

Patch-Verwaltung mit GFI LANguard N.S.S. und Microsoft SUS

Eine kosteneffiziente und einfache Lösung für netzwerkweites Patch-Management

Dieses White Paper bietet einen Überblick darüber, wie der Netzwerk-Schutz im Bereich der Sicherheits-Patches durch den gemeinsamen Einsatz von GFI LANguard Network Security Scanner (N.S.S.) und den Microsoft Software Update Services (SUS) automatisch auf den neuesten Stand gehalten werden kann.

Einführung

Die Patch-Verwaltung zählt zu den wichtigsten Aufgaben der Netzwerk-Administration. Patch-Management bedeutet, dass alle Rechner des Netzwerks regelmäßig auf fehlende Patches überprüft werden müssen und neu veröffentlichte Sicherheits-Updates umgehend zu installieren sind. Wird dies versäumt, ist das Netzwerk gleich doppelt verwundbar: Zum einen ist das System durch den lückenhaften Netzwerk-Schutz generell gefährdet, zum anderen werden böswillige Benutzer, Hacker und Virenprogrammierer durch die Bekanntgabe der Schwachstelle regelrecht dazu aufgefordert, neue Angriffsversuche zu starten.

Zahlreiche Beispiele belegen dies, und es zeigt sich immer wieder, dass viele Netzwerk-Administratoren trotzdem die Patch-Installation vernachlässigen – Würmer wie der SQL Slammer vom Januar 2003, der bekannte Sicherheitslücken ungepatchter Microsoft SQL 2000 Server ausgenutzt und sich rasant verbreitet hat, sind der beste Beweis. Der Netzwerk-Schutz ist oftmals lückenhaft, weil die Installation von Patches bis vor kurzem viel zu umständlich war und daher vernachlässigt wurde. Die Verwaltung von Patches kann mittlerweile jedoch von ausgereiften Patch-Management-Lösungen übernommen werden, sodass keine Gefahr mehr von fehlenden Patches ausgeht.

Dieses White Paper informiert Sie, wie Ihr Netzwerk-Schutz durch den gemeinsamen Einsatz des GFI LANguard Network Security Scanner (N.S.S.) mit den Microsoft Software Update Services (SUS) stets auf den neuesten Stand gehalten werden kann.

Einführung	2
Implementierung der Patch-Management-Lösungen in Ihrem Netzwerk.....	3
Zusammenfassung	8
Über GFI	9

Über GFI LANguard Network Security Scanner (N.S.S.)

GFI LANguard N.S.S. ist der führende Sicherheits-Scanner für Windows-Systeme. Er überprüft Ihr Netzwerk auf potenzielle Sicherheitslücken, indem das gesamte System unter anderem nach fehlenden Sicherheits-Patches und Service Packs, offenen Freigaben und Ports sowie nicht verwendeten Benutzerkonten durchsucht wird. Dank seiner leistungsfähigen Berichtsfunktionen können Sie Ihr Netzwerk noch besser gegen Hacker-Angriffe absichern. GFI LANguard N.S.S. ermöglicht zudem die Remote-Verteilung fehlender Patches und Service Packs für Applikationen und Betriebssystemen.

Über Microsoft Software Update Services (SUS)

Microsoft SUS ist ein kostenfreies Tool zur Patch-Verwaltung, das Netzwerk-Administratoren beim Verteilen von Sicherheits-Patches unterstützt. Vereinfacht gesehen ist Microsoft SUS eine Variante des Windows Update-Dienstes, die bei Netzwerken zum Einsatz kommt. Stehen neue

Windows-Updates bereit, greifen die einzelnen Workstations jedoch nicht auf das Internet, sondern auf den Microsoft SUS-Server zu und laden die Updates von diesem Server herunter. Die Verbindung zu Windows-Update und somit zum öffentlichen Internet erfolgt somit nur über den Microsoft SUS-Server.

Über den Windows Update-Service erhält der Microsoft SUS-Server alle Informationen zu sicherheitsrelevanten Updates und verteilt diese dann zusammen mit den zugehörigen Patches automatisch an die einzelnen Workstations und Server in Ihrem Netzwerk. Der Microsoft SUS-Server ermöglicht es Administratoren, die Verteilung von Updates gezielt zu steuern: Alle Aktualisierungen, die über die öffentliche Windows Update-Site zur Verfügung gestellt werden, können vor der Verteilung im firmeninternen Netzwerk vom Administrator getestet und freigegeben werden. Die Verteilung und Installation erfolgt dann nach einem vom Systembeauftragten festgelegten Zeitplan.

Warum GFI LANguard N.S.S. mit dem Microsoft SUS-Server kombinieren?

Microsoft SUS stellt eine gute Lösung für die Verteilung von Betriebssystem-Patches dar. Es werden alle Arten von Betriebssystem-Patches unterstützt, auch Patches für Applikationen, die Bestandteil des Betriebssystems sind (z. B. IIS und IE).

Einschränkungen des Microsoft SUS-Servers

Folgende Funktionen werden von Microsoft SUS jedoch nicht unterstützt und stehen nur über GFI LANguard N.S.S. zur Verfügung:

- Sofortige Verteilung und Installation von Patches (besonders wichtig bei neuen Viren, die versuchen, als kritisch eingestufte Sicherheitslöcher auszunutzen).
- Installation von Patches für Microsoft-Applikationen und Service Packs für MS Office, MS SQL Server, MS Exchange Server und MS ISA Server.
- Überprüfung der korrekten Installation aller Patches anhand zuverlässiger Berichte.
- Verteilung von Patches an Rechner mit Windows NT.
- Verteilung von Software-Patches und Software von Drittanbietern.

Aus diesem Grund gewährleistet der gemeinsame Einsatz von GFI LANguard N.S.S. und Microsoft SUS, dass Windows-Rechner in allen sicherheitsrelevanten Bereichen immer auf dem neuesten Stand sind.

Implementierung der Patch-Management-Lösungen in Ihrem Netzwerk

Schritt 1: Installation des Microsoft SUS-Servers

Die Konfigurierung des Microsoft SUS-Servers ist im Vergleich zu anderen Patch-

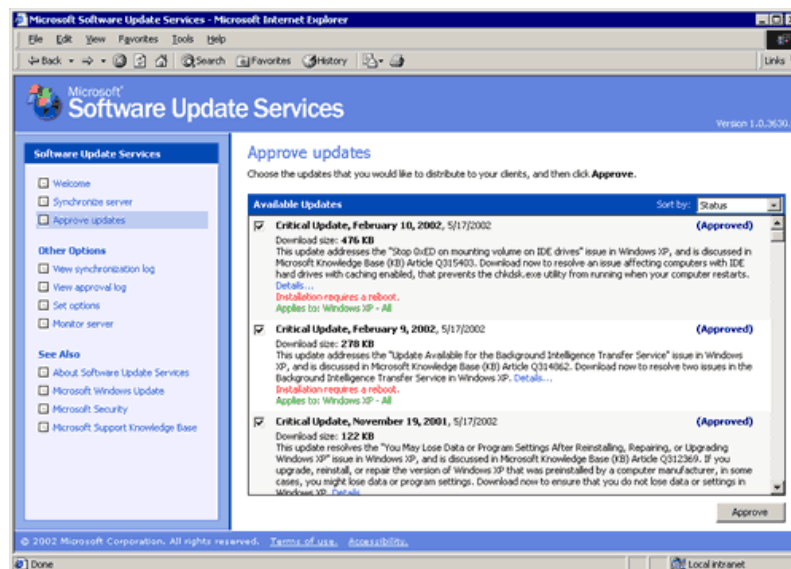
Management-Tools etwas aufwändiger, da es sich um kein Desktop-basiertes Scan-Werkzeug handelt, sondern vielmehr um einen automatisierten Server, der seine Arbeit im Hintergrund verrichtet. Nach der erfolgreichen Einrichtung des Servers verläuft die Patch-Verwaltung jedoch vollkommen automatisch und verringert somit den Verwaltungsaufwand erheblich.

Die Installation ist sehr einfach. Installieren Sie den Microsoft SUS-Server (erfordert IIS), und richten Sie ihn so ein, dass er nach Updates sucht. Zusätzlich müssen Sie sicherstellen, dass auf Ihren Workstations und Servern entweder Windows 2000 SP3, Windows XP SP1, Windows 2003 oder der Microsoft SUS-Client installiert ist. Bitte beachten Sie, dass Windows NT nicht unterstützt wird.

Der SUS-Client lässt mit Hilfe der Funktion "Deploy Custom Software" von GFI LANguard N.S.S. und der Gruppenrichtlinien schnell verteilen. Danach müssen Sie die Client-Workstations über die Gruppenrichtlinien so konfigurieren, dass sie die automatischen Updates von Ihrem SUS Server abrufen. Eine ausführliche Anleitung hierzu finden Sie in der Microsoft-Dokumentation zu den SUS.

Verwaltung des Microsoft SUS-Servers

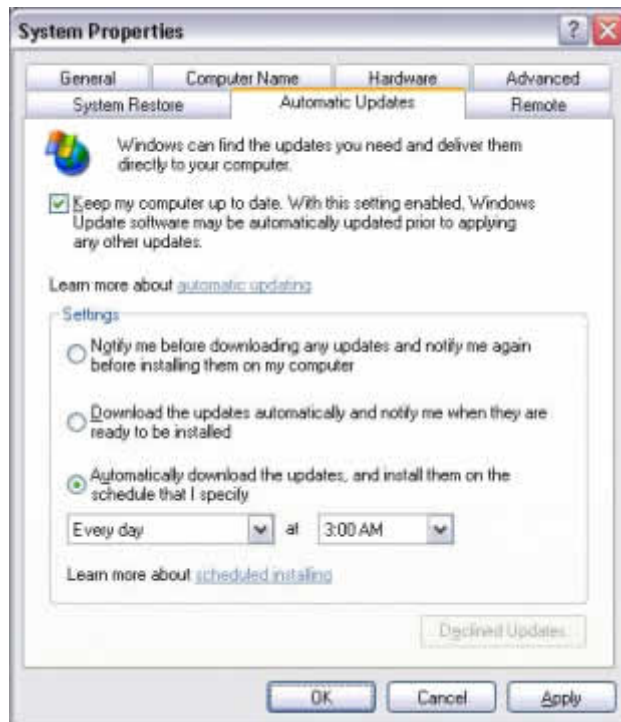
Da die Administration des Microsoft SUS-Servers vollständig Web-basiert ist, können Sie ihn per Fernzugriff verwalten. Alle verfügbaren Updates werden vom Microsoft SUS-Server automatisch heruntergeladen. Sind neue Aktualisierungen erhältlich, werden Sie per E-Mail darüber informiert. Diese Updates können Sie dann für die Verteilung freigeben oder auch ablehnen. So behalten Sie stets die Kontrolle über alle Installationen in Ihrem Netzwerk. Zwischen der Freigabe-Oberfläche und dem Windows-Update-Interface für Aktualisierungen von Einzelrechnern besteht kein großer Unterschied.



Freigabe von Updates über das Verwaltungs-Interface des Microsoft SUS-Server

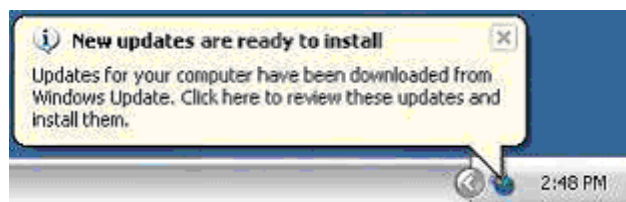
Der Microsoft SUS-Client

Sind Microsoft SUS-Server und -Client installiert, werden alle Updates automatisch verteilt. Als Administrator können Sie die Details hierfür genau festlegen. Patches lassen sich nach einem festen Zeitplan verteilen, wobei die Installation vom einzelnen Benutzer begrenzt beeinflusst werden kann, sofern Sie dies wünschen. Der folgende Screenshot zeigt die zur Verfügung stehenden Optionen. Diese lassen sich mit Hilfe der Gruppenrichtlinien selbstverständlich auch sperren.



Registerkarte “Automatic Updates” mit verschiedenen Einstellungsoptionen

Ist der Microsoft SUS-Client vollständig konfiguriert, werden die Patches automatisch verteilt. Sind neue Updates verfügbar, werden Benutzer über eine Nachricht in der Task-Leiste informiert (siehe Abbildung).



Neue Updates werden über die Task-Leiste angekündigt

Schritt 2: Patch-Verwaltung mit GFI LANguard N.S.S.

Nachdem der Microsoft SUS Server in Ihrem Netzwerk einsatzbereit ist, muss GFI LANguard N.S.S installiert werden, damit folgende Bereiche der Patch-Verwaltung ebenfalls zur Verfügung stehen:

- Installation von Patches für Microsoft-Applikationen und Service Packs für MS Office, MS SQL Server, MS Exchange Server und MS ISA Server.
- Überprüfung, ob fehlende Patches und Service Packs korrekt installiert werden konnten (inklusive HTML-Kontrollbericht).
- Verteilung von Patches an Rechner mit Windows NT.
- Patch-Installation für Drittanbieter-Software (eignet sich auch zur Installation von Virensignatur-Updates).
- Sofortige Installation wichtiger Patches in Notfällen, wo die Verteilung per SUS nicht zeitnah genug erfolgen kann.

Suche nach fehlenden Patches mit GFI LANguard N.S.S.

Nachdem Sie den N.S.S. installiert haben, ist es wichtig, dass Sie Ihr Netzwerk regelmäßig scannen. Nur so können Sie sicher sein, dass sämtliche Patches und Service Packs von Microsoft SUS verteilt wurden. Der Scan-Vorgang nimmt nicht viel Zeit in Anspruch, und der N.S.S. informiert Sie unter dem Knoten "Alerts" zu allen fehlenden Patches und SPs.

Bevor Sie mit dem Scannen Ihres Netzwerkes beginnen, geben Sie einfach den zu überprüfenden IP-Bereich ein. Um die zu scannenden Rechner festzulegen, können Sie ebenso den Scan-Assistenten nutzen, der über das Menü "File" gestartet wird. Es lassen sich komplette Domänen, einzelne Rechner oder ein kompletter IP-Bereich überprüfen. Jedes vom N.S.S. gefundene Gerät wird sofort im linken Fenster der N.S.S.-Oberfläche angezeigt. Im rechten Fenster werden Sie über den Verlauf und aktuellen Stand des Scan-Prozesses detailliert informiert.

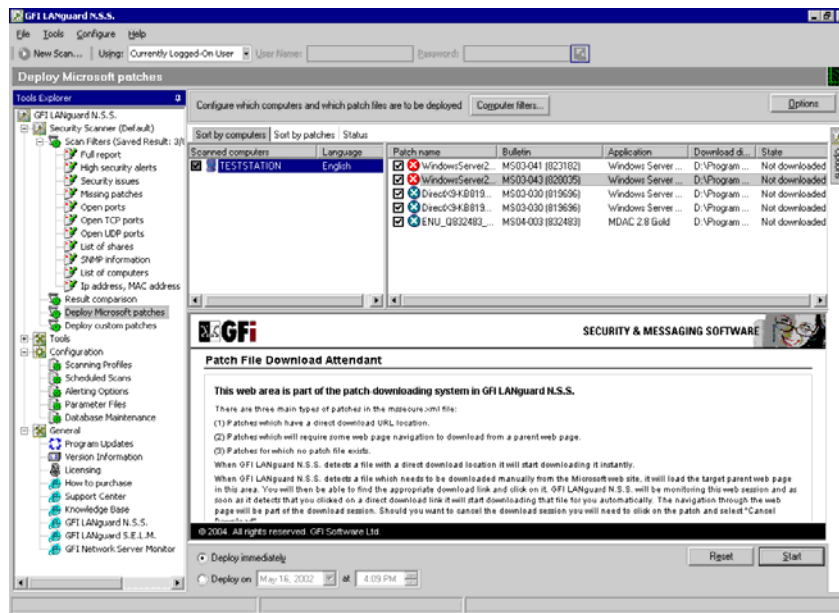
Ist der Netzwerk-Scan abgeschlossen, finden Sie fehlende Patches und Service Packs unter dem Knoten "Vulnerabilities". Funktioniert die Aktualisierung der Client-Rechner per Microsoft SUS einwandfrei, werden Sie nur über fehlende Applikations-Patches und SPs informiert.



Informationen zu fehlenden Patches

Mit einem rechten Mausklick auf einen Patch oder ein SP können Sie dessen Verteilung und

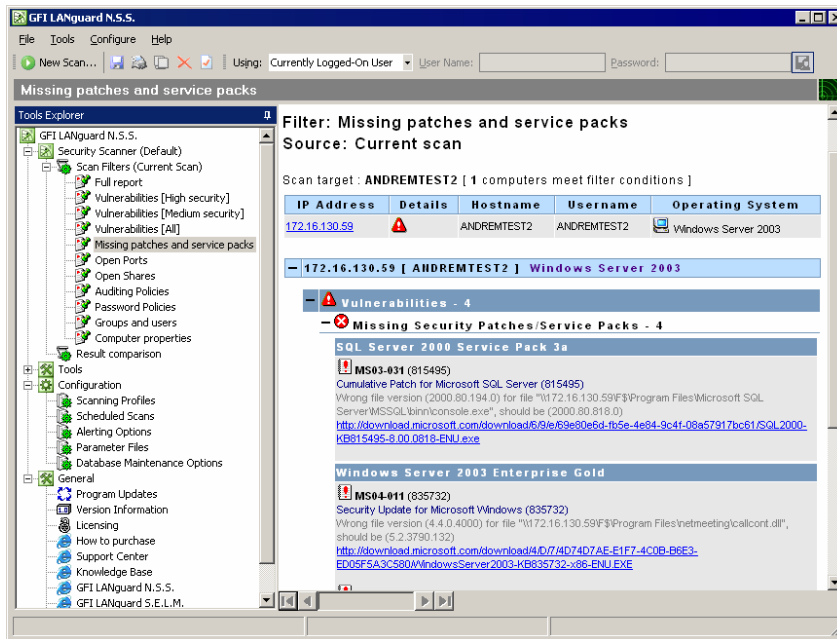
Installation auf dem entsprechenden Rechner oder allen Computern veranlassen. Über den im folgenden Screenshot abgebildeten Knoten für die Patch-Verteilung lässt sich schnell festlegen, welche Patches den einzelnen Rechnern zugewiesen werden sollen.



Installation von Patches

Schritt 3: Berichterstellung

Nach dem Scannen Ihres Netzwerks können Sie einen präzisen Bericht erstellen lassen, in dem alle fehlenden Patches und Service Packs aufgeführt sind. Hierfür rufen Sie einfach das Menü "File" auf, gehen auf "Filters" und wählen dann "Missing patches".



N.S.S.-Bericht zu fehlenden Patches und Service Packs

Zusammenfassung

Mit Microsoft SUS steht Ihnen ein sehr gutes Tool zur Patch-Verwaltung zur Verfügung, das zudem auch noch kostenfrei ist. Leider unterstützt es jedoch nicht die Verteilung von Patches für Microsoft-Applikationen wie Office, Exchange oder SQL Server. Eine umfassende Scan-Funktionalität fehlt ebenfalls: Deployment-Protokolle müssen manuell überprüft werden, um herauszufinden, ob die Verteilung von Patches erfolgreich war.

Microsoft SUS Server eignet sich hervorragend für die Verwaltung von Betriebssystem-Patches. Obwohl Sie an Stelle des Microsoft SUS-Servers auch nur ein Patch-Management-Produkt einsetzen können, sparen Sie mit der Microsoft-Lösung trotz der anfangs aufwändigen Konfigurierung auf Dauer gesehen sehr viel Zeit – und halten Ihr Netzwerk immer automatisch auf dem neuesten Stand. Die Entscheidung für Microsoft SUS-Server als Verwaltungs-Tool sollte daher leicht fallen, auch wenn die Software nicht alle Bereiche des Patch-Managements abdeckt. Diese Lücke muss durch ein ergänzendes Patch-Management-Tool wie GFI LANguard Network Security Scanner geschlossen werden.

Die Verbindung von GFI LANguard N.S.S mit Microsoft SUS bietet sämtliche Funktionen, die sonst nur in weitaus kostenintensiveren Patch-Management-Lösungen zu finden sind. Je nach Anzahl der zu verwaltenden Rechner können bei solchen Produkten die Kosten zwischen US\$ 1.500 (100 Rechner) und US\$ 8.000 (500 Rechner) liegen. Beim gemeinsamen Einsatz von GFI LANguard N.S.S. und Microsoft SUS können Sie mit SUS Ihr Betriebssystem aktualisieren (Windows 2000, XP, .NET, inkl. IIS, IE, Windows Media) und mit dem N.S.S. SPs,

Patches für Microsoft-Anwendungen, Windows NT-Patches und Software von Drittanbietern auf den neuesten Stand bringen.

Wenn Sie GFI LANguard N.S.S. zusammen mit Microsoft SUS verwenden, erhalten Sie ein leistungsstarkes und flexibles Patch-Management zu einem konkurrenzlos günstigen Preis – Microsoft SUS ist kostenfrei, und GFI LANguard N.S.S. ist bereits ab EUR 295,- (25 IPs, zzgl. gesetzl. MwSt.) erhältlich. Weitere Informationen zu GFI LANguard N.S.S. und eine kostenfreie Testversion finden Sie unter <http://www.gfisoftware.de/de/lannetscan>.

Über GFI

GFI (www.gfisoftware.de) ist ein führender Entwickler und Anbieter von Produkten für Netzwerk- und Inhaltssicherheit sowie von Kommunikationslösungen. Das Produktportfolio von GFI umfasst unter anderem den Netzwerk-Fax-Server GFI FAXmaker for Exchange/SMTP, die Sicherheitslösung GFI MailSecurity for Exchange/SMTP zur Überprüfung von E-Mail-Inhalten und zum Schutz vor E-Mail-basierten Exploits und Viren, die Server-basierte Anti-Spam-Software GFI MailEssentials for Exchange/SMTP, GFI LANguard Network Security Scanner (N.S.S.) für Sicherheits-Scans und Patch-Management, GFI Network Server Monitor zum automatischen Versand von Warnmitteilungen und zur Fehlerbehebung bei Netzwerk- und Server-Problemen, GFI LANguard Security Event Log Monitor (S.E.L.M.) zur Ereignisprotokoll-basierten Eindringlingserkennung und netzwerkweiten Verwaltung von Ereignisprotokollen sowie GFI LANguard Portable Storage Control (P.S.C.) zur netzwerkweiten Kontrolle wechselbarer Speichermedien. GFI-Produkte sind im Einsatz bei Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, der US-Steuerbehörde IRS und der USAF. GFI unterhält Niederlassungen in den USA, Großbritannien, Deutschland, Zypern, Rumänien, Australien und Malta und wird von einem weltweiten Netzwerk von Distributoren unterstützt. GFI ist "Microsoft Gold Certified Partner" und erhielt die Auszeichnung "Microsoft Fusion (GEM) Packaged Application of the Year". Weitere Informationen erhalten Sie unter <http://www.gfisoftware.de>.

© 2004 GFI Software Ltd. Alle Rechte vorbehalten. Die in diesem Dokument aufgeführten Informationen geben den von GFI zum Zeitpunkt der Veröffentlichung vertretenen Standpunkt zum Thema des White Papers wieder. Änderungen aufgrund von veränderten Marktbedingungen sind vorbehalten. Die in diesem Dokument präsentierten Informationen stellen keine Verpflichtung seitens GFI dar, und für ihre Genauigkeit wird nach dem Datum der Veröffentlichung keine Garantie übernommen. Dieses White Paper dient nur der Produktinformation. GFI ÜBERNIMMT KEINE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE HAFTUNG FÜR DIE IN DIESEM DOKUMENT PRÄSENTIERTEN INFORMATIONEN. GFI, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity und die zugehörigen Produkt-Logos sind eingetragene Marken oder Marken von GFI Software Ltd. in den Vereinigten Staaten und/oder anderen Ländern. Alle in diesem Dokument aufgeführten Produkte oder Firmennamen sind Eigentum der jeweiligen Inhaber.