Sicherheit im Netz

Leserbeitrag von "heat" geschrieben am 25.03.2004

Basisvoraussetzungen und -einstellungen für Eure Sicherheit

1. Windows-Patches regelmäßig installieren. Ihr findet Sie unter http://windowsupdate.microsoft.com

2. Virenscanner Benutzt immer einen Virenscanner! Neben vielen kostenpflichtigen Programmen ist AntiVir von H+BEDV ein gutes und zuverlässiges Programm, das darüber hinaus für den Privatgebrauch auch noch kostenlos zu haben ist. Ihr findet es unter www.free-av.de

3. Firewall Den besten Schutz bieten derzeit PC Firewall 2004, ZoneAlarm Pro 4 oder das kostenlose Outpost (http://www.agnitum.com/download/outpost1.html)

4. Sinnlose Accounts löschen Um zu verhindern daß solche Account für Trojaner u.ä. verwendet werden, solltet Ihr alle unbenutzten Accounts in Windows löschen. Dazu geht Ihr in der Systemsteuerung auf Verwaltung, dort auf Computerverwaltung. Unter „Lokale Benutzer und Gruppen" im rechten Fensterabschnitt auf „Benutzer" doppelklicken. Nun könnt Ihr alle Accounts löschen, die Ihr nicht braucht.

5. Remote-zugriff sperren Rechtsklick auf Arbeitsplatz -> Eigenschaften -> Remote und hier alle Häkchen entfernen

Weitere Maßnahmen zur Erhöhung der Sicherheit

6. NetBIOS abstellen (um Unbefugten den Zugriff auf Eurem Rechner zu verwähren) Geht bei Netzwerkumgebung auf Eigenschaften und sucht dort Eure Internetverbindung. Rechtsklick darauf und wiederum Eigenschaften. Hier das TCP/IP-Protokoll markieren -> Eigenschaften; danach unter „Allgemein" die Schaltfläche „Erweitert" betätigen. Geht nun auf WINS; dort könnt Ihr bei den NetBIOS-Einstellungen die Option „NetBIOS über TCP/IP deaktivieren" wählen. NetBIOS ist vom Internet entkoppelt
WICHTIG: da neue Treiber diese unheilige Allianz wieder aufleben lassen könnten solltet Ihr zusätzlich noch die Ports 135-139 an der Firewall für UDP und TCP schließen.

7. RPC-Dienst (ermöglicht Buffer-Overflow-Angriffe, Blaster & Co., Exploit, Backdoor-Programme) Um Euch dagegen abzusichert schließt an Eurer Firewall folgende Ports: 135, 137, 138, 139, 445 und 593 für UDP und TCP

8. Office Beliebte Schwachstellen sind einmal mehr die Microsoft-Produkte Internet Explorer und Outlook. Bei Outlook besteht die Möglichkeit HTML und Skriptsprachen in Nachrichten einzubauen. Dadurch werden die eMails bunt aber auch gefährlich. Oft wird deswegen der Umstieg auf opera oder Pegasus Mail empfohlen. Wollt Ihr auf Outlook nicht verzichten, holt Euch regelmäßig die von Microsoft angebotenen Updates (http://officeupdate.microsoft.com) und schaltet die Vorschau ab (bei Outlook 2003 mit „Ansicht" -> „Lesebereich" -> „AUS"; bei den anderen Outlook-Versionen meist mit „Ansicht" -> „Vorschaufenster")

Die meisten Angriffe richten sich neben Outlook auch gegen den Internet Explorer, da dieser Browser auf 80-90% aller rechner weltweit benutzt wird. Angriffe wie Web-Hijacking, Betrug beim Online-banking (Diebstahl von PIN und TAN) usw. sind keine Seltenheit mehr.

Einzige Empfehlung hier: benutzt den kostenlosen Browser Opera (http://www.opera.com/download).

9. Filesharing Datentausch per eMule, kazaa und co. bedeutet Risiko. Die Firewall muß das jeweilige Programm inklusive aller Zugriffe passieren lassen und Eure IP wird für andere sichtbar. Dagegen kann man nichts tun, also lautet hier die Devise „leech at own risk".
Gegen eventuell gesaugte Viren, Würmer u.ä. hilft ein Antivirenprogramm.

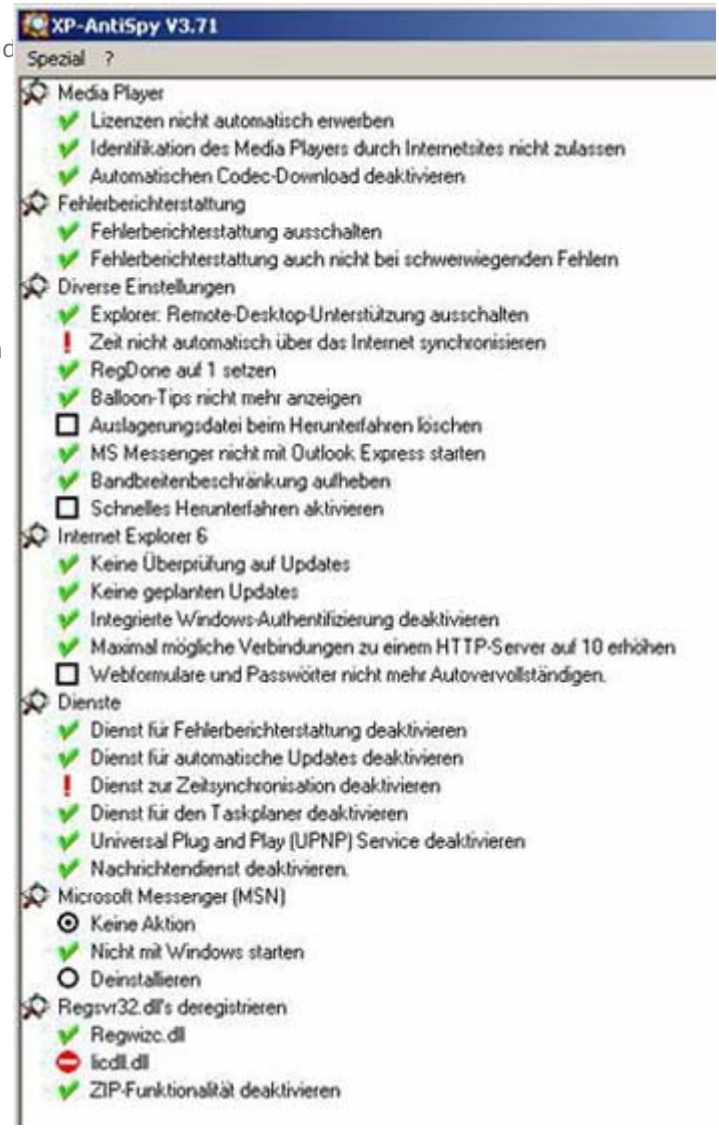
10. Chat Das wohl beliebteste Chat-Programm überhaupt ist ICQ. Um auch hier eine Sicherheitslücke zu schließen, solltet ihr:

a) im Hauptmenü unter „Allgemein" („General") den Punkt "Aufnahme in die Kontaktliste anderer Benutzer nur mit meiner Erlaubnis" („my authorization is required before users add me to their contact list") aktivieren.

b) alle Unbekannten aussperren. Entweder durch sofortige Aufnahme auf die Ignore-Liste nachdem Euch so ein potentieller Hacker angesprochen hat oder gleich alle Fremden ganz aussperren. Geht dazu im „Hauptmenü" auf „Einstellungen und Sicherheit" („Preferences and Security") -> „Spam-Filter („Spam Control") und setzt alle Häkchen bei den Optionen (siehe Bild). Somit sind alle Hacker ausgesperrt.

Abschließend noch ein paar allgemeine Tipps

Benutzt XpantiSpy (Download unter http://www.chip.de/downloads/c_downloa



Hierbei handelt es sich um ein kleines, kostenloses Programm, das sich als sehr nützlich erwiesen hat. So kann antiSPY nicht nur die Bandbreitenbeschränkung aufheben (statt 2 gleichzeitigen Downloads sind dann 10 möglich) oder das Senden von Fehlerberichten an Microsoft unterbinden. Es hat weit mehr nützliche Funktionen wie z.B. Deaktivieren von automatischen Updates, Deaktivieren von automatischen Codec-Downloads uvm.

Im folgenden seht Ihr die wichtigsten Ports, über die ein Angriff stattfinden kann. Vielen von diesen Ports sind sehr wichtig und werden von eigentlich allen Programmen benutzt. Trotzdem sollte man zusehen, dass man diese in der Firewall blockiert und nur bestimmten Programmen erlaubt, darauf zuzugreifen:

- 21 FTP-Server
- 22 SSH-Server
- 25 SMTP
- 80 HTTP
- 110 POP3
- 135, 137, 138, 139, 445 Windows Remote-Dienste wie NetBIOS oder RPC

- 1214 Kazaa Lite
- 1755 Windows Media Player
- 1863 MSN Messenger
- 4661, 4662, 4665, 4672 eMule
- 5050 Yahoo-Messenger
- 5190 ICQ, AIM
- 6881 bis 6889 BitTorrent

Benutzt Tools wie Ad-Aware (http://download.com.com/3000-2094-10214379.html oder SpyBot – Search and Destroy (http://download.com.com/3000-2144-10194058.html?tag=lst-0-1) um Euren Rechner nach Ungeziefer wie Trojaner, Würmer, Backdoor-Programme, Web-Dialer etc. abzusuchen und ihn davon zu befreien.

• Nutzt Ihr W-LAN? Dann verschlüsselt es mit mindestens 128 bit!

• Nutzt Spam- und Virenschutz Eures eMail-Providers (z.B. GMX)

Zurück zur Startseite