Herding Cats:
The Invisible Mr. Security Guy

May 2012

BrandenWilliams
SECURE BUSINESS GROWTH

Hey Mr. Security Guy… It’s time.

There are so many ways we can take this column from that intro, but here’s where I want to go today. The topic of the issue is Security Architecture, and it’s looking totally different with every passing day. If you have been in the industry for longer than ten years, think about how you used to focus your activities on one main firewall and a robust anti-virus system to keep things running (aside from the random chaos monkey ripping core infrastructure offline). If you have been around for five years, think about all this compliance stuff we’ve had to deal with, primarily lead by PCI DSS and in some cases the healthcare acts in the US and privacy acts in Europe. If you’ve been in for just a couple of years, think about hacktivism, advanced threats, and the organized cybercrime that dominated 2011.

Security architecture is always in a strange place. Either its always playing catch-up with new and innovative attacks, or its draconian nature undermines its ability to be functional to the business. The former tends to be much more of the norm as companies rely on basic stuff like compliance to allow them to redirect a few dollars toward more advanced things like advanced attacks. Draconian security exists in places like financial services and governments, but isn’t it interesting how some controls force people to think creatively about ways to defeat them? Does “Just email the attachment to my GMail account,” or “rename the .exe to .txt so my company’s filters won’t block it” sound familiar?

Another interesting phenomenon that’s happening is our physical control over resources is increasingly disappearing as we create efficiency in our systems by operating in an abstraction of the physical layer. If we can’t put our finger on the machine that is running some IT application anymore, how do we build architecture to secure it?

One challenge I am pushing people to take on is thinking about how security can be consumed transparently (i.e., built-in) by the end user. That forces the issue of securing information, wherever it may be. We have the technology—and it’s affordable! Ten years ago, very few companies used things like secure enclaves outside of physical processes in a physical world. Finding a company with an additional firewall in between a grouping of servers in 2002 could be the equivalent of seeing a leprechaun riding a unicorn on a rainbow. Today? It’s pretty common.

What about encryption for data at rest? In 2002 it didn’t happen that much either (albeit more than secure enclaves). Computing resources were much more expensive back then when you tried to accomplish things like encryption, but now embedded devices do it just fine[1]. There is almost no reason to trust any computing resource this day and age because we can architect solutions to enable business without blind trust. Ask yourself this: do you trust any network you connect to? Do you click through SSL Certificate warnings? Do you through caution to the wind and avoid SSL all together? Most of you probably don’t, but I guarantee someone close to you does.

It’s time for us to change our ways. We need automation, deep visibility into our systems and activity, the ability to build risk decisions into our infrastructure and to alter our posture in an automated and agile way. And the most important part, we can’t be jerks about it! We have to seamlessly integrate security into our businesses such that they don’t even know we were there. Security must be architected to be consumed transparently.

FOOTNOTES

[1] *When they mind their* ps *and* qs *that is…*

There’s an old business adage that reminds us that consumers want simplicity. They don’t want to jump through hoops to do business with any company. Business people don’t want to jump through hoops every time security shows up. They just want things to work, they want them to work well, and they need to focus on what they do best (which isn’t information security). If you’re banging your head against the desk every time you read something like this, consider that your approach may be all wrong. When’s the last time you sat down with a business leader and just let them talk about their business and what’s important to them? It’s painful at times, but building that rapport is critical to you unlocking the Security Ninja achievement!

Contact information for requests for permission to reproduce or distribute materials available are listed below.

About the Author:

Branden R. Williams, CISSP, CISM, has been making a name for himself in the Information Technology and Security arena since 1994, as a high school Junior. Now, a graduate of the University of Texas, Arlington earning his BBA in 2000 with a concentration in Marketing and the University of Dallas, where he earned an MBA in Supply Chain Management & Market Logistics, in 2004, Williams is sought after as both an Adjunct Professor and Information Technology & Security Strategy Leader in the corporate world.

Williams regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog, buy his book, or reach him directly at http://www.brandenwilliams.com/.