
Patchmanagement met GFI LANguard N.S.S. & Microsoft SUS

Een rendabele en gemakkelijke oplossing voor
netwerkwijd patchmanagement

In dit white paper kunt u lezen hoe u de GFI LANguard Network Security Scanner (N.S.S.) en Microsoft Software Update Services (SUS) kunt gebruiken om uw netwerk automatisch bij te werken met de nieuwste veiligheidspatches.

Inleiding

Patchmanagement is één van de belangrijkste onderdelen van netwerkbeheer. Patchmanagement bestaat uit het scannen van machines op het netwerk voor ontbrekende patches en het installeren van deze patches zodra ze beschikbaar zijn. Als u dit niet doet wordt uw netwerk twee keer zo kwetsbaar: het netwerk is kwetsbaar én dit feit is nu openbaar gemaakt. Hierdoor is de kans groter dat uw netwerk zal worden misbruikt door kwaadaardige gebruikers, hackers en virusschrijvers.

Veel netwerkbeheerders vergeten echter om de juiste patches te installeren. Het bewijs hiervoor wordt geleverd door wormen zoals Slammer, de worm die zich in 2003 wist te verspreiden door bekende kwetsbaarheden in ongepatchte Microsoft SQL 2000 servers. Tot voor kort was de belangrijkste reden hiervoor het feit dat het installeren van patches een hele klus was. Dankzij de komst van geavanceerde tools voor patchmanagement is dit nu verleden tijd.

In dit white paper kunt u lezen hoe u de GFI LANguard Network Security Scanner (N.S.S.) en Microsoft Software Update Services (SUS) kunt gebruiken om uw netwerk automatisch bij te werken met de nieuwste veiligheidspatches.

Inleiding	2
Implementatie van patchmanagement op uw netwerk.....	3
Conclusie.....	8
Over GFI.....	9

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

GFI LANguard N.S.S. is de toonaangevende Windows security scanner. GFI LANguard Network Security Scanner (N.S.S.) controleert uw netwerk op mogelijke veiligheidsrisico's door uw gehele netwerk te scannen op ontbrekende veiligheidspatches, service packs, open shares, open poorten, ongebruikte gebruikersaccounts en meer. Dankzij de handige rapportagefuncties kunt u uw netwerk nog beter tegen hackers beschermen. GFI LANguard N.S.S. kan ook vanop afstand ontbrekende patches en service packs in applicaties en besturingssystemen plaatsen.

Over Microsoft Software Update Services (SUS)

Microsoft SUS is een gratis tool voor patchmanagement van Microsoft waarmee netwerkbeheerders gemakkelijker veiligheidspatches kunnen installeren. Simpel gezegd is Microsoft SUS een versie van Windows Update die u op uw netwerk kunt runnen. In plaats van dat elk werkstation met het internet verbinding moet maken om Windows te updaten, maakt elk werkstation verbinding met de Microsoft SUS Server om de updates binnen te halen. Alleen de Microsoft SUS Server heeft toegang tot het internet en Windows Update nodig.

Door verbinding te maken met Windows Update meldt Microsoft SUS Server kritieke updates

en worden deze updates automatisch over uw werkstations en servers verdeeld. Microsoft SUS server geeft de beheerder controle over updates: de beheerder kan updates van de openbare Windows Update site testen en goedkeuren voordat ze op het intranet worden geïnstalleerd. De installatie verloopt volgens de planning van de beheerder.

Waarom is het goed om GFI LANguard N.S.S. en Microsoft SUS server te combineren?

Microsoft SUS server is een goede oplossing voor de verdeling van besturingssysteempatches. Alle besturingssysteempatches worden ondersteund, inclusief patches voor applicaties die deel uitmaken van het besturingssysteem (bijvoorbeeld IIS en IE). -{ }-

Beperkingen aan Microsoft SUS Server

Microsoft SUS biedt echter niet de volgende functies die wel worden geboden door GFI LANguard N.S.S.:

- Onmiddellijke installatie van patches (dit is bijzonder belangrijk in het geval van gevaarlijke virusuitbraken die onmiddellijke patchinstallatie vereisen)
- Installatie van patches voor Microsoft applicaties en service packs voor Microsoft Office, Microsoft SQL Server, Microsoft Exchange Server en Microsoft ISA Server.
- De mogelijkheid om te controleren of alle patches juist zijn geïnstalleerd
- Installatie van patches op computers met Windows NT
- Installatie van software patches en software van derden.

GFI LANguard N.S.S. en Microsoft SUS vormen dus de ideale combinatie om uw Windowscomputers up-to-date te houden.

Implementatie van patchmanagement op uw netwerk

Stap 1: Installatie van Microsoft SUS server

Doordat Microsoft SUS server een geautomatiseerde server is die op de achtergrond werkt en niet desktopgebaseerd is, is de configuratie wat ingewikkelder dan bij andere tools voor patchmanagement. Na de configuratie verloopt het patchmanagement echter geheel automatisch, dus het is de moeite waard.

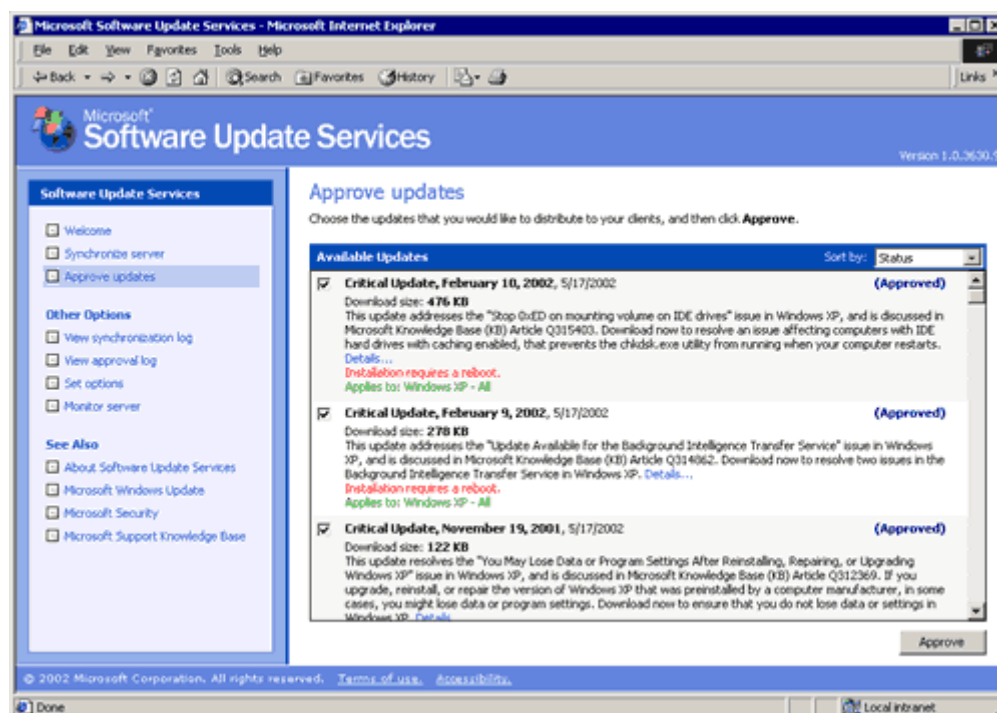
De installatieprocedure is vrij eenvoudig. U installeert de Microsoft SUS server (hiervoor is IIS vereist) en configureert deze om naar updates te zoeken. Vervolgens moet u zich ervan verzekeren dat op uw werkstations en servers Windows 2000 SP3, Windows XP SP1/SP2, Windows 2003 of de Microsoft SUS client geïnstalleerd is. Windows NT wordt niet ondersteund.

U kunt de SUS client gemakkelijk installeren met behulp van de functie 'deploy custom software' van GFI LANguard N.S.S. en de Group Policy. Vervolgens moet u de Group Policy

weer gebruiken om de werkstations zo te configureren dat ze de automatische updates van uw SUS server halen. Dit wordt duidelijk omschreven in de documentatie bij Microsoft SUS.

Beheer van de Microsoft SUS server

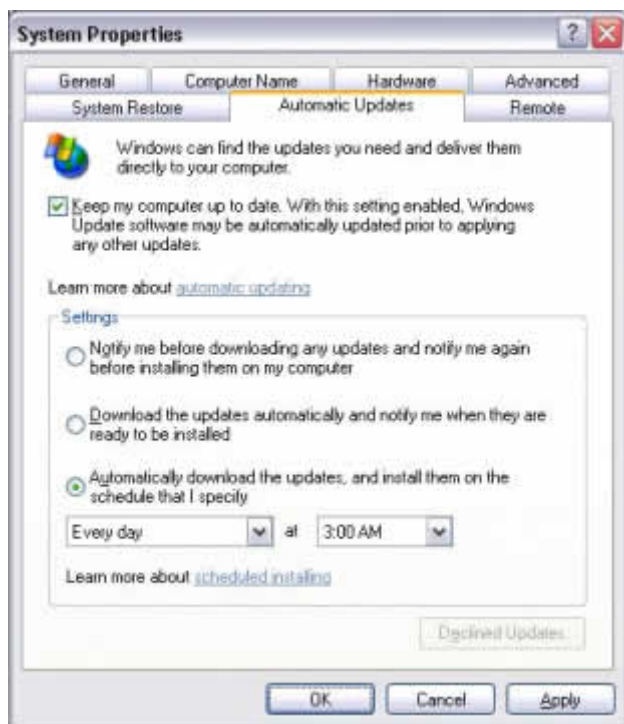
Het beheer van Microsoft SUS server is volledig webgebaseerd. Beheer op afstand behoort dus tot de mogelijkheden. De Microsoft SUS server downloadt alle beschikbare updates automatisch en brengt u via e-mail op de hoogte van nieuwe updates. Nieuwe updates kunnen worden goedgekeurd voor installatie of afgekeurd. U heeft dus volledige controle over wat er op uw netwerk wordt geïnstalleerd. Het goedkeuren verloopt grotendeels op dezelfde manier als het updaten van een enkele machine met behulp van Windows Update.



Het goedkeuren van updates via de beheerinterface van Microsoft SUS

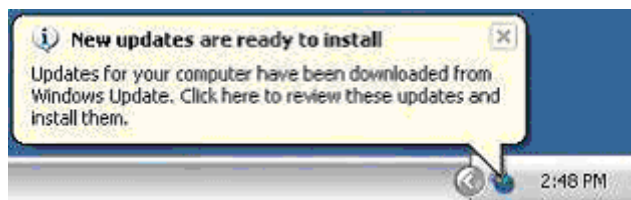
De Microsoft SUS client

Als u eenmaal zowel de Microsoft SUS server als de Microsoft SUS client heeft geïnstalleerd, worden alle updates automatisch gedistribueerd. Als beheerder kunt u configureren hoe dit moet gebeuren. U kunt bepalen wanneer dit moet gebeuren en indien gewenst kunt u de gebruiker een zekere mate van controle over het proces geven. In het onderstaande screenshot ziet u de beschikbare opties. Uiteraard kunt u deze opties blokkeren met behulp van Group Policy.



Configuratiescherm “Automatic Updates” met opties

Nadat u de Microsoft SUS client heeft geconfigureerd, worden de patches automatisch geïnstalleerd. De gebruiker wordt geïnformeerd door middel van een bericht in de taakbalk (zie afbeelding).



Nieuwe updates worden aangekondigd in de taakbalk

Stap 2: Patch management met GFI LANguard N.S.S.

Als de Microsoft SUS server eenmaal op uw netwerk staat, moet u GFI LANguard N.S.S. installeren om de volgende taken uit te voeren:

- Installatie van patches voor Microsoft applicaties en service packs voor Microsoft Office, Microsoft SQL Server, Microsoft Exchange Server en Microsoft ISA Server
- Controleren of ontbrekende patches en service packs zijn geïnstalleerd en het verzenden van HTML-rapporten hierover
- Installatie van patches op computers met Windows NT
- Installatie van softwarepatches van andere fabrikanten (kan ook worden gebruikt voor de

installatie van virus signature updates)

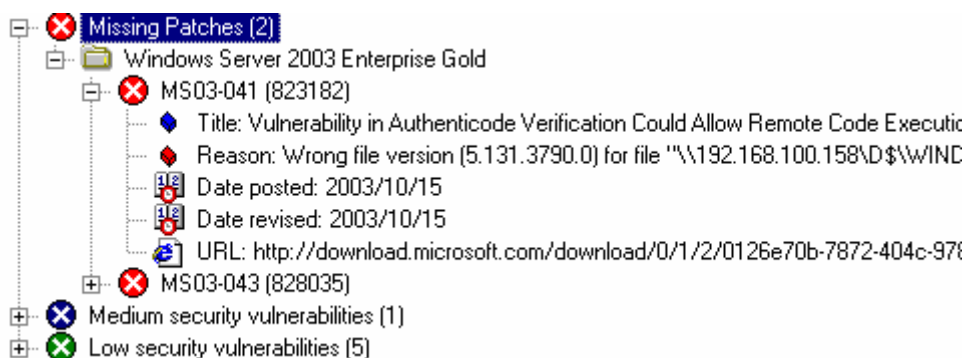
- Onmiddellijke installatie van belangrijke patches in noodgevallen waarin men het zich niet kan veroorloven om op SUS te wachten.

Zoeken naar ontbrekende patches met GFI LANguard N.S.S.

Als N.S.S. eenmaal is geïnstalleerd, is het belangrijk om uw netwerk regelmatig te scannen om te controleren of alle patches en service packs door Microsoft SUS zijn gedistribueerd. GFI LANguard N.S.S. scant snel uw netwerk en informeert u onder de Alerts node over alle ontbrekende patches en service packs.

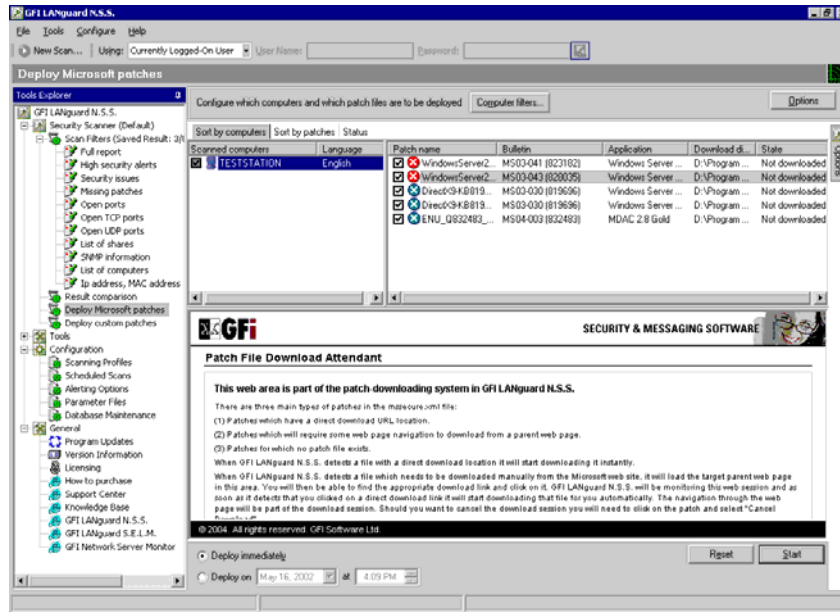
Voordat u begint met het scannen van uw netwerk voert u het IP-bereik in bovenin de scanner interface. U kunt ook de Scan Wizard (onder Bestand) gebruiken om te specificeren welke computers gescand moeten worden. U kunt domeinen, specifieke computers of een volledig IP-bereik scannen. Klik op Finish om het scanproces te starten. Elke door GFI LANguard gevonden machine verschijnt in het linkerpaneel. In het rechterpaneel vindt u gedetailleerde voortgangsinformatie.

Als de scan eenmaal compleet is, vindt u ontbrekende patches en service packs onder de node "Vulnerabilities". Als Microsoft SUS alle clientmachines correct bijwerkt, ziet u hier alleen ontbrekende applicatiepatches.



Informatie over ontbrekende patches

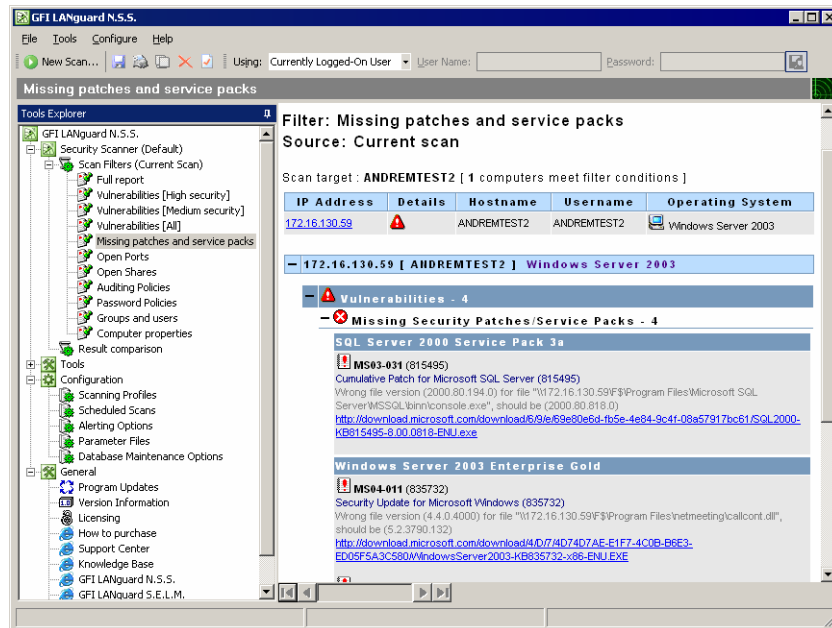
Door met de rechtermuisknop op een patch of service pack te klikken kunt u deze op de gewenste computer(s) installeren. Met de node "Deploy Patches" (zie screenshot) kunt u gemakkelijk specificeren welke patches u op welke computers willen installeren.



Installatie van patches

Stap 3: Rapportage

Als u uw netwerk eenmaal heeft gescand, kunt u ook een beknopt rapport creëren met een lijst van alle ontbrekende patches and service packs. Ga naar Bestand > Filters en selecteer "Missing patches" om een dergelijk rapport te genereren.



GFI LANguard N.S.S. rapport over ontbrekende patches/service packs

Conclusie

Microsoft SUS Server is perfect geschikt voor het beheer van besturingssysteempatches. Hoewel u ook een product voor patchmanagement zou kunnen gebruiken, kunt u met Microsoft SUS Server op de lange termijn veel tijd besparen. Na de installatie is het gemakkelijk om uw netwerk up-to-date te houden. Als u ook nog bedenkt dat Microsoft SUS Server gratis is, is de keuze eenvoudig. Het patchmanagement van Microsoft SUS Server is echter niet volledig. Microsoft SUS Server installeert geen patches voor applicatiesoftware zoals Office, Exchange of SQL Server. Bovendien kan hij niet scannen: u moet de logs bekijken om te controleren of de patches met succes zijn geïnstalleerd. Naast Microsoft SUS Server moet u dus een tool voor patchmanagement gebruiken.

GFI LANguard N.S.S. in combinatie met Microsoft SUS biedt alle functies die u tegenkomt in duurdere oplossingen voor patchmanagement voor een minimale prijs. De meeste producten voor patchmanagement kosten \$1,500 voor 100 computers en \$8,000 of meer voor 500 computers. Met de combinatie van GFI LANguard N.S.S. en Microsoft SUS kunt u besturingssystemen updaten met behulp van Microsoft SUS (Windows 2000, XP, .NET, IIS, IE, Windows Media) en service packs, Microsoft applicatiepatches, Windows NT patches en software van derden met behulp van GFI LANguard N.S.S.

De gecombineerde oplossing van GFI LANguard N.S.S. en Microsoft SUS is niet alleen krachtiger en flexibeler, maar ook goedkoper: Microsoft SUS is gratis en licenties voor GFI LANguard N.S.S. zijn al verkrijgbaar vanaf €450 voor 32 IP's. Ga naar <http://www.gfi.nl/nl/lannetscan/> voor meer informatie over dit product en een gratis trialversie.

Over GFI

GFI is een toonaangevende ontwikkelaar van software voor netwerkbeveiliging, inhoudsbeveiliging en messaging. Dankzij bekroonde technologie, een agressieve prijsstrategie en een sterke focus op MKB-bedrijven helpt GFI bedrijven over de hele wereld om maximale continuïteit en productiviteit te bewerkstelligen. GFI is opgericht in 1992 en heeft kantoren in Malta, Londen, Raleigh, Hong Kong, Adelaide en Hamburg die wereldwijd meer dan 200.000 installaties ondersteunen. GFI is een kanaalgericht bedrijf met meer dan 10.000 partners over de hele wereld. GFI is ook een Microsoft Gold Certified Partner. Meer informatie over GFI is te vinden op <http://www.gfi.nl>.

© 2007 GFI Software Ltd. Alle rechten voorbehouden. De informatie in dit document geeft het standpunt van GFI weer betreffende de besproken onderwerpen op de datum van publicatie. Aangezien GFI moet reageren op veranderende marktomstandigheden, moet dit document niet als een toezegging van GFI worden geïnterpreteerd. Na de publicatiedatum kan de correctheid van de informatie niet worden gegarandeerd. Dit white paper dient puur ter informatie. GFI GEEFT IN DIT DOCUMENT GEEN ENKELE GARANTIE, EXPLICIET NOCH IMPLICIET. GFI, GFI EndPointSecurity, GFI EventsManager, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor en de bijbehorende logo's zijn ofwel geregistreerde handelsmerken of handelsmerken van GFI Software Ltd. in de Verenigde Staten en/of andere landen. Alle product- en bedrijfsnamen in dit persbericht zijn mogelijk handelsmerken van hun respectievelijke eigenaren.

