

Software-Verteilung oder Patch Management?

Ständig müssen unzählige Service Packs, Hot Fixes und Updates für beinahe alle Anwendungen auf die Rechner im Netzwerk verteilt werden. Doch «Patchen» sollte über die reine Installation von Patches hinausgehen. *Thomas Bräuer*



Thomas Bräuer
ist Account Manager bei
bw digitronik und dort Product
Manager für die Patch-
Management-Lösungen.

Viele Unternehmen wenden beträchtliche Mittel für eine Security-Umgebung auf, die sie vor möglichen Angriffen bewahren soll. Ist es aber trotz aller Vorsichtsmassnahmen einem Wurm, Trojaner oder Virus gelungen, sich zum Desktop vorzuarbeiten, ist sein Vernichtungswerk nicht mehr aufzuhalten. Im Nachhinein erscheinen die Investitionen für ein aktives Patch Management im Vergleich zum entstandenen Schaden geradezu als gering. Dem IT-Administrator gaukeln die Software-Verteilungs-Tools oft trügerische Sicherheit vor. Die Patches werden an die Arbeitsstationen verteilt, aber ohne Gewähr, dass sie angenommen oder ordnungsgemäss installiert wurden. Eine verlässliche Security Policy ist ausschliesslich über eine aktive Patch-Management-Lösung zu realisieren.

Wussten Sie, dass ...

... binnen sechs bis zwölf Monaten 20 Prozent aller Rechner nicht korrekt gepatched werden und somit ungepatched bleiben?

... 90 Prozent aller erfolgreichen Hacker-Angriffe auf Systeme mit bekannten Sicherheitslücken erfolgen?

... für nahezu alle Angriffe bereits aktuelle Security Patches verfügbar sind?

... sich 95 Prozent aller Sicherheitslücken durch aktives Patch Management schliessen lassen?

Anforderungen an das Patch Management

Eine Patch-Management-Lösung muss über Funktionen verfügen, mit denen die Sicherung eines Unternehmensnetzwerkes rationell und schnell erfolgen kann. Die Prozesse des Patch Managements müssen automatisiert ablaufen und verschiedene Plattformen wie Microsoft, Linux, Sun, HP, IBM, MAC etc. abdecken können. Audits helfen den Installationsvorgang exakt zu überprüfen.

Eine zeitliche Steuerung, die die Vertei-

lung der Patches ohne erhöhten Verwaltungsaufwand sofort oder zu einem gegebenen Zeitpunkt ausserhalb der Betriebszeiten ermöglicht, ist unverzichtbar. Die Architektur sieht eine zentrale Steuerung und Kontrolle, bei gleichzeitiger dezentraler Anwendung vor, damit auch die Geräte mobiler Anwender sowie externe Standorte mit minimaler Netzwerkbelastung bedient werden können. Ausgebaute Reporting-Funktionen schaffen Klarheit und erlauben, den tatsächlichen Stand der Patches auf jeder Maschine festzustellen. Eine Funktion, um den Patch vor seiner unternehmensweiten Verteilung zu testen, ist zwingend. Gute Patch Tools integrieren all diese Funktionen und ersparen dem Administrator mühselige Abstimmungsarbeit.

Lösungskonzepte

Sich mit einem erfolgreichen Patch-Management-Prozess auseinander zu setzen, ist mehr als lediglich das Verteilen von Patches. Grundsätzlich bieten sich verschiedene Lösungen an. Die meisten klassischen Software-Verteilungs-Tools können auch Patches ausrollen. Oft anzutreffen ist der Windows Server Update Service (WSUS), der naturgemäss auf homogene Microsoft-Umgebungen beschränkt ist und nur einen Teil der hauseigenen Produkte abdeckt. Auch Software-Verteilungs-Suiten können Patches verteilen, sachbedingt ist die Bedienung etwas umständlich. Reine Patch-Management-Lösungen hingegen verfügen über einen hohen Funktionsumfang bei gleichzeitiger komfortabler Bedienung. Die grosse Herausforderung des Patch Managements ist der hohe Zeitdruck für die Verteilung und Installation. Ist eine Sicherheitslücke entdeckt, muss sie schnellstmöglich behoben werden.

Die Stufen des Patch-Management-Prozesses:

- Nachforschen, Inventarisieren und Abgleichen

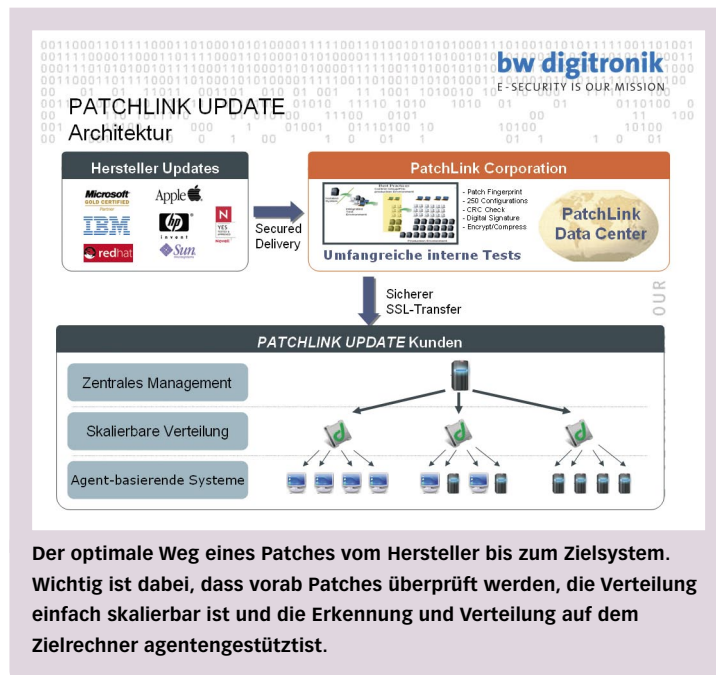
- Voraussetzungen und Abhängigkeiten prüfen
- Patch bereitstellen, Script erstellen und Testen
- Verteilen und Neustart einplanen
- Überprüfen und Nachweis erbringen
- Beobachten
- Updates einspielen
- Berichte und Reports erstellen

Eine intelligente Patch-Management-Lösung muss all diese Stufen beherrschen und der IT-Abteilung die Möglichkeit bieten, alle Aufgaben automatisiert ablaufen zu lassen.

Intelligentes Patch Management

Unvollständig verteilte Patches – weil sie nicht bis zu den Rechnern gelangten oder deinstalliert wurden oder gar einzelne Dateien, die durch das Überschreiben durch ein Dritthersteller-Produkt wieder zur Schwachstelle wurden – müssen festgestellt und repariert werden können. Anhand der intelligenten Fingerprint-Technologie, die beispielsweise in der Lösung von Patchlink integriert ist, kann dies fortlaufend geprüft werden. Dabei vergleicht der Agent die Fingerprints mit den auf dem Zielrechner vorhandenen Dateien. Stellt der Agent eine Abweichung fest, wird je nach Ursache ein Patch installiert oder die Sicherheitslücke geschlossen. Somit kann eine nahezu 100-prozentige Abdeckung gewährleistet werden.

Besonders bei der Massenverteilung von Patches bestehen potenzielle Fehlerquellen. So kann ein fehlerhafter Patch ungewollt ein ganzes Netzwerk lahm legen. Es muss geprüft werden können, ob die Patches erfolgreich eingespielt wurden. Durch einen erneuten Scan eines Agenten auf dem Zielsystem wird eindeutig festgestellt, ob die Patches am Zielrechner korrekt installiert und aktiviert sind. Diese Validierung wird in Berichten dokumentiert. Zu jeder Zeit



können individuelle Reports erstellt werden, die den aktuellen Patch-Status des gesamten Netzwerkes anzeigen. Umfassende Reporting-Funktionen helfen, wenn der Administrator Rechenschaft über die betreuten Systeme und ihren Zustand abliefern muss.

Einschleppung verhindern

Eine umfassende Patch-Management-Lösung verfügt über weitere sicherheitsrelevante Funktionen wie ein Quarantänen-System. Damit werden mobile Geräte vor der Verbindung mit dem Netzwerk umfassend geprüft und po-

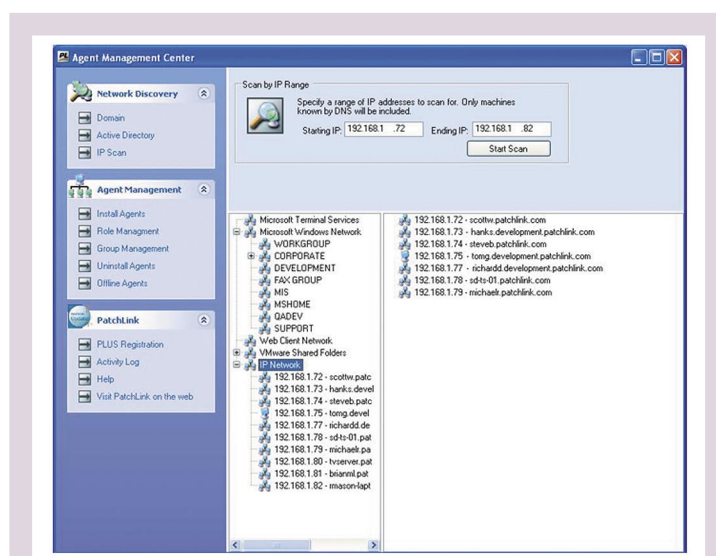
tenzielle Gefahren rechtzeitig behoben. Kombiniert mit einem Network Access Device kann auch das Management der Endpunktsicherheit wirkungsvoll ausgeübt werden. Dies dient dem Schutz von Netzwerken durch die Sicherstellung einer Vorbereitung von Desktops, Laptops und Servern in einer «Reinraum-Umgebung» für ihre Kompatibilität mit den Sicherheitsregeln. Dabei wird sichergestellt, dass nur Rechner, die die firmeninternen Sicherheitsrichtlinien erfüllen, Zugriff zum Firmennetzwerk erhalten.

«Als vor einem Jahr ein kritischer Server abstürzte, weil er den falschen Software Patch verwendete, verbrachten Mitarbeiter der IT-Abteilung fünfzehn Stunden am Telefon, um herauszufinden, welches Patch installiert werden sollte. Am Schluss mussten wir den Server neu aufbauen. Wir konnten das Problem mit einer intelligenten Patch-Management-Lösung beheben; es hat sich dank der erzielten Einsparungen für Arbeitskräfte bereits bezahlt gemacht.» berichtet Jason Hittleman, VP Information Systems, RKA Petroleum.

IT- und Security-Administratoren und – Verantwortliche sowie Entscheidungsträger aus Geschäftsleitung und Verwaltungsrat profitieren folgendermassen von einer Patch-Management-Lösung:

- Risikoverminderung durch Beseitigung der Schwachstellen
- Einhaltung der Sicherheitsregeln
- Erhöhung der Verfügbarkeit
- Skalierbarkeit auch für Enterprise-Umgebungen
- Reduzierung der Kosten für das Patch Management

Mit einer intelligenten Patch-Management-Lösung tragen Unternehmen zur Senkung der Betriebskosten bei, verfügen über Anwendungen auf dem aktuellsten Stand und bewahren sich durch stets geschlossene Sicherheitslücken vor Hacker-Angriffen. ■



Mithilfe des Agent-Management-Centers können Agenten automatisch im Netz verteilt werden, ohne das vom Benutzer am Zielsystem eine Interaktion verlangt wird