Info von COMPUS Computer GmbH zum Thema Netzwerksicherheit

1. Einleitung und Übersicht

Wir wollen Sie über die Situation Ihres Microsoft-Netzwerkes bezüglich Sicherheit kurz informieren und dabei mögliche Maßnahmen zur Verbesserung vorschlagen. Bitte haben Sie Verständnis dafür, daß diese Darstellung naturgemäß unvollständig sein muß, da das Thema sehr komplex ist.

Es geht in dieser Information um zwei Themen:

- Wie kann ich dafür sorgen, daß meine Software bezüglich Servicepacks und Patches auf dem aktuellen Stand ist? Von besonderer Bedeutung ist dabei das Serverbetriebssystem (z. B. Windows 2000 Server), das Arbeitsplatzbetriebssystem (z. B. Windows XP) und die Anwendungssoftware Office (z. B. Office XP).

- Wie kann ich dafür sorgen, daß mein Virenschutz optimal funktioniert?

Es geht in diesem Infobrief nicht um weitergehende Sicherheitsmaßnahmen wie Firewalls, Datensicherung, organisatorische Sicherheitsrichtlinien etc. Wenn Sie hier Beratungsbedarf haben, sollten Sie sich von uns beraten lassen und ggf. einen **Sicherheitscheck** von uns durchführen lassen: **consulting@compus.de**

2. Abgrenzung Softwareupdates versus Virenschutz

Softwareupdates (darunter fallen die Begriffe Softwareupdate, Servicepack, Hot Fix, Patch etc.) sind unter anderem dazu da, erkannte Sicherheitslücken in der Software zu beheben. Dabei ist es entscheidend, daß vor der Installation eines Softwareupdates (z. B. SP 4 für Windows 2000 Server) geprüft wird, ob dieses Update auch von der eingesetzten Anwendungssoftware (z. B. DATEV) freigegeben wurde.

Der Virenschutz dient dazu, alle Daten, dabei insbesondere eingehende E-Mails, auf solche „Besonderheiten“ zu untersuchen, die in den bisher bekannten Internetattacken, dabei insbesondere auch E-Mail-Attacken, vorkommen. Internet-Attacken nutzen dabei entweder Sicherheitslücken in der Software aus oder sie verwenden das Netzwerk ganz normal in den Grundfunktionen. Durch Softwareupdates lassen sich lediglich die vom Hersteller der Software aktuell erkannten Sicherheitslücken beheben. Und umgekehrt kann der Virenschutz auch nicht alle erkannten Internet-Attacken abfangen.

Da es technisch und kostenmäßig nicht praktikabel ist, die gesamte eingesetzte Software im Netzwerk immer auf dem aktuellen Stand zu halten und dies wegen der eingesetzte Anwendungssoftware auch meist nicht möglich ist, kommt dem Virenschutz besondere Bedeutung zu. Dabei hat der Virenschutz auch die

Aufgabe, Internet-Attacken, die nichts mit Sicherheitslücken unseres Systems zu tun haben, zu erkennen und geeignete Maßnahmen auszulösen. Er schützt das Netzwerk weitgehend im Hinblick auf alle bekannten Internet-Attacken. Internet-Attacken, die noch nicht als solche erkannt wurden, kann der Virenschutz naturgemäß nicht erkennen und abwehren. Und wie bereits ausgeführt kann der Virenschutz auch nicht alle bekannten Internet-Attacken abfangen.

Für die Beschreibung der Problematik und der Unterschiede von Internet-Attacken (Virus, Wurm, Trojanisches Pferd etc.) verweisen wir auf den sehr interessanten Übersichtsartikel ***Epidemic*** des Magazins **Business Week** vom 8. September 2003:

3. Empfehlung zu Softwareupdates und Patches

Dazu finden Sie umfassende Informationen auf der Microsoft-Webseite:

www.microsoft.com

Wichtige Hinweise finden Sie insbesondere auf der Microsoft Webseite unter Security:

http://www.microsoft.com/security/

Die wichtigsten Schritte hin zu einem sicheren PC finden Sie unter folgendem Link, wobei hier etwas Vorsicht angebracht ist, da sich diese Hinweise nicht immer so umsetzen lassen:

http://www.microsoft.com/security/protect/

Wenn Sie z. B. von jedem Ihrer PCs im Netzwerk die Updates automatisch aus dem Internet downloaden, bekommen Sie ein Problem, wenn Sie keinen Proxiserver oder einen Software Update Services Server (SUS Server) in Ihrem Netzwerk eingerichtet haben. Denn dann kann es passieren, daß größere Updates von jedem Benutzer geladen werden, was Ihren Internetanschluß hoffnungslos überlasten kann. Für einem Privat-PC sind diese Einstellungen natürlich genau richtig.

Welche Updates bzw. Patches in Ihr Netzwerk wann eingespielt werden sollten, besprechen Sie am besten mit den Consultants von COMPUS. Ferner sollten wir uns über die Installation eines Software Update Services Server (SUS Server) in Ihr Netzwerk unterhalten. Hier ist ein Kompromiß zwischen Sicherheitsbedürfnis und Kosten zu finden. Und ferner ist vorab sicherzustellen, daß die Freigabe der eingesetzten Anwendersoftware vorliegt.

Unsere Empfehlung lautet:

- *Bei größeren Netzwerken sollten Sie einen Software Update Services Server (SUS Server) in Ihrem Netzwerk installieren (ab ca. 10 User). Damit kann in effizienter Weise die Aktualisierung der Microsoft-Software durchgeführt werden. Die Installation und Pflege der SUS ist jedoch aufwendig und kann nur von qualifizierten Spezialisten durchgeführt werden.*

- *Bei kleineren Netzwerken sollten die Updates als Teil der Systempflege zumindest monatlich erfolgen. Bei kritischen Softwarefehlern eventuell sogar täglich.*

- *Informieren sie sich regelmäßig über die aktuellen Stand auf den Microsoft-Webseiten. Wenn Sie Fragen haben, suchen Sie bitte den Kontakt zum COMPUS Consulting über* ***consulting@compus.de***

- *Ferner empfehlen wir Ihnen, den* ***Security Newsletter von Microsoft*** *zu abonnieren, denn darüber erhalten Sie die wichtigsten Informationen zeitnah:* ***www.microsoft.com/technet/security/notify.asp***

4. Empfehlung zum Virenschutz

Viren werden häufig, aber nicht ausschliesslich, über E-Mails in das Netzwerk eingeschleusst.

Für optimalen Virenschutz empfehlen wir Ihnen:

- *Benutzen Sie einen leistungsfähigen Virenschutz wie z. B. NAI oder DATEV-VIWAS. Stellen Sie sicher, daß die Version aktuell ist (Updates oder Nachfolgeversionen)*

- *Sorgen Sie dafür, daß der Virenschutz auf allen Servern und PC aktiv ist.*

- *Sorgen Sie dafür, daß das aktuelle Virenpattern über das Internet geladen wurde und dem Virenschutz zur Verfügung steht. Nur wenn die Virenpattern aktuell sind, ist optimaler Schutz gewährleistet. Dabei ist ein Update der Pattern bezüglich der Mailserver mindestens alle 4 Stunden und bezüglich der Arbeitsplätze mindestens alle 24 Stunden anzustreben.*

- *Lassen Sie alle Arbeiten zu dem Thema Virenschutz nur durch Fachleute erledigen, die dies laufend und damit mit hoher Qualität für Sie erledigen können.*

Aber auch damit ist naturgemäß nicht absolut sichergestellt, daß nicht ein neuer noch unbekannter Virus sich in Ihr System einschleicht.

Fragen an unser Consultingteam: **consulting@compus.de**

5. Zusammenfassung

Wie Sie sehen, erfordert die Aktualisierung Ihrer Netzwerksoftware als auch die Betreuung Ihres Virenschutzes besondere Beachtung und Fachkenntnis. Aber auch damit ist das Risiko nicht vollständig auszuschließen, da es einerseits keine totale Absicherung gibt und andererseits immer ein Kompromiss zwischen Sicherheitsbedürfnis und Kosten gefunden werden muß.