

Re: [Full-Disclosure] Antivirus Software Solutions?

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-11/1263.html>

From: Paul Schmehl (pauls_at_utdallas.edu)

Date: 11/28/03

To: full-disclosure@lists.netsys.com

Date: Fri, 28 Nov 2003 08:58:58 -0600

--On Friday, November 28, 2003 12:20 PM +1100 Paul Szabo

<psz@maths.usyd.edu.au> wrote:

>

> *Do not use "traditional" AV at all (as that would never protect you from
> the latest virus). Rather, set up your email gateway to "defang" all
> suspicious emails (e.g. containing EXE or SCR or PIF, or ZIP,
> attachments); it is a matter to debate whether to reject (bounce), drop,
> or somehow encode such things so as to render harmless. - Probably you
> will want your email gateway to run UNIX/Linux, so you can set this up.*

>

This is a good first step, but you should also have a/v protection at the gateway. Look at amavisd and vexira if you're allowed to use open source. If you have to use commercial products, Sophos has a good gateway product. Trend is popular but not as good.

You might also consider some of the newer IPS appliances such as Tippingpoint, Fortigate or ISS's Proventia M. These provide virus protection for all protocol streams, not just email, http and ftp. (We are evaling all three of those.)

> *Once your email gateway is "safe", any AV on desktops becomes much less
> important, but you may still want some "traditional" AV on your desktops;
> any reasonably well supported product should do.*

>

This is horrible advice. You **must** have traditional a/v on your desktops or some equivalent replacement. The desktop is you last line of defense and often the only one that will "catch" things. Gateway a/v scanners such as trend will do **nothing** to protect you against worms such as Blaster and Slammer. There are just too many avenues for attack to leave the desktops unprotected; removeable media (CDs, floppies, DVDs, Zip disks), IRC, ICQ, P2P, IM, web, etc., etc.

Furthermore, you don't want just "any reasonable well supported product". You want a product that is highly effective against none viruses. Some that fall in to that category are Sophos, McAfee, Kaspersky and Norton.

Full-Disclosure: Re: [Full-Disclosure] Antivirus Software Solutions?

Foregoing the use of top notch protection on the desktops is a recipe for disaster.

Paul Schmehl (pauls@utdallas.edu)
Adjunct Information Security Officer
The University of Texas at Dallas
AVIEN Founding Member
<http://www.utdallas.edu>

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>