

## ■ Backgrounder: Brainware PatchDeploy versus Microsoft SUS/WUS

# Patch-Management: Automatisierung reicht nicht aus

**Patch-Management ist eine der wichtigsten Massnahmen im Bereich der IT-Sicherheit. Patches müssen schnell und gezielt verteilt werden, aber dennoch getestet sein. Am besten funktioniert das in der Kombination von Patch Management-Lösungen mit voller Integration in das Client Lifecycle Management und zusätzlichen Diensten des Herstellers. Brainware Columbus PatchDeploy bietet genau das – und geht damit weit über das hinaus, was man mit Microsoft's eigenen Lösungen erreichen kann.**

Microsoft hat in den vergangenen Jahren massive Anstrengungen unternommen, um die Sicherheit der eigenen Software zu erhöhen. Dennoch gibt es regelmässig Patches, mit denen aktuelle Fehler behoben werden. Auch andere Softwarehersteller haben inzwischen Programme für das Patch-Management. Um diese Patches schnell, zuverlässig und fehlerfrei auf die Zielsysteme zu bringen, braucht es spezielle Software. Microsoft hat mit den WUS (Windows Update Services) und ihrem Vorläufer SUS (Software Update Services) eigene Lösungen. Diese stossen aber – auch für die Aktualisierung von Windows-Betriebssystemen

*«Patches sind nichts anderes als Software, die verteilt werden muss – nur schneller und nach anderen Kriterien»*

### «Brainware PatchDeploy» – besseres Patch-Management

- Optionale Unterstützung für Patches von Drittanbietern
- Durch Brainware mehrfach getestete Patches
- Flexible Workflows für die Freigabe und Verteilung von Patches
- Flexible Auswahl und Zuordnung der Patches
- Volle Integration mit der Inventarisierung
- Einheitliche Oberfläche mit anderen Client Management-Funktionen
- Flexible Kontrolle der Netzlast
- Umfassende Analyse- und Berichtsfunktionen



men und Microsoft-Anwendungen – schnell an ihre Grenzen. Die Anforderungen an das Patch-Management, die Lösungsansätze von Brainware Columbus PatchDeploy und die Einschränkungen von Microsoft WUS/SUS sowohl im Standalone-Betrieb als auch in Verbindung mit dem SMS werden in diesem Dokument erläutert.

## 2 Zehn Anforderungen an das Patch-Management

*Patch-Management ist durch seine Stellung zwischen der Client-Konfiguration und dem Sicherheitsmanagement einer der anspruchsvollsten Bereiche der IT. Trotz vieler Anpassungen an den Clients und Servern durch die Patches muss ein stabiler Systemstatus gewährleistet sein. Software für Patch-Management muss daher vielen Anforderungen genügen.*

### 1. Schnelle Reaktion auf Bedrohungen

Die Zeiträume zwischen dem Bekanntwerden eines Bedrohungsszenarios und einer konkreten Gefährdung durch aktive Angriffe sind in den vergangenen Jahren stark gesunken. Vor wenigen Jahren hat es in der Regel noch Monate gedauert, bis Angreifer eine bekannte Lücke auch genutzt haben. Inzwischen kommt es vor, dass erste Würmer und andere Angriffsvarianten schon nach wenigen Tagen zu beobachten sind. Spezielle Tools für Hacker und eine zunehmende Professionalisierung der Angreifer sind dafür verantwortlich.

Man kann es sich also nicht mehr leisten, nur alle paar Wochen oder gar Monate Updates insbesondere der Clients mit Internet-Zugang durchzuführen. Die Reaktion muss innerhalb weniger Tage nach Verfügbarkeit von Patches und damit dem Bekanntwerden von Schwachstellen erfolgen. Denn leider gibt es hier einen Zusammenhang: Wenn – vor allem – Microsoft Patches herausgibt, wissen die potenziellen Angreifer zwangsläufig auch mehr über neue Schwachstellen und können damit Tools entwickeln, um diese auszunutzen.

Der Prozess von der Verfügbarkeit von Patches über deren Analyse, Test und Bereitstellung auf den Clients und Servern muss daher so optimiert werden, dass es gelingt, schnell – aber auch gezielt und koordiniert – auf Bedrohungen zu reagieren und Patches zu installieren.

### 2. Patchen, wo nötig – und nur dort

Patch-Management muss zuverlässig arbeiten. Patches müssen garantiert auf allen Systemen eingerichtet werden, auf denen sie benötigt werden. Weil jeder Patch aber auch einen Eingriff in eine stabile Arbeitsumgebung darstellt, sollten er auch nur dort eingerichtet werden, wo es erforderlich ist – ebenso

### Patches – nicht nur für mehr Sicherheit

Patch-Management kann und darf nicht auf die erste Hilfe bei Sicherheitsrisiken bedroht werden. Sicherheits-Patches stehen zwar im Mittelpunkt. Wenn man aber beispielsweise die Anzahl der Patches betrachtet, die Microsoft herausgibt, wird deutlich, dass es dort wesentlich mehr Patches gibt, die «einfache» Softwarefehler beseitigen als solche, mit denen Sicherheitsprobleme gelöst werden. Bei anderen Herstellern ist das nicht anders. Patch-Management muss vor Sicherheitsrisiken schützen – und andere Fehler ebenfalls beseitigen.

wenig, wie noch einmal versucht werden sollte, einen bereits vorhandenen Patch einzurichten. Das setzt voraus, dass man genau weiss, welchen Status welches System aktuell hat.

Zuverlässigkeit heisst aber auch, dass man mit getesteten Patches arbeitet – nichts ist schlimmer als womöglich Tausende von Clients durch einen unzureichend geprüften Patch lahm zu legen. Leider gab es diese Fälle schon. Und je mehr Patches man für unterschiedliche Betriebssysteme und Anwendungen einspielen muss, desto komplexer wird die Analyse. Durch die wachsenden Anforderungen an Compliance und IT-Governance muss zudem nachvollziehbar sein, wann welche Patches auf welchen Systemen installiert wurden. Denn wer möchte schon sprachlos sein, wenn er gefragt wird, ob er rechtzeitig die erforderlichen Sicherheitsmassnahmen ergriffen hat, wenn doch mal etwas schief geht?

### 3. Definierte Prozesse, klare Genehmigungsverfahren

Völlig unterschätzt wird oft die Bedeutung von definierten Prozessen, strukturierten Genehmigungsverfahren und abgestuften Berechtigungen im Patch-Prozess. Wer weiss schon, dass die aktuellen Richtlinien zur Prüfung von Unternehmen in der EU unter anderem auch definierte Prozesse mit einer definierten Übergabe von IT-Anwendungen – und Änderungen an diesen wie beispielsweise Patches – als notwendig erachten? Da die Zuverlässigkeit und Sicherheit der IT zunehmend Prüfungsgegenstand ist, werden immer öfter unangenehme Fragen an die IT gestellt.

Patch-Management, das solche Prozesse und eine klare Trennung von Verantwortlichkeiten nicht unterstützt, ist damit keine Lösung, sondern ein Problem. Je flexibler die Werkzeuge sind, desto besser kann man den jeweiligen Anforderungen gerecht werden.

### 4. Viele Patches – komplexe Abhängigkeiten

Die grosse Anzahl an Patches lässt vor allem auf Betriebssystemebene ein anderes Problem entstehen: Mehrere Patches können auch im Konflikt zueinander stehen. Die richtige Reihenfolge der Patch-Installation muss damit ebenso beachtet werden wie definierte Systemvoraussetzungen. Patch-Management wird immer komplexer.

Wenn – was aus Sicherheitsgründen unverzichtbar ist – auch Anwendungen von anderen Herstellern als Microsoft gepatcht werden, steigt die Komplexität. Manche Patches setzen zunächst ein bestimmtes Service Pack oder einen speziellen Betriebssystem-Patch voraus. Nur wenn man den vollen Überblick sowohl über diese Abhängigkeiten als auch den Status der Systeme hat, können auch die richtigen Patches gewählt werden.

### 5. Qualität statt Quantität

Oder: Der richtige Patch ist entscheidend. Es geht nicht darum, auf jedes System jeden denkbaren Patch zu installieren. Wenn ein System keinen Internet-Zugang hat, weil der Browser nur für die Administration lokaler Server-Anwendungen genutzt wird, sind

bestimmte Patches nicht erforderlich. Viele Patches haben auch nur eine niedrige Bedrohungsstufe, weil Angriffe bei richtiger Konfiguration der Firewall oder anderer Systemeinstellungen nicht durchführbar sind. Ausserdem ist nicht jeder Patch sicherheitsrelevant. Und andere Patches müssen oft nur konditional installiert werden – bei konkreten Fehlern oder spezifischer Hardware.

Das heisst, dass man zumindest nicht jeden Patch sofort installieren muss. Wichtige Patches müssen so schnell installiert werden, wie es in kontrollierter Weise möglich ist. Andere Patches können etwas warten und beispielsweise in lastarmen Zeiten oder in Verbindung mit anderen Rollouts verteilt werden. Eine Bedrohungsanalyse und darauf aufsetzend eine differenzierte Steuerung des Patch-Managements machen aus einer Lösung zur schnellen, flächendeckenden und lastintensiven Verteilung von Änderungen eine Software für die koordinierte und effiziente – qualitativ hochwertige – Aktualisierung der Systeme im Netzwerk.

### 6. Den Status kennen

Bei der Analyse geht es nicht nur darum, Bedrohungen zu kennen, sondern auch den Überblick über den Zustand der Systeme zu haben. Dazu muss man nicht nur wissen, was man geändert hat. Man muss auch wissen, wie die Systeme vor der Einrichtung von Patches ausgesehen haben und welche Massnahmen wie die Installation neuer Software-Releases oder von Service Packs vielleicht noch Einfluss auf den Status hatten.

Ohne die differenzierte Inventarisierung der installierten Software mit der Erkennung von Patches und Service Packs lassen sich keine Aussagen zum Systemstatus treffen. Damit lässt sich weder das Bedrohungspotenzial schnell ermitteln noch beantworten, wo welche Patches installiert wurden. Ein Patch-Management ohne enge Integration mit einem leistungsfähigen Software-Inventar, das installierte Anwendungen, Patches und Service Packs automatisch erkennt und den korrekten Zustand verifizieren kann, ist allenfalls die halbe Lösung.

## 7. Sicherheit erreichen – ohne alles lahm zu legen

Sicherheit ist wichtig. Deshalb darf Patch-Management aber noch lange nicht dazu führen, dass der normale Betrieb von Netzwerken empfindlich gestört wird, weil die Netze durch die Verteilung von Patches überlastet werden. Das ist allenfalls bei extrem sicherheitskritischen Patches tolerierbar. Das trifft aber maximal auf zwei bis drei Prozent aller Patches zu. Alle anderen Patches müssen innerhalb eines Zeitfensters eingerichtet werden, das einige Stunden, wenige Tage oder auch Wochen umfassen kann. Entsprechend flexibel muss auch die Patch-Management-Lösung sein.

Aber selbst wenn Patches schnell verteilt werden müssen, sollte das so schonend wie möglich erfolgen. Eine flexible, konfigurierbare Bandbreitensteuerung und eine – wenn auch noch so kleine – zeitliche Staffelung der Verteilung von Patches ist für effizientes Patch-Management zwingend.

## 8. Es gibt nicht nur Microsoft

Auch wenn über 90% aller Clients mit Microsoft Windows arbeiten und auch Microsoft Office einen sehr hohen Marktanteil hat – selbst in Unternehmen, die auf Microsoft setzen, kann man sich nicht auf die Patches für Microsoft-Produkte beschränken. So ist fast überall auch der Acrobat Reader im Einsatz, um nur ein Beispiel zu nennen. Auch Anwendungen wie Winzip, Lotus Notes oder Browser wie Firefox finden sich in sehr vielen Unternehmen. Hinzu kommen Anwendungen, die im oder für das Unternehmen entwickelt wurden.

Patch-Management muss natürlich die Aktualisierungen für Microsoft's Betriebssysteme und Anwendungen unterstützen. Wenn es sich aber darauf beschränkt, lässt man gefährliche Lücken. Lösungen, die nicht für ergänzende Patches zumindest erweiterbar sind, sind daher keine Antwort auf Sicherheitsprobleme, sondern lassen viele Fragen offen.

## 9. Die vorhandene Infrastruktur nutzen

Eine der Schwachstellen vieler Patch Management-Lösungen ist, dass mit einer eigenen Infrastruktur gearbeitet wird. Es werden zusätzliche Server und, bei den meisten Anwendungen, auch spezielle Client-Komponenten benötigt. Der konzeptionelle und administrative Aufwand dafür ist nicht akzeptabel.

Da Patches – wie eingangs erwähnt – nichts anderes als Softwarepakete sind, die verteilt werden müssen, macht es Sinn, das Patch-Management eng mit der eingesetzten Lösung für das Client Lifecycle-Management zu integrieren. Damit können auch spezielle Funktionen wie die Bandbreitensteuerung genutzt werden.

Die Integration macht aber auch Sinn, weil es beim Patch-Management nicht nur um Sicherheits-Patches geht, sondern auch um die Behebung anderer Probleme. Diese werden aber oft über Helpdesk-Anforderungen entdeckt. Das enge Zusammenspiel sowohl mit Helpdesk- als auch Remote Control-Lösungen ist damit nicht nur sinnvoll, sondern für ein effizientes Systemmanagement zwingend.

## 10. Einfach administrierbar, mit gutem Support

Die bisher genannten Anforderungen sind beachtlich. Damit Patch-Management funktioniert, muss es aber auch einfach zu administrieren sein. Am einfachsten gelingt das, wenn man eine bereits bekannte Benutzerschnittstelle nutzen kann und wenn der Support des Herstellers passt – beispielsweise durch die Unterstützung bei der Erstellung von Patch-Paketen für eigene Software.

## Die Funktionen im Vergleich

	Microsoft WUS	Columbus PatchDeploy
Zugriff auf Microsoft-Patches	Ja	Ja
Zusätzlich geprüfte Patches	Nein	Ja
Integration mit dem Inventar	Nein	Ja
Reports für installierte Patches	Ja	Ja
Reports für installierte Komponenten	Nein	Ja
Konfigurierbare Prozesse	Nein	Ja
Trennung zwischen Test- und Produktivsystemen	Teils	Ja
Flexible Filterung von Patches	Teils	Ja
Bandbreitensteuerung	Teils	Ja
Zeitlich gesteuerte Verteilung	Nein	Ja
Auswahl von Gruppen von Zielsystemen	Ja	Ja
Patches für Drittanbieter	Nein	Ja
Patches für eigene Anwendungen	Nein	Ja
Integration mit Client-Management-Anwendungen	Nur SMS	Ja
Integration mit Helpdesk	Nein	Ja
Integration mit Remote Control	Nur SMS	Ja
Vorhandene Systemmanagement-Server sind nutzbar	Nur SMS	Ja
Einheitliche Oberfläche mit Systemmanagement-Lösungen	Nein	Ja

## Die Ansätze im Vergleich

*Microsoft hat zunächst mit den SUS (Software Update Services) eine Lösung entwickelt, mit der nur Sicherheits-Patches für Windows-Clients verteilt werden konnten. Die WUS (Windows Update Services) oder WSUS (Windows Server Update Services), wie der Nachfolger genannt wird, können mit einer erweiterten Funktionalität aufwarten. Dennoch bleiben im Vergleich mit den genannten Anforderungen und im Vergleich mit Columbus PatchDeploy von Brainware viele Punkte offen.*

Sowohl die WUS als auch Columbus PatchDeploy nutzen Microsoft's Update-Dienste, um aktuelle Patch-Informationen zu Microsoft-Produkten zu empfangen. Im Gegensatz zu Microsoft hat Columbus aber noch eine Zwischenstufe integriert, um die Patches genau zu prüfen und optimierte Pakete zu erstellen. Dadurch entsteht zwangsläufig eine kleine Zeitverzögerung, die aber deutlich unter den kürzesten Zeiträumen liegt, die bisher für aktive Angriffe nach der Veröffentlichung einer Sicherheitslücke beobachtet wurden. Dafür erhält man eine höhere Qualität.

Die erste echte Schwachstelle zeigen die WUS bei der Steuerung des Patch-Prozesses. Es gibt zwar die Möglichkeit, Gruppen von Systemen zu definieren und Patches besser zu filtern. Dennoch sind die Listen von Patches vor allem nach der Installation sehr lang. Darüber hinaus fehlt die Integration mit einem Inventar. Die Informationen darüber, ob ein Patch erforderlich ist, müssen lokal und relativ aufwändig auf den Clients ermittelt werden.

Trotz der Trennung in verschiedene Systemgruppen fehlen bei den WUS auch weitergehende Workflow-Funktionen, mit denen sich beispielsweise Genehmigungsverfahren abbilden lassen. Damit wächst das Risiko, dass Patches unkoordiniert ausgerollt werden. Auch differenzierte Sicherheitskonzepte wie das Rollenkonzept von Columbus Brainware gibt es nicht. Die fehlende Integration mit dem Inventar bedeutet auch, dass sich eben nicht die komplexen Abhängigkeitsprüfungen durchführen lassen. Auch der einfache Blick auf den Status der Systeme fehlt. Die Berichte der WUS zeigen nur, was mit der Anwendung gemacht wurde – aber nicht, was beispielsweise durch die Softwareverteilung verändert wurde.

Logischerweise kennt der WUS auch keine ausgefeilten Mechanismen für die Bandbreitensteuerung, da die Verteilung der Patches nur über HTTP erfolgt – wie auch beim Download von Microsoft's Update-Website. Das liegt schon daran, dass der in den neueren Windows-Versionen integrierte Client verwendet wird. Was mancher mit dem Service Pack 2 von Windows XP erlebt hat, kann daher mit den WUS immer wieder Realität werden: Überlastete Server und überlastete Netzwerke.

Wenig überraschend ist, dass Microsoft sich auch auf die eigenen Betriebssysteme und Anwendungen beschränkt. Bei Columbus PatchDeploy lassen sich dagegen auch Patches von Drittanbietern und für eigene Anwendungen integrieren.

Eines der grössten Probleme der WUS ist sicherlich die erforderliche Infrastruktur. Um sie zu nutzen, wird eine eigene Server-Infrastruktur benötigt, während man bei Columbus PatchDeploy mit den vorhandenen Columbus-Servern arbeiten kann. Mehr noch: Die WUS erfordern auch spezielle Versionen des .NET-Frameworks und die Einrichtung der IIS, die wiederum zu den Anwendungen gehören, für die besonders viele Sicherheits-Patches installiert werden müssen.

Wenn das noch nicht überzeugt: Columbus PatchDeploy ist voll in die Oberfläche der anderen Columbus-Anwendungen integriert. Ausserdem gibt es exzellenten Support vom Hersteller bis hin zur Unterstützung bei der Paketierung von Patches für eigene Anwendungen – und nicht nur die Verteilung von Hersteller-Patches an die anonyme Masse.