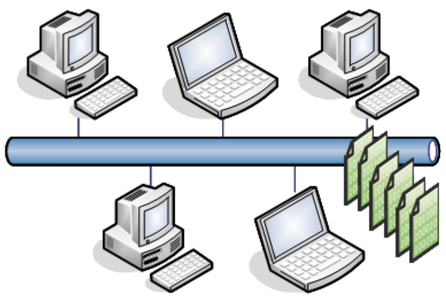
# Fachhochschule Brandenburg
# Fachbereich Informatik und Medien



## Client/Server-basiertes Management-Werkzeug auf Basis des MBSA zur Überprüfung der Softwareupdate-Stände aller Windows-Computer in LANs

*Diplomarbeit, vorgelegt von Steffen Lange*

### Sicherheit durch Patchmanagement

Das Betriebssystem Windows ist wie jede Software nicht frei von Fehlern. Die verheerenden Wurm-Angriffe auf Windows-Computer in den vergangenen Jahren decken folgende zwei Sicherheitsprobleme auf:

1. All diese Würmer nutzen ungepatchte Sicherheitslücken aus.
2. Es bleibt immer weniger Zeit zwischen Erscheinen des Patches und Auftreten eines Exploits.

Zudem betrifft diese Problematik heute neben besonders exponierten Servern auch jeden gewöhnlichen PC.

Die Verwaltung von Softwareupdates – das Patchmanagement – ist aus diesem Grunde ein Schlüsselelement jedes Sicherheitsprozesses und wird im einfachsten Fall als vierphasiger sich wiederholender Prozess umgesetzt.

**Benachrichtigung**

Eine zeitnahe Benachrichtigung über neu veröffentlichte Softwareupdates muss sichergestellt werden.

**Bewertung & Tests**

Jedes Update muss hinsichtlich der Ausnutzbarkeit der entdeckten Sicherheitslücke bewertet werden. Tests stellen dabei sicher, dass keine Fehlfunktionen anderer Software auftreten.

**Verteilung**

Durch geeignete Verfahren erfolgt die Verteilung des Updates im Netzwerk.

**Überprüfung**

Die Überprüfung stellt die erfolgreiche Installation von Updates sicher.

In Windows-Netzwerken von kleineren Firmen und Endkunden ohne Windows Server-System ist das Patchmanagement häufig auf das reine Verteilen der Softwareupdates durch den in Windows integrierten Automatischen Update-Dienst beschränkt. Von den Patchmanagement-Phasen werden dabei nur die ersten Drei abgedeckt – eine Überprüfung der Patch-Stände findet nicht statt.

### Aufgabenstellung

Zielstellung dieser Arbeit ist das Schließen dieser Lücke durch Entwicklung der Anwendung *Patch-Monitor/2* zur Überprüfung der korrekten Verteilung von Softwareupdates in oben skizzierten Windows-Umgebungen.

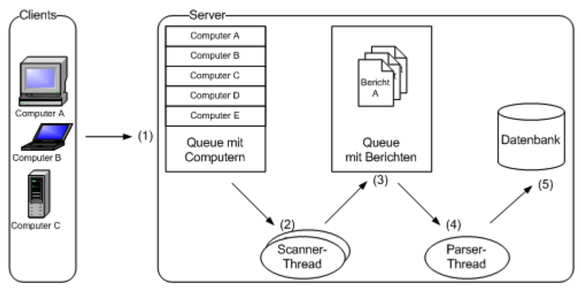
Eine lückenlose Überwachung der bereits installierten und noch fehlenden Sicherheitsupdates auf allen Windows-Computern wird durch eine Client/Server-basierte Applikation realisiert.

Der Client *Security Helper Scanner Service* in Form eines Systemdienstes kontaktiert dazu beim Betriebssystemstart den Server *Patch-Monitor*, welcher daraufhin die Überprüfung durchführt. Dem Administrator steht somit für seine kontrollierenden Verwaltungsaufgaben eine zentrale Anlaufstelle zur Verfügung.

### Funktionsprinzip

Microsoft Baseline Security Analyzer

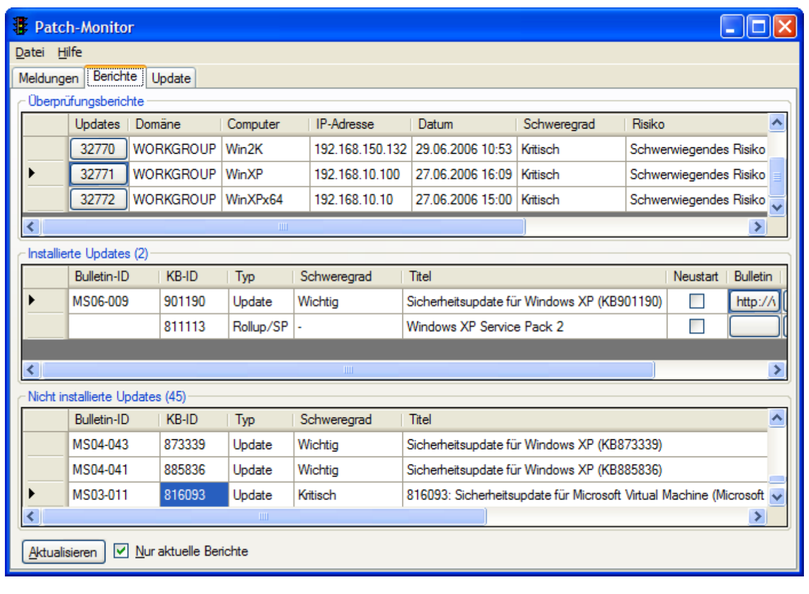
Es stellt sich die grundlegende Frage, wie die Patch-Stände der einzelnen Systeme übers Netzwerk zu ermitteln sind. Als praktikabelste Lösung stellte sich der Rückgriff auf die Befehlszeilenschnittstelle des Microsoft Baseline Security Analyzers 2 (MBSA) heraus.




**Eine Überprüfung läuft wie folgt ab:**

- **(1)** Zunächst muss der auf allen Windows-PCs installierte Client dem Server seine Anwesenheit im Netzwerk anzeigen. Der Server erfasst darauf dieses System als Überprüfungsziel in der Computer-Warteschlange.
- **(2)** Parallel ablaufende Überprüfungs-Threads entnehmen dann die Zielsysteme aus der Warteschlange und führen die Überprüfung mittels des MBSA durch.
- **(3)** Der vom MBSA erzeugte Überprüfungsbericht wird nun der Berichte-Warteschlange hinzugefügt.
- **(4) & (5)** Zuletzt parst der Datenbank-Thread der Reihe nach die Berichte aus der Warteschlange und speichert die Ergebnisse in der Datenbank.

### Patch-Monitor



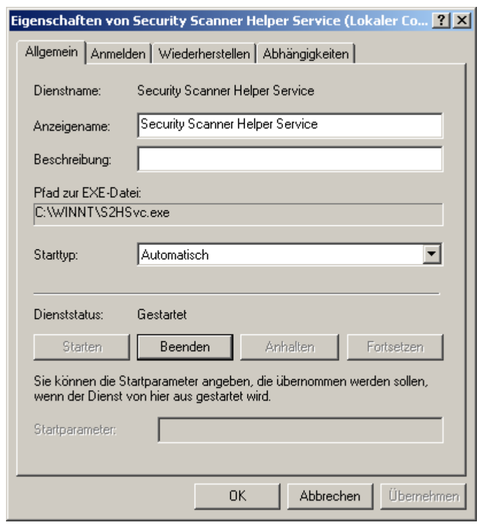

*Management-Oberfläche des Patch-Monitors*

### Einsatz-Szenarien

Die gesammelten Update-Stände bilden eine fundierte Datenbasis für verschiedenste Patchmanagement-Aufgaben. Eine um erweiterte Reporting- und Notification-Funktionalitäten ausgebaute Verwaltungsoberfläche ermöglicht die Erstellung vielseitiger Berichte:

- Welche Systeme erfüllen mit ihrem Patchstand nicht die Basissicherheit?
- Auf welchen Computern fehlt das Update KB12345?
- Wie lange dauert die durchschnittliche Verteilung eines Sicherheitsupdates?
- Welche Computer wurden schon längere Zeit nicht mehr überprüft?

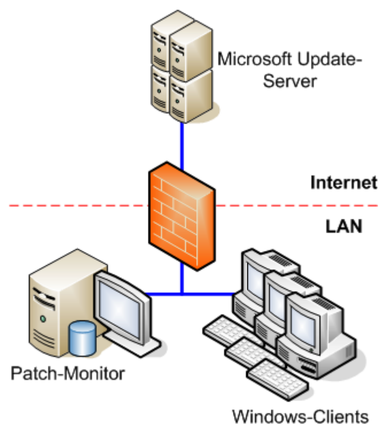
### Client




*Dienst-Eigenschaften des Clients (S2HSvc)*

### Fazit

Zusammenfassend kann festgestellt werden, dass durch Einsatz des Automatischen Update-Dienstes in Verbindung mit der neu entwickelten Patch-Monitoring-Lösung auch in kleineren Windows-Netzwerken das Patchmanagement praktikabel handhabbar ist.




*Beispielhafte Netzwerkstruktur*

**Betreuer: Prof. Dr. Barbara Wiesner**
**Dipl.-Ing. Karsten Sydow**

**Kolloquium: 25. August 2006**