

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/2005-07/0074.html>

From: Harlan Carvey (*keydet89_at_yahoo.com*)

Date: 07/20/05

Date: Wed, 20 Jul 2005 11:48:51 -0700 (PDT)

To: focus-ms@securityfocus.com

- > *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 targetted 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.*

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

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

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>
