

Re: xp sp2 an 2003er domäne

Source:

<http://www.tech-archive.net/Archive/German/Server/microsoft.public.de.german.windows.server.networking/2004-09>

From: Mark Heitbrink [MVP] (*spam-only_at_gruppenrichtlinien.de*)

Date: 09/23/04

Date: Thu, 23 Sep 2004 17:02:39 +0200

dom schrieb:

> *warum findest du das fahrlässig?*

Was passiert bei einem erfolgreichem Angriff, zB durch ein bekanntes Sicherheitsloch, daß ungepatcht vor sich rundümpelte?

Richtig. Dein komplettes System liegt offen!

Der Angreifer ist nicht nur eingedrungen, sondern er steht mitten im Raum und hat keine Sicherheitsbarrieren mehr die ihn aufhalten.

Wenn die Firewall auf einem anderen System geknackt werden sollte, dann müssen die bösen Jungs von da aus erst mal weiterkommen.

> *Einen Kabelrouter zu besorgen wäre nicht das problem.*

Der wäre zB genaugenommen "zu blöde" um angegriffen zu werden. Dort findet der Angreifer keine Plattform auf der er weitere Angriffstools hinterlegen kann, oder Hintertüren einrichten kann.

> *ABer das ist ei UNI-Netz und ich habe keinen Einfluss drauf.*

> *Ich muss den an ne Dose hängen, oder?*

Im LAN ohne eigenen DSL Anschluss? Dann natürlich ja.

Der DSL Router war auch nur ein Beispiel.

Wenn dir eine ÖIP zur Verfügung steht, dann steht da meistens ein vollwertiger Router von deinem ISP.

> *Also du schlägst vor dass ich da ne Firewall vor klemm.*

Si Hombre.

> *dennoch: wie konfigurier ich die dann?*

Wenn es dir nur um den Zugriff von Mitarbeitern von zuhause geht, dann nur via VPN zulassen, sonst werden keinerlei Dienste publiziert.

> *ich seh da keinen Unterschied. Ausser dass ich keine WinFW
> verwende...*

Du verwendet nicht ein und dasselbe System für alle Dienste, sondern trennst nach Aufgaben und sicherst dich nach vorne mit einer zusätzlichen Hürde gegen einen potentiellen Angreifer ab.

Man kann jetzt philosophieren, aber eine Firewall ist normalerweise keine Software oder Hardware im Speziellen, sondern ein Konzept.

Ein Rechner mit ext./int. Schnittstelle so minimal wie nötig ausgestattet von der Softwareseite bietet immer noch die geringste Angriffsfläche. Dort kann sauber gefiltert werden.

> *Im Endeffekt müsste ich die FW aber genauso aufmachen
> wie die am Server. oder?*

Die Frage ist ja: Was soll von aussen erreichbar sein?
Wenn du externe Mitarbeiter hast, die auf Dateiebene oder andere Bereiche zugreifen müssen dann muss nichts nach "draussen" zugelassen werden, bzw. dann heisst die Lösung VPN.

Intern, also alle Rechner die dann in deinem lokalen Netz stehen können frei mit dem Server kommunizieren. Das ist ja normalerweise auch der Sinn, man muss ja arbeiten können, aber von "ausen" soll keiner dein Netzwerk und die darin verfügbaren Dienste "sehen".

Deswegen: Anmeldung eines externen Clients via VPN, alle Dienste werden dann darin getunnelt und sind verschlüsselt und sicher.

> *Ich finds toll dass du dir gedanken macht. wirklich. Aber
> eine Lösung für das Problem hätte ich doch gerne. 'tschuldigung :)
> Also: XP Client kommt nicht in die Domäne. was tun?*

Firewall für externe Schnittstelle. Intern keine Einschränkung.
Was mindestens also 2 NICs erfordert und wie schon mehrmals angedeutet: ein weiterer Rechner mit 2 NICs wäre besser ;-)

Wo steht denn überhaupt der Client der nicht in die Dömäne kann?

Tschö
Mark

--

Mark Heitbrink - MVP Windows Server

microsoft.public.de.german.windows.server.networking: Re: xp sp2 an 2003er domäne

Homepage: www.gruppenrichtlinien.de

W2K FAQ : <http://w2k-faq.ebend.de>

PM: Vorname@Homepage, Versende-Adresse wird nicht abgerufen.