

some thoughts on the Slammer fiasco

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2003-01/4704.html>

From: rip (riplips@yahoo.com)

Date: 01/26/03

From: "rip" <riplips@yahoo.com>
Date: Sun, 26 Jan 2003 10:44:13 -0800

None of my production servers were affected by this worm. Why? Because we don't run "bet your business", large revenue generating systems on windoz. We use VMS!!! After over 10 years and billions of dollars in revenue generation, we have never experienced ANY downtime due to viruses (or even loss of data due to StorageWorks).

So why is this? The same dude (Cutler) who architected VMS was also the Architect for NT (now windoz 2000). It is absolutely impossible for an external IP connection to "Take over" a process on VMS because at it's core has a priviledged based process creation/image activation architecture. Windoz has absolutely no concept of this idea and thus will ALWAYS be vulnerable to viruses. The only workaround is to block ports and have MS "hack" their own software. Pretty poor!!!

So where was MS appology for this mess? Are they monitarily responsible? Will there be cival suits? When are they going to completely "create" a brand new OS thats secure? I use the word create loosely since MS has NEVER created their own OS; they bought everyone including windoz.

Lastly, your premise of "loosers" is stupid. The entire internet was brought down by a poorly written application. Imagine that, application data traffic swamping the internet. So, the entire internets availability is the responsibility of clones to patch the MS products? No, lesson learned. Firewalls are worthless and routers (Cisco with million line access lists) were not designed to handle this. Is it the responsibility of a router to manage application traffic? i think what we need is a whole new level of technology to manage and secure application data traffic. Don't expect it from MS or Cisco; they'll just point fingers at each other.

Lesson learned: Don't use MS to run your critical apps on and get them OFF the internet. Amazing that Bank of America's ATM network got infected from the internet. Why does that ATM network have any connections to the internet. Eventually the "internet" will be like a low cost mass transit system like a bus or subway and those who want highly available/secure networks will buy their own private jets for transportation (completely isolated, autonomous networks. Forget VPN).

rip

>-----Original Message-----

>

>These are my thoughts regarding some of the moronic posts seen here

>recently.

>

>WTF are you running a software firewall on an SQL box for. SQL should stand

>alone. And please buy a hardware firewall.

>

>Here is a question someone running Oracle would not ask.

"Can (software

>firewall of your choice) block port X.

>

>I am an SQL Server DBA and quite frankly ashamed of the low level of

>knowledge and lack of willingness to keep up with simple security updates on

>the part of the losers here whining about how to keep their servers safe.

>Either learn how to play, or get of the field. And people wonder why SQL

>Server DBAs make less than a DBA for Oracle, DB2, Sybase, etc.

>

>"But is was sooo easy to install, I clicked next. I'm safe now, right?"

>Personally, I hope the IT slump goes on for 5 more years to weed out

>wannabes like the people here.

>

>Sid

>

>

>.

>