



Verwaltung vom Systemupdates für Windows-Clients im Netzwerk

Nicht nur zur Schließung von Sicherheitslücken oder zur Behebung sonstiger Fehler, sondern auch zur Erweiterung durch Zusatzfunktionalitäten werden von Microsoft kostenlose Software-Aktualisierungen angeboten. Nicht nur beim Betriebssystem selbst, sondern auch bei einzelnen Anwendungen gibt es immer wieder nachladbare Erweiterungen und Aktualisierungen sowie Behebungen entdeckter Fehler und Lücken.

Dadurch, dass heutzutage Internetanschlüsse bei Firmennetzwerken schon selbstverständlich geworden sind, ist es leider notwendig geworden, Sicherheitslücken möglichst umgehend nach deren Entdeckung zu beheben, da damit gerechnet werden muss, dass böswillige Programmierer diese Lücken rasch ausnutzen.

Grundsätzliche Anmerkungen

Sollen die Rechner in einem bestimmten Netzwerk auf einem aktuellen Stand gehalten werden, so ist es nicht damit getan, alle Rechner auf „Automatisches Update“ zu stellen. Zum einen nicht, weil dann nur Sicherheitsupdates für das Betriebssystem eingespielt werden, nicht aber für alle weiteren Applikationen, zum anderen deswegen nicht, weil dort entweder eine Benutzereinwirkung erforderlich ist, oder die Rechner zu einem festgelegten Zeitpunkt regelmäßig neu gestartet werden müssen, was sich bei Servern vielleicht noch auf einen Termin außerhalb der Geschäftszeiten legen lässt, bei Arbeitsplatzrechnern, die außerhalb der Arbeitszeit ausgeschaltet sein sollen, aber sehr schwierig ist.

Es sollte auch bedacht werden, dass sich bei der Nutzung von Applikationen von Drittanbietern durch ein Update Nebenwirkungen einstellen können, insbesondere bei Applikationen, die für eine Vorgängerversion des aktuell genutzten Betriebssystems programmiert wurden (z.B. bei MS-DOS-Anwendungen unter Windows2000). Es sollte also stets geprüft werden, ob ein Sicherheitsupdate wirklich installiert werden kann und ob dies geschehen muss. Nicht alles, was vom automatischen Windows Update ungefragt installiert wird, ist wirklich notwendig – Zu jedem Update gibt es immer eine Beschreibung, unter welchen Umständen eine Lücke ausgenutzt werden kann, und anhand dieser lässt sich beurteilen, ob ein spezifischer Rechner überhaupt gefährdet ist.

Folgende Punkte sind also zu beachten:

- Welche Updates stehen zur Verfügung?
- Welche Updates müssen installiert werden und auf welche lässt sich verzichten?
- Wie können diese Updates möglichst unaufwändig installiert werden?

Es stehen nun verschiedene Hilfsmittel zur Verfügung, die eine sowohl Administrator- als auch Anwenderfreundliche Ermittlung und Verteilung verfügbarer Updates ermöglichen, diese sollen jetzt vorgestellt werden.

Microsoft Baseline Security Analyzer (MBSA)

Dieses kostenlos erhältliche Programm scannt Rechner lokal und im Netzwerk auf fehlende Updates sowie auf weitere potentielle Risiken wie einfache Benutzerkennwörter oder Netzwerkdienste, die womöglich nicht benötigt werden (z.B. SMTP-Server auf Arbeitsplatzrechner).

Sowohl das Betriebssystem (NT4, 2000, XP, 2003) als auch weitere Microsoft-Applikationen und Server werden überprüft, die Ergebnisse werden in Berichten ausgegeben und können auch gespeichert werden, eine Installation der Updates findet nicht statt.

Microsoft System Update Services (SUS)

Dieses ebenfalls kostenlos erhältliche Programm synchronisiert sich mit dem Microsoft Windows Update Server und lädt verfügbare Betriebssystemupdates (und nur solche, keine Treiber-Updates und auch keine für Applikationen) herunter, um sie lokal zur Verfügung zu stellen. Jedes Update muss dabei von einem Administrator autorisiert werden, bevor es Clients bereitgestellt wird, so dass nicht benötigte oder nicht gewollte Updates gesperrt bleiben. Über die „Automatische Updates“-Funktion der Microsoft Betriebssysteme ab Version 2000 werden diese dann zugeteilt, SUS lässt also als Proxy und als Filter für die Automatischen Updates verstehen.

Automatische Updates Gruppenrichtlinie

SUS ist bei der Zuteilung der Updates auf eine spezielle Gruppenrichtlinie angewiesen, die von Microsoft heruntergeladen werden kann und nachträglich in das Active Directory von Windows 2000 Server und Windows Server 2003 eingebunden wird. Diese regelt nicht nur die Zuweisung an die Clientrechner, sondern es kann auch festgelegt werden, dass nach der Update-Installation kein Neustart erfolgen soll, so dass sich die Auswirkungen auf am Rechner arbeitende Benutzer auf eine kurzzeitig leicht beeinträchtigte Performance beschränken.

Die Gruppenrichtlinie lässt sich auch ohne SUS nutzen, in diesem Falle werden die Updates vom Microsoft-Server heruntergeladen und es kann keine vorherige Auswahl getroffen werden.

Shavlik HFNetChk Pro

Hierbei handelt es sich um ein kommerzielles Produkt (10 Lizenzen und weniger sind kostenlos) der Firma Shavlik Technologies (www.shavlik.com), das auf einer Vorgängerversion des Microsoft Baseline Security Analyzer beruht, aber in eine andere Richtung weiterentwickelt worden ist. Es scannt Rechner in einem Netzwerk wie der MBSA auf Sicherheitslücken, aber nicht auf andere Updates und auch nicht auf installierte Dienste und unsichere Benutzerkonten. Dafür können die nötigen Updates gleich ausgewählt und zugewiesen werden, wobei verschiedene Möglichkeiten (Uhrzeit, sofortiger Neustart ja/nein) zur Verfügung stehen, das Programm lässt sich auch vollständig automatisieren. Im Gegensatz zum SUS weist HFNetChk Pro auch weiteren Microsoft-Programmen (Office, Serverprodukte) Updates zu, allerdings kann es keine Windows Service Packs zuteilen, was wiederum beim SUS möglich ist.

Fazit

Für eine möglichst vollständige Update-Verwaltung in Windows-Netzwerken müssen also mehrere Produkte ergänzend eingesetzt werden. Die folgende Tabelle soll dies abschließend verdeutlichen:

	Windows-Update Website	Automatische Updates	MBSA	SUS	HFNetChkPro
Sicherheitsupdates (Betriebssystem)	x	x	x	x	x
Treiberupdates	x				
Updates/Service Packs (Betriebssystem)	x		x	x	
Updates (andere MS Software)			x		x
Updateverteilung im Netz				x	x
Selektionsmöglichkeit	x			x	x
Automatisierbarkeit		x		x	x