IT Business™

Our Mission

The mission of *IT Business* is to provide a platform for discussion and analysis of the successful use of IT to enhance business processes.

IT Business Brief

Diversity - A Best Practice for Security

by Gary C. Kessler

Ashton, Metzler & Associates

Leverage Technology & Talent for Success

Security

March 6, 2003

A note from the founders

Fifteen years ago, when T1-based networks were first being introduced into the enterprise, concerns were sometime expressed about having "too many eggs in one basket." This same concern is now raised about Voice over IP (VoIP) implementations. But, interestingly, this concern is seldom if ever raised concerning security issues, where, as it turns out, this is a much more legitimate issue.

From a security perspective, the trend to go with the most popular operating systems and applications has a distinctly negative side. Namely, if hackers are going to attack a vulnerability, they will go for the vulnerability that has the most potential impact. For a browser-based vulnerability, the hacker can have orders of magnitude more impact by exploiting a vulnerability in Microsoft Internet Explorer than by attacking users of Opera.

In this IT Business Brief our colleague Gary Kessler, a well-known analyst and associate professor at Champlain College, advises enterprises that consistency may not be good from a security perspective, and that variety is not only the spice of life - but also the singular factor that may save your network.

- Steven Taylor, Distributed Networking Associates / Webtorials.Com

Jim Metzler
jim@itbusinessmedia.com

Steven Taylor
steve@itbusinessmedia.com

IT Business Brief

Published by
IT Business Media.
www.ITBusinessMedia.Com

Cofounders
Jim Metzler
jim@itbusinessmedia.com

Steven Taylor
steve@itbusinessmedia.com

Design/Layout Artist
Debi Vozikis

Contact Jim Metzler
or Steven Taylor for
advertising information

Diversity - A Best Practice for Security

- Gary C. Kessler

Why do we use software that we know to be insecure, winking all the while as if sharing a secret joke?

After all, there are a slew of applications that, though widely used, have long lists of documented security vulnerabilities. Many programs default to non-secure settings, for example, and it can be difficult to configure the settings properly. Still, even with the security features appropriately enabled, users often don't use applications in a secure fashion, anyway.

Some of the most vulnerable applications are, unfortunately, among the most commonly deployed: Outlook. Internet Explorer. Internet Information Services (IIS). SQL Server. Instant messaging.

When I question my IT manager and CIO colleagues about why we use software that we know to be risky, their answers vary from "increased productivity" and "it comes with the operating system" to "users like it" and "the consultant recommended it."

Hmmm…perhaps we should be choosier about the applications that touch our networks. By simply deploying applications by default—as dictated by dominant software vendors, users, and consultants—we are, to some degree, shirking our responsibility to protect our organization's information resources. Yes, we do shoulder the blame and the task of cleaning up in the aftermath of a breach, virus, or other attack. But part of our job is to thwart those attacks, to the degree possible, in the first place.

Choosing More Resilient Apps

I know several people who use multiple anti-virus programs ostensibly so that they stand a better chance of detecting a new virus before it causes damage. I recommend, however, expanding this approach to include multiple defensive strategies.

Let me provide an example from my own anti-virus practices. First, there's the choice of an e-mail client. Outlook is a very popular tool for propagating viruses, largely because it defaults to *auto-execute* certain programs, defaults to preview e-mail, and uses the Microsoft Messaging Application Program Interface (MAPI). Although the program is available essentially free of charge, it is certainly not the only such option.

For example, I use Qualcomm Eudora. I like it because the Eudora e-mail client does not default to those functions responsible for spreading the majority of viruses and worms.

Second, I use Norton AntiVirus (NAV) and keep it on *auto-protect* mode using the program's Automatic LiveUpdate feature. There are other fine anti-virus packages, as well. The point is that an anti-virus program that is continually at work in the background to detect viruses—and one that is updated rapidly as new viruses are found—is an invaluable tool.

Those who believe that two anti-virus packages are better than one usually assume that at least one of them will detect a virus that the other might miss. I don't have confidence in this assumption. So the third component of my anti-virus strategy is to apply Internet Security Systems' BlackICE PC Protection.

BlackICE not only provides rudimentary firewall and intrusion detection, but it confirms every new application before it runs on a PC. It also confirms every application's access to the network. If a virus does slip through, then, I still have a chance to catch it before it executes and yet another chance before it propagates across the network.

Defense in Depth

What I've been describing is a *defense-in-depth* approach to security. This is hardly a new strategic concept. Just like castles have multiple layers of physical security—high brick walls surrounded by moats surrounded, in turn, by flat, open ground—I recommend multiple layers of protection to thwart viruses. And I recommend coupling this strategy with *biodiversity*.

By bioversity, I mean using a mix of vendors. In farms and forests, many different species thrive alongside each other. A single bug cannot wipe out an entire area. Biodiversity as applied to security means that our network applications, operating systems, and defensive mechanisms-encryption, firewall, intrusion detection, and so forth-should be built by different vendors.

And, of course, I recommend avoiding insecure software, such as those applications noted early in this article.

For example, there are alternatives to the Internet Explorer (IE) browser. Admittedly, it can be difficult to employ these secure alternatives because of the sheer number of Web page designers who use IE-specific code. Still, how can a Web site programmer or owner seriously claim to promote secure networking if it forces users to employ an insecure piece of software?

Similarly, there are vulnerabilities in Microsoft HTML extensions. The company said several years ago that breaking them up would be devastating to information security. Microsoft advocated that a single vendor should build all of your software so that you get a seamless approach to defense.

I think this argument is as specious as it is self-serving. The monolithic approach only requires that a Bad Guy find a single chink in the security armor to do his dirty work, rather than having to penetrate multiple, disparate security mechanisms.

To improve the situation, it's up to consumers to take a stand. If an application is a known security target, then at least consider using other software. Just because an application comes with an operating system doesn't mean you have to use it. You might have to put your money where your mouth is as you select the best application, but it won't cost as much as you think—and certainly not as much as a major security incident.

Though we will never eradicate all security risks, doing a little bit of work can help shift the odds in our favor. Defense in depth and vendor diversity are two avenues.

Gary C. Kessler *is an independent computer and networking security consultant at Gary Kessler Associates (www.garykessler.net/gka.html). He is also associate professor and program director, Computer Networking, at Champlain College in Burlington, Vt. Kessler chairs the Vermont chapter of InfraGard, a cooperative effort between U.S. government, businesses, academia, law enforcement agencies, and other organizations to increase the security of the U.S. infrastructure. He can be reached at kumquat@sover.net.*