Ist SP2 sicher?

Modem-Benutzer mit eigenem Netzwerk sollten sich vorsehen: Unter Umständen sind ihre Daten weltweit einsehbar. Mit einem kleinen Trick sind Sie wieder auf der sicheren Seite.

von Gaby Salvisberg

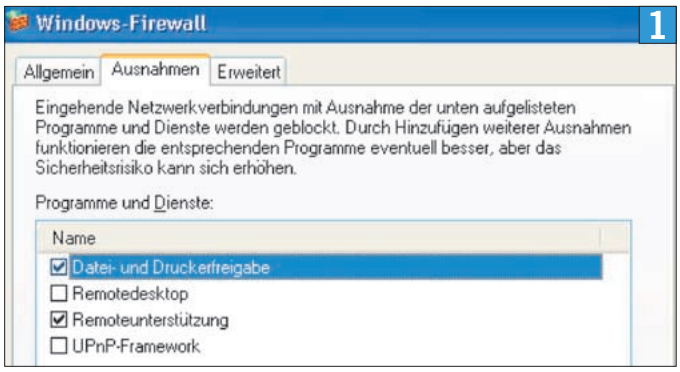
Unsere Schwesterzeitschrift PC-Welt hat im September eine gravierende Sicherheitslücke im Service Pack 2 (SP2) für Windows XP entdeckt: Wer das SP2 über ein bestehendes Windows XP mit SP1 installiert, erlaubt unter gewissen Umständen jedem Internetbenutzer direkten Zugriff auf die Festplatte – und dies trotz aktivierter XP-Firewall!

Betroffen sind Benutzer, die sich unter Windows XP SP2 mit einem herkömmlichen Modem per DFÜ-Adapter ins Internet einwählen, sofern der PC in einem lokalen Netzwerk Daten freigegeben hat und sofern die Internetverbindungsfreigabe abgeschaltet ist. In diesem Fall sind nach einer Installation von SP2 über ein bestehendes SP1 alle Dienste sowie Datei- und Druckerfreigaben weltweit sichtbar. Internetverbindungen, die mit Geräten hergestellt werden, in denen NAT (Network Address Translation) aktiviert ist, sind hingegen nicht betroffen, z. B. jene mit ADSL-Router.

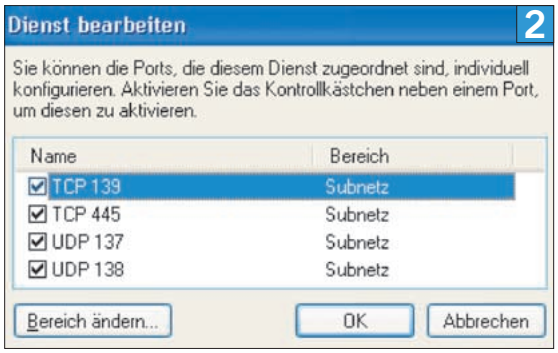
Schuld daran ist ein Bug: Normalerweise wird die DFÜ-Verbindung mit aktivierter Windows-Firewall betrieben, während man im lokalen Netzwerk eher darauf verzichtet, da man sich gegenseitig Zugriff auf Daten geben möchte. Der Bug bewirkt, dass bei der Installation des neuen Service Packs falsche Einstellungen übernommen werden: War die Firewall nur für den DFÜ-Adapter (herkömmliches Modem) aktiv, ist sie es nach der SP2-Installation für *alle* Netzwerkadapter. Gleichzeitig wird aber ebenfalls für *alle* Netzwerkadapter eine Ausnahme für die «Datei- und Druckerfreigabe» festgelegt.

So stehen Ihre Dateien bei der nächsten DFÜ-Einwahl im ganzen Internet zur Verfügung.

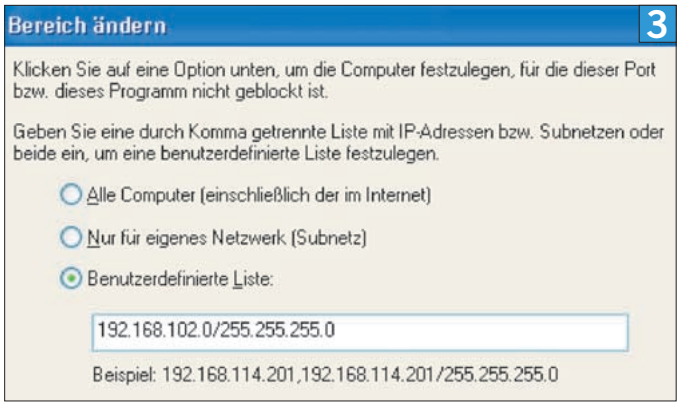
Lösung des Problems: Öffnen Sie via START die SYSTEMSTEUERUNG, klicken Sie allenfalls auf ZUR KLASSISCHEN ANSICHT WECHSELN und anschliessend auf WINDOWS-FIREWALL. Klicken Sie hier auf das Register AUSNAHMEN, Screen 1. Wenn Sie sowieso nicht vorhaben, Daten freizugeben, entfernen Sie alle vorhandenen Häkchen.



Diese Dienste werden dank der AUSNAHMEN nicht durch die Firewall geschützt



Dies sind die Ports, für welche die Ausnahmen gelten



Tragen Sie den IP-Bereich Ihres Netzwerks ein

Komplizierter wirds, wenn Sie die internen Freigaben behalten, aber jene via DFÜ-Netzwerk unterbinden wollen. Klicken Sie in diesem Fall DATEI- UND DRUCKERFREIGABE an und gehen Sie zur Schaltfläche BEARBEITEN. Nun sehen Sie die vier Ports (Software-Anschlüsse), die von diesem Freigabedienst verwendet werden, Screen 2.

Für jeden dieser Ports muss jetzt festgelegt werden, dass er nur im internen Netz sichtbar sein soll. Machen Sie zuerst den IP-Bereich Ihres Netzwerks ausfindig. Das ist normalerweise 192.168.x.0, wobei für das «x» eine Zahl zwischen 0 und 255 stehen kann, also z. B. 192.168.102.0. Zusätzlich brauchen Sie die so genannte Subnetzmaske, die normalerweise 255.255.255.0 heisst.

Welche Bereiche und Nummern Sie verwenden, erfahren Sie, indem Sie zu START/AUSFÜHREN gehen (oder *Ctrl+R* drücken) und durch Eintippen von CMD ein DOS-Fenster öffnen. Tippen Sie nun im DOS-Fenster *ipconfig /all* ein und schliessen Sie die Eingabe mit *Enter* ab. Sie benötigen die Infos, die Sie hinter «IP-Adresse» und «Subnetzmaske» sehen. Ist Ihre IP z. B. 192.168.102.y (y kann eine Zahl zwischen 1 und 255 sein) mit der Subnetzmaske 255.255.255.0, dann notieren Sie 192.168.102.y/255.255.255.0. Falls die PCs in den TCP/IP-Einstellungen *fixe* IP-Adressen haben, tippen Sie genau jene Adressen ein, die auf Ihre Freigaben zugreifen dürfen.

Klicken Sie den obersten Port in Screen 2 an und gehen zu BEREICH ÄNDERN. Aktivieren Sie im nächsten Fenster die Option «Benutzerdefinierte Liste». Dort tragen Sie den ausfindig gemachten IP-Bereich zusammen mit der Subnetzmaske ein, Screen 3.

Ist der Eintrag für den obersten Port erledigt, markieren Sie am besten das Eingetippte und kopieren es mit *Ctrl+C*. Passen Sie jetzt nur noch die anderen drei Ports via BEREICH ÄNDERN an, indem Sie auch dort die «Benutzerdefinierte Liste» wählen und die zuvor kopierten IP-Adressen per *Ctrl+V* ins entsprechende Feld einfügen. ■

MINITIPP NETZWERKE

Windows XP ist flexibel

Notebook-Besitzer kennen das: Im Büronetzwerk werden IP-Adressen per DHCP vergeben, während man zuhause eine feste IP-Adresse verwendet. Deshalb müssen Sie häufig Einstellungen verändern. Das ist unter Windows XP aber nicht nötig! Gehen Sie in der SYSTEMSTEUERUNG zu NETZWERKVERBINDUNGEN und lassen Sie sich per Rechtsklick auf Ihre Verbindung deren EIGENSCHAFTEN anzeigen. Aktivieren Sie «IP-Adresse automatisch beziehen», dann erscheint ein neues Register ALTERNATIVE KONFIGURATION. Darin wiederum geben Sie «Benutzerdefiniert» jene Einstellungen ein, die Ihr Notebook verwenden soll, wenn es beim Aufstarten keine IP-Adresse zugewiesen bekommt. *(sal)*