

SecurityFocus Microsoft: RE: Should web servers, eg. IIS 6 have anti--virus installed on them?

RE: Should web servers, eg. IIS 6 have anti--virus installed on them?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2005-07/0071.html>

From: Steve Bostedor (Steveb_at_tshore.com)

Date: 07/20/05

Date: Wed, 20 Jul 2005 15:01:50 -0400

To: "Harlan Carvey" <keydet89@yahoo.com>, <focus-ms@securityfocus.com>

That's all hind sight, Harlan. Getting people to protect their servers with basic tools like antivirus is far more feasible than trying to turn everyone into exploit clairvoyants!

It is a very simple and indisputable fact that antivirus played a major part in saving many very important companies a very large sum of money. Ignoring that is not advisable.

It's irresponsible to expose a server to the Internet without antivirus protection on it no matter what its role is.

It seems to me that there is an air of arrogance in the thought process that says "I was able to beat it last time, so I have no worries about the future". Many of the companies that lost millions thought that they had all of the bases covered. Contrary to what you're trying to imply, it was not that they were just lazier than you or less "elite". Not every company can afford a 24/7 security geek standing at their routers checking the exploits at the door! We can all afford basic antiviral protection, though.

You may be patting yourself on the back because it didn't hit you this time but it was pure luck that it was a patch that you were aware of. Letting your guard down is such an amateur and arrogant mistake.

– Steve

<http://www.vncscan.com>

-----Original Message-----

From: Harlan Carvey [<mailto:keydet89@yahoo.com>]

Sent: Wednesday, July 20, 2005 2:49 PM

To: focus-ms@securityfocus.com

Cc: Steve Bostedor; Susan Bradley, CPA aka Ebitz – SBS Rocks [MVP]; jeff@shawgo.com

Subject: RE: Should web servers, eg. IIS 6 have anti--virus installed on them?

RE: Should web servers, eg. IIS 6 have anti--virus installed on them?

SecurityFocus Microsoft: RE: Should web servers, eg. IIS 6 have anti--virus installed on them?

- > *I wouldn't dream of leaving one of our web servers*
- > *without antivirus*
- > *software on it for a second! Everyone take a second*
- > *and remember back*
- > *to the Code Red and the various SQL worms. All that*
- > *it took was a*
- > *buffer overflow and a virus was on your system*
- > *before you could blink.*

Yes, and all that it took to protect against Code Red was to have disabled the .idq/.ida script mapping. SQL Spida infected systems with blank 'sa' passwords. SQL Slammer targeted UDP port 1434.

In all of these cases, A/V should not have been needed, had proper administration been conducted in the first place.

Again, the security process was broken in each case, and installing A/V was just a band-aid.

- > *We were saved because by the time that it hit our*
- > *servers, Symantec had*
- > *a cure and stopped it.*

Why did these hit your servers in the first place? Why did you have .idq/.ida script mappings enabled? Were they required? Why did you have a blank 'sa' password on your SQL database server? Why were you exposing UDP 1434 to the Internet?

- > *This is just one example of*
- > *what COULD happen to*
- > *you should you neglect to properly secure your web*
- > *servers with at LEAST antivirus protection.*

Had properly and well documented procedures been observed in the first place, A/V would not have been necessary.

Harlan

Harlan Carvey, CISSP
"Windows Forensics and Incident Recovery"
<http://www.windows-ir.com>
<http://windowsir.blogspot.com>

RE: Should web servers, eg. IIS 6 have anti--virus installed on them?