

Re: 2003 Web Server – Sicherheitsbedenken

Source:

<http://www.tech-archive.net/Archive/German/Server/microsoft.public.de.german.windows.server.setup/2004-03/0058>

From: Konrad Neitzel (*neitzel_at_softmediatec.de*)

Date: 03/13/04

Date: Sat, 13 Mar 2004 19:38:45 +0100

Hallo Michael!

Michael H. Fischer [MVP] wrote:

>>Egal was du machst, wenn du einen windows Webservice direkt ins
>>Netz stellst, kannst du damit rechnen, dass irgend ein Hacker den
>>aufmacht.

> *Mit Verlaub: Blödsinn.*

Nee ... da würde ich dem Vorredner durchaus Recht geben. Ich würde das "windows" aber etwas weniger betonen. Ich habe in dem Bereich leider auch schon meine Erfahrungen machen dürfen ... Und nur weil ich einmal ganz stolz auf einen FreeBSD Rechner war, den ich gut gepflegt habe und so, habe ich mich sicher gefühlt ... Damals ein Freund eines Freundes mich eines besseren belehrt ...

Nur eben stellt sich die Frage, was man denn für Gefahren hat! Und dann stellt sich heraus, dass die Hauptgefahr nicht irgendwelche Top Hacker sind, die es tatsächlich gibt, sondern einfache 08/15 Attacken.

Einfache Frage:

Warum soll ein Hacker gross versuchen, meinen kleinen Popel-server zu hacken? Er startet eines seiner 08/15 Tools und hat Zugriff auf hunderte Server, die schlechter (sprich: Gar nicht!) abgesichert waren. Er hat doch gar kein Interesse, sich irgend einen Server genauer anzusehen!

>>Ohne eine Firewall kann man das nicht verantworten. Nur die Ports
>>aufmachen, die man braucht, reicht nicht für eine Security aber
>>für den Hacker.

> *Teilweise korrekt. Natürlich sollte man auch die Anwendungen, die an
> diesen Ports lauschen, korrekt konfigurieren und patchen.*

Ja genau. Für einen einfachen Server ohne wichtige Daten würde ich sagen:
– Nimm ein Angebot, bei dem der Rechner vom Hoster kostenlos neu aufgebaut wird. Dann sicherst Du regelmässig Einstellungen und Daten und

zur Not baust Du den Rechner halt oft genug auf. Scheiss drauf :)
Es mag durchaus sein, dass Du auch mal von irgendwelchen Viren oder so befallen wirst ... Das erkennst Du dann hoffentlich und gut ist es!
– Patch Management! Wenn Microsoft Patche heraus gibt, die für die Sicherheit wichtig sind: Installier diese so schnell wie möglich!
– Beschäftige Dich mit den Einstellungen, die möglich sind. Und lass weg, wo Du nicht weisst, ob Du es brauchst. Jede Applikation, die Du installierst, könnte die Lücke beinhalten, die ein böder Bube benötigt.
– Lass einen Virenschanner regelmässig laufen. Mich hat so ein Teil durchaus schon ein paar Mal "gerettet". Und evtl. reicht es Dir ja auch schon, wenn Du einen Befall erkennst und dann den Server neu aufbauen lässt ...

Windows ist in meinen Augen sicherheitstechnisch nicht unbedingt schlechter als Linux. Nur eben kommen bei Windows einige blöde Dinge hinzu:
– Größere Verbreitung: Daher kommen Attacken viel öfters vor.
– Man "vertut" sich sehr leicht bei der Administration. (Ich habe zwar keine Ahnung, aber den IIS habe ich mit dem kleinen Haken installiert bekommen ... dann noch hier und da ein kleiner Klick und man ist offen für die Welt :) Wenn man sich klug macht vor einem Einsatz im Netz, dann ist man eigentlich auf einer sicheren Seite. (Der Vorteil bei Linux. Einige Anwendungen kriegt man erst zum laufen, wenn man eine Stunde Doku gelesen hat *g*)

> *Was soll das für eine sein und wie schützt sie dich "besser"?*
Naja ... eine "richtige" Firewall ist schon etwas feines. Dann sind viele Dinge gar nicht erst möglich. Für einen einzelnen Server halte ich es für overhead.
(Aber evtl. liege ich auch total falsch! Ich habe den Eindruck, dass der Thread von jemanden gestartet wurde, der sich jetzt irgendwo einen kleinen root-Server mit W2K3-Web Edition besorgt hat!)

Eine richtige Firewall ist etwas feines – und richtig heisst, dass ich diese "Personal Firewalls" für nicht ganz so toll halte ...

Wenn der IIS nur darauf wartet, dass da ein böser Wurm seine 08/15 Anfrage startet (und damit sofort sein Ziel gefunden hat!), dann nützt diese halt nichts, denn den IIS wird die Firewall bei einem Webserver ja nicht blocken :)

Meine Kernaussagen in der Mitte des Artikels sind hoffentlich klar geworden. Je mehr Ahnung man selbst hat, desto besser kann man seinen Rechner konfigurieren ...

Mit den besten Grüßen,

Konrad Neitzel