

Firewall-Wizards: Re: [fw-wiz] Too Paranoid?

Re: [fw-wiz] Too Paranoid?

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2002-10/0704.html>

From: Ryan M. Ferris (rferris@rmfdevelopment.com)

Date: 10/02/02

From: "Ryan M. Ferris" <rferris@rmfdevelopment.com>
To: "Kevin Steves" <stevesk@pobox.com>, "Paul D. Robertson" <proberts@patriot.net>
Date: Wed Oct 2 13:26:14 2002

It strikes me as somewhat depressing that there isn't a ('vendor independent') single resource dedicated to describing how to secure the important commercial software that routinely appeal to IT staffs to "punch a hole in the firewall". This type of issue came up repeatedly with many financial institutions that I have consulted. Remarkably (admittedly in times less dominated by security concerns) the IT unit usually caved into the business unit demands.

Having been on the other side (development), I see what the attitude was (is). Management, development, test are so frenzied chasing the critical bugs out of poorly managed and rushed development projects that the attitude is "I think client security is the responsibility of our clients." (actual lead developer quote!). In test, you are lucky if someone allows you to work on a security test plan for the product, much less actually let you take the time to run the test suite.

If organizations of the type like Real Networks, ADP, Microsoft were smarter, perhaps they could have their cake and eat it too: Form a 'vendor independent' association that tests and publishes recommended security and securing guidelines for their software and software configuration. What security you might lose in published guidelines, you would win back in widespread adoption of guidelines because these vendors would have some obligation to put the association guidelines into their test suites. The vendors themselves would only be under an "umbrella" organization type influence to secure their product. They wouldn't have to guarantee their product's security, just point the client to the association website for advice.

One would guess Sales Departments would have a big interest in such an association and such guidelines.

Ryan M. Ferris

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

From: "Kevin Steves" <stevesk@pobox.com>
To: "Paul D. Robertson" <proberts@patriot.net>

Re: [fw-wiz] Too Paranoid?

Firewall-Wizards: Re: [fw-wiz] Too Paranoid?

Cc: <firewall-wizards@honor.icsalabs.com>; <stevesk@pobox.com>

Sent: Tuesday, October 01, 2002 8:35 PM

Subject: Re: [fw-wiz] Too Paranoid?

> *On Sun, Sep 29, 2002 at 12:25:27PM -0400, Paul D. Robertson wrote:*
> > *I've had this fight with personnel/benefits systems before, and once we*
> > *got to the "it needs these two TCP ports" place, isolating it wasn't all*
> > *that difficult.*
>
> *It tends to boild down to: we have a strong business need for this*
> *application, we need to figure out how best to configure and secure it*
> *in our environment--at least at the financial type places I've worked*
> *at.*
>
> *Wide port ranges, UDP use, IP multicast, HA, dynamic routing, strange*
> *DNS usage--consider it a challenge for the design skills. I've*
> *generally found the vendors willing to work with you to come up with a*
> *configuration that can be acceptable, but it can be a challenge.*
>
> _____
> *firewall-wizards mailing list*
> firewall-wizards@honor.icsalabs.com
> <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>
>