

Re: warum PnP Dienst über Netzwerk?

Re: warum PnP Dienst über Netzwerk?

Source:

<http://www.tech-archive.net/Archive/German/Win2000/microsoft.public.de.german.win2000.networking/2005-08/ms>

- *From:* "Daniel Melanchthon [MSFT]" <danielme@xxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Fri, 19 Aug 2005 22:08:12 +0200
-

Frank Lindner schrieb:

> Ich habe noch keinen Dienstleister gefunden, der ein sicheres LAN durch
> Betreuung von Win-Clients garantieren kann. Nur viel Gequacke und bei
> nachfragen nach Haftung im Schadenfall betretenes Schweigen.

Vielleicht liegt das auch daran, dass es keine 100%ige Sicherheit gibt?

Ein Samba-Server als FileServer interessiert ein Angriff auf TCP 445 und
TCP 139 nicht.

Auch Samba schützt nicht gegen Softwarefehler. Ein kurzer Blick auf
Secunia fürdert sieben Schwachstellen zu Tage:

<http://secunia.com/advisories/13453/>
<http://secunia.com/advisories/13189/>
<http://secunia.com/advisories/13139/>
<http://secunia.com/advisories/12696/>
<http://secunia.com/advisories/12516/>
<http://secunia.com/advisories/12130/>
<http://secunia.com/advisories/10842/>

Klar, die sind gefixed. Nur heißt das gerade, dass auch Samba kein 100%
sicheres LAN ermöglicht. Von dem Linux untendrunter ganz zu schweigen.

Windows Terminal-Server, z.B. in ein eigenes Netz und ein OpenVPN Server
als Bridge oder Router dazwischen sichert sensible Bereiche optimal ab.
Einzig 3389 für rdp Zugriff wird noch geroutet, der Rest bleibt draußen.

Wie war das noch gleich mit den letzten Patches für OpenVPN und den RDP-Port?

Re: warum PnP Dienst über Netzwerk?

OpenVPN Multiple DoS Vulnerabilities
<http://secunia.com/advisories/16463/>

Windows Remote Desktop Protocol Denial of Service Vulnerability
<http://secunia.com/advisories/16071/>

Somit hast Du damit auch schon Schwachstellen im Komnzept, die 100%ige Sicherheit ausschliesen.

Das ist deutlich effizienter als die MS-Beschreibungen über das fummeln an registry Einträgen zu lesen, wo dann steht, dass MS auch nicht weiß was in produktiven Umgebungen passiert.

Der Disclaimer beim Registry-Editieren steht in jedem Artikel. Man sollte wissen, was man da tut und das ganze sorgfältig machen. Mehr hat das nicht zu bedeuten und das Ändern eines Registry-Keys **ist** deutlich effizienter als ein kompletter Netz-Nneuaufbau mit den von Dir genannten Komponenten.

> Es gibt auch Server, die nicht auf SP1 gepatched werden können, weil da
> Software drauf läuft wo der Hersteller 8 Monate für eine Freigabe läuft.

While not the current target of these attacks, it s important to note that on Windows XP Service Pack 2 and Windows Server 2003 an attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely by anonymous users or by users who have standard user accounts on Windows XP Service Pack 2 or Windows Server 2003. This is because of enhanced security built directly into the affected component. Even if an administrator has enabled anonymous connections by changing the default setting of the RestrictAnonymous registry key, Windows XP Service Pack 2 and Windows Server 2003 are not vulnerable remotely by anonymous users or by users who have standard user accounts.

Quelle: <http://www.microsoft.com/technet/security/advisory/899588.mspx>

Nix für ungut aber manchmal sollte man die Kirche im Dorf lassen.

--

Re: warum PnP Dienst über Netzwerk?

Re: warum PnP Dienst über Netzwerk?

..:Daniel Melanchthon:.

Technologieberater - Exchange Server

<http://blogs.technet.com/dmelanchthon>

This posting is provided "AS IS" with no warranties, and confers no rights.

.