Anwendungen anderer Hersteller bereit. Die Lösung, die eine Implementierung eines vielseitigen, einfachen intelligenten Agenten auf allen Endgeräten umfasst, unterstützt eine breite Palette an Gerätetypen, angefangen von Servern bis zu Desktop-PCs, „standortunabhängigen" Laptops mit Internetverbindung und speziellen Geräten, wie z. B. Point-of-Sale-Einheiten (POS), Geldautomaten und Self-Service-Kiosks.

Ein einziger Management-Server kann bis zu 250.000 Endgeräte unabhängig von deren Standort, Verbindungstyp und -geschwindigkeit oder Status unterstützen und zusätzliche Server bieten praktisch uneingeschränkte Skalierbarkeit. Auf Richtlinien basierende Kontrollmechanismen stellen IT-Administratoren differenzierte, höchst automatisierte Funktionen für das Patch-Management zur Verfügung und umfassende Berichte unterstützen Complianceanforderungen. Die Einhaltung von Richtlinien wird vom intelligenten Agenten unabhängig von der Netzwerkverbindung des jeweiligen Endgeräts fortlaufend überprüft und durchgesetzt. Andere Produkte sind Back-End-lastig und erfordern viel Hardware und eine hohe Zahl an Mitarbeitern zur Unterstützung von Implementierungen (in vielen Fällen Dutzende bis zu Hunderten von Servern, mehrere Agenten pro Endgerät und zahlreiche Administratoren), um dieselbe Umgebung zu unterstützen, die Tivoli Endpoint Manager mit einem Management-Server, einem Endgeräteagent und einem Zwanzigstel der benötigten Mitarbeiter abdeckt.

Ein weiterer wichtiger Aspekt der Architektur ist die Unterstützung für Endgeräte, die sich sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks befinden. Standortunabhängige Einheiten, wie z. B. Laptops, können Patches über eine beliebige Internetverbindung, beispielsweise über eine Wi-Fi- oder sogar Modemverbindung, abrufen. Der Patch-Management-Prozess ist für den Benutzer transparent und IBM Fixlet-Nachrichten kontrollieren die gesamte, vom Endgeräteagenten benötigte Bandbreite und CPU abhängig von dessen Standort und Verbindung, um die Netzauslastung zu optimieren.

Kontinuierliche Compliance

Viele Unternehmen müssen die Einhaltung von Patch-Management-Prozessen festlegen, dokumentieren und nachweisen, um gesetzlichen Vorschriften, Service-Level-Agreements (SLAs) und unternehmensinternen Richtlinien gerecht zu werden. Vorschriften wie Sarbanes-Oxley, PCI DSS und HIPAA/HITECH fordern beispielsweise einen regelmäßigen, vollständig dokumentierten Patch-Management-Prozess, ferner muss bei Prüfungen die fortlaufende Einhaltung dieser Vorschriften (Compliance) nachgewiesen werden. Leider investieren viele Unternehmen enorm viel Zeit und Ressourcen in das Patch-Management und werden trotz allem den Complianceanforderungen nicht gerecht. Die Funktionalität von Tivoli Endpoint Manager zur Durchsetzung von Richtlinien und zur schnellen Erstellung von Complianceberichten trägt zu einer Verbesserung der Auditbereitschaft und der Auditberichte von Unternehmen bei.

Wie Kunden es einsetzen

Unternehmen können den Anforderungen des Patch-Managements mit Tivoli Endpoint Manager optimal gerecht werden. Für Kunden bedeutet dies unter anderem eine schnellere Implementierung, bessere Compliance, reduzierte IT-Kosten und kürzere Managementzyklen.

Anforderung: Implementierung von Patch-Management in Tagen oder Wochen – nicht Monaten oder Jahren

- Albany County, NY, konsolidierte in nur zwei Tagen mehrere Tools für das Patch- und Konfigurationsmanagement.
- Die Restaurantkette O'Charley's Restaurants implementierte in nur vier Tagen Patches für über 350 Restaurants.
- SunTrust Banks implementierte mit nur zwei Mitarbeitern innerhalb von drei Monaten eine Lösung für 50.000 Endgeräte an insgesamt fast 1.800 Standorten.
- An der International Islamic University Malaysia stellte man in nur sechs Wochen eine vollständige Implementierung auf 7.000 Fest- und mobilen Computern von sieben Hochschulanlagen mit Bandbreitenbegrenzung fertig.

Anforderung: Compliance mit SLAs, unternehmensinternen Richtlinien und Vorschriften

- Purolator erreichte eine Compliance von 100 Prozent mit einem 24h-SLA ihres Managed Service-Providers.
- SunTrust Banks erzielte eine Patch-Compliance auf 50.000 Endgeräten von 98,5 Prozent.
- Concord Hospital verbesserte die Patch-Compliance von 40 bis 60 Prozent auf 93 Prozent.
- Das Unternehmen Entergy IT, das SLAs erfüllen muss, die eine Patchimplementierung auf über 22.000 Endgeräten innerhalb von zehn Tagen nach dem Release anfordern, hat seit 2004 über 4,9 Millionen Patches im gesamten Unternehmen implementiert und während dieser Zeit gegen kein einziges SLA verstoßen.

Anforderung: Reduzierung der IT-Kosten

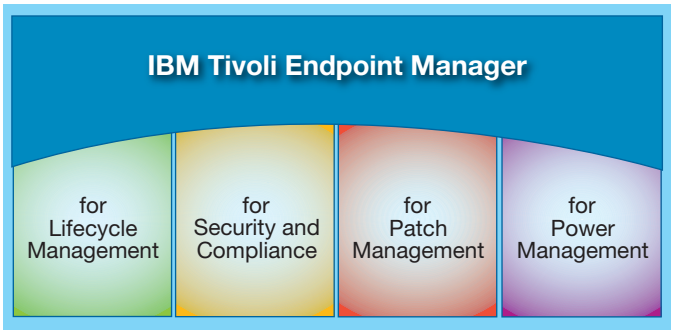
- BGC Partners sparte teure Geschäftsreisen an ferne Serviceniederlassungen auf sechs Kontinenten und damit Zehntausende US-Dollar ein.
- Tax Tech reduzierte die Mitarbeiterkapazität für das Patch-Management von 20 auf einen Mitarbeiter.
- Stena Lines erzielte eine Sparquote bei den Arbeitskosten von 12:1, indem der Zeitaufwand für die Verwaltung von Patchprozessen von 240 Stunden auf 20 Stunden reduziert wurde.
- Die Western Federal Credit Union meldete eine Reduzierung der Arbeitskosten von 50 Prozent durch Automatisierung und vereinheitlichtes Patch-Management.

Anforderung: Reduzierung der Patch-Management-Zyklen

- Concord Hospital reduzierte die Patchzyklen von Wochen auf gerade einmal 15 Minuten.
- SunTrust Banks reduzierte die Patchzyklen von zwei bis drei Wochen auf zwei bis drei Tage.
- Tax Tech automatisierte vollständig die nächtliche Patchverteilung an über 1.000 Standorten, die über ein Virtual Private Network (VPN) verbunden sind.
- Die Desktop and Server Management Group von Entergy installierte in 24 Stunden 70.000 Patches im gesamten Unternehmen.
- Kronos verteilt innerhalb von 15 Minuten Software-Updates, Richtlinien und Patches an alle berechtigten Endgeräte auf der ganzen Welt.

Ein umfassendes Portfolio mit Endgerätemanagement- und Sicherheitslösungen

IBM bietet Funktionen für das Patch-Management im Rahmen eines eigenständigen Produkts (IBM Tivoli Endpoint Manager for Patch Management) oder als integraler Bestandteil von zwei umfangreicheren Lösungen für das Endgerätemanagement (IBM Tivoli Endpoint Manager for Lifecycle Management und IBM Tivoli Endpoint Manager for Security and Compliance). Die Produktfamilie Tivoli Endpoint Manager wird von derselben Konsole, demselben Management-Server und demselben Endgeräteagenten ausgeführt und unterstützt Unternehmen bei der Konsolidierung von Tools, der Reduzierung der Anzahl von Endgeräteagenten und der Senkung von Managementkosten.



IBM Tivoli Endpoint Manager ist eine Familie von Produkten, die alle von derselben Konsole, demselben Management-Server und demselben intelligenten Endgeräteagenten ausgeführt werden.

Tivoli Endpoint Manager ist Bestandteil eines umfassenden IBM Sicherheitsportfolios, das Unternehmen dabei unterstützt, Sicherheitsrisiken für Benutzer und ID-Management, Daten und Informationen, Anwendungen und Prozesse, Netzwerke, Server und Endgeräte sowie physische Infrastrukturen zu gewährleisten. Durch Verbesserung der Anzeige und Kontrolle in Echtzeit und durch Verbesserung von Endgerätesicherheit und -management unterstützt das IBM Portfolio die immer größer und intelligenter werdenden Rechenzentren von heute, um die digitalisierten, vernetzten und intelligenten IT-Prozesse eines smarten Planeten zu vereinfachen.

Die Technologie von Tivoli Endpoint Manager bietet Folgendes:

- **Einen einzigen intelligenten Agenten** – Tivoli Endpoint Manager arbeitet mit einem branchenführenden Konzept, das auf jedem Endgerät einen einzigen intelligenten Agenten vorsieht. Dieser Agent führt mehrere Funktionen (z. B. fortlaufende Selbstanalyse und Richtliniendurchsetzung) aus und hat dennoch nur eine minimale Auswirkung auf die Systemleistung, da durchschnittlich weniger als zwei Prozent der Endgerät-CPU verwendet werden. Der Agent leitet auf intelligente Weise Aktionen ein, indem er Nachrichten zum zentralen Management-Server sendet und bedarfsorientiert Patches, Konfigurationen oder andere Informationen zum Endgerät holt, um eine bestimmte Richtlinie einzuhalten. Aufgrund der Intelligenz und Geschwindigkeit des Agenten, kennt der zentrale Management-Server immer den Compliance- und Änderungsstatus von Endgeräten. Dadurch ist eine schnelle und aktuelle Erstellung von Complianceberichten möglich.

- **Direkte Antworten** – Ganz gleich, ob es darum geht, herauszufinden, wie viele Instanzen von Adobe Acrobat installiert sind, oder zu überprüfen, welche Laptops von einem Rückruf des Herstellers betroffen sind, bietet Tivoli Endpoint Manager unternehmensweit Antworten innerhalb von Minuten. Dank des intelligenten Agenten gibt es keinen Grund mehr, zu warten, bis langwierige Scans zum Abschluss gebracht werden, bis ein zentraler Server alle Einzelheiten analysiert hat oder bis Tausende SQL-Abfragen fertiggestellt werden, bevor Dashboards und Berichte generiert werden können. Jeder Agent bewertet die Relevanz der jeweiligen Anfrage, analysiert die Informationen, gibt eine Rückmeldung und ergreift basierend auf den Analysen ggf. sogar bestimmte Maßnahmen.
- **Abdeckung standortunabhängiger Endgeräte** – Der Firmen-Laptop wird schon lange nicht mehr nur innerhalb des Unternehmens eingesetzt. Benutzer stellen auch von außerhalb Verbindungen zum Unternehmensnetzwerk her – zu Hause, im Hotel, am Flughäfen und sogar im Flugzeug. Tivoli Endpoint Manager bleibt immer einen Schritt voraus und bietet sogar die Möglichkeit, standortunabhängige Endgeräte in Echtzeit zu verwalten.

Fazit

Tivoli Endpoint Manager erfüllt wichtige Anforderungen, mit denen viele Unternehmen derzeit konfrontiert sind. Dafür stellt die Lösung eine zentralisierte, unternehmensweite Lösung für das Patch-Management für Server, Desktops und mobile Einheiten zur Verfügung, die einen Großteil des Patch-Test-Prozesses automatisiert und dadurch die IT entlastet. Die Implementierung von Tivoli Endpoint Manager ist innerhalb von Tagen möglich und ein einziger Management-Server unterstützt bis zu 250.000 Endgeräte. Das Ergebnis: Die Erfolgsquoten bei der Patchimplementierung steigen erheblich, die Einhaltung von Vorschriften wird verbessert und Kosten werden reduziert.

In einer Welt, in der es auf Sekunden ankommt, kann Tivoli Endpoint Manager den Unterschied zwischen einer erfolgreichen Strategie für das Patch-Management und einer unsicheren ausmachen.

Weitere Informationen

Wenn Sie mehr über IBM Tivoli Endpoint Manager erfahren möchten, wenden Sie sich an Ihren IBM Vertriebsbeauftragten oder IBM Business Partner oder besuchen Sie uns unter: **ibm.com**/tivoli/endpoint

Tivoli-Software von IBM

Tivoli-Software von IBM unterstützt Unternehmen durch das effiziente und effektive Management von IT-Ressourcen, Aufgaben und Prozessen dabei, dynamischen Geschäftsanforderungen gerecht zu werden, ein flexibles und reaktionsfähiges IT-Service-Management zu erreichen und gleichzeitig die Kosten zu senken. Das Tivoli-Portfolio umfasst Software für das Management von Sicherheit, Compliance, Storage, Performance, Verfügbarkeit, Konfigurationen, Betrieb und IT-Lifecycle und wird von erstklassigen IBM Service- und Supportangeboten sowie der IBM Forschung unterstützt.

Finanzierungslösungen von IBM Global Financing ermöglichen Ihnen ein effektives Cash-Management, schützen Sie vor dem Risiko veralteter Technologie, optimieren die Gesamtbetriebskosten und verbessern den Return on Investment (ROI). Durch die Global Asset Recovery Services (GARS) von IBM können zudem Umweltschutzanforderungen mit neuen und energieeffizienteren Lösungen erfüllt werden. Weitere Informationen zu IBM Global Financing finden Sie unter: **ibm.com**/financing

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

[1] http://cybersecureinstitute.org

TIW14065-DEDE-00