Herding Cats:
Hunt

March 2012

BrandenWilliams
SECURE BUSINESS GROWTH

It is a great time to be a security professional. Take a look at other industries and professions and compare them with infosec. There are very few that are skyrocketing in influence, importance, and criticality like we are.

As I said in February's Herding Cats, the bad guys won last year and 2012 hasn't started off any slower. The targets have shifted from consumers to corporations (for the big hacks anyway), and in some cases those big corporation hacks do affect individual consumers depending on the data taken. Five years ago before the TJX breach, you would have a hard time looking around the room and finding someone who had been a victim of or affected by a data breach. Today nearly everyone has had it happen to them at some point whether you are a frequent traveler or just someone who got lucky with their digital details in the wrong place at the wrong time.

Companies have moved a ton of their information into digital formats, and their workers are increasingly mobile and using strange, non-corporate or non-standard devices to do things with that information. Instead of users being happy with whatever their company gave them, they bring their consumer preferences to the workplace and demand similar features and utility. This creates an offshoot of IT called Consumer-driven IT[1] that not only increases the complexity of IT systems but vastly increases the attack surface available to the bad guy.

Many security professionals remind us that "We have to be right all the time, whereas the bad guys only have to be right once." Technically, this is correct, but it minimizes the efforts by the bad guys. We both put in the effort, but the odds are stacked against us when we look at where IT is going contrasted from where it has been. The bad guys manage their resources much better than the good guys do, and its time we tip the scales in the other direction.

Let's say that I am going after some intellectual property that is in-development, and I want to steal it such that I can play rapid catch-up with my competitor in the market. Physical means of access might still be used, but if I know that this information might live on a system that is not owned by corporate IT, not under direct control of corporate IT, and maintains some level of functionality when not connected to the corporate network, I know that I can focus on the user instead of the system. It's pretty easy to get someone to click a link, visit a webpage, or even open an attachment if you provide the right context around your requests.

To make matters worse, we tend to focus on our own systems but completely ignore systems and people we do business with on a day to day basis. Hiccups in the informational supply chain is just as damaging to a company as those found in the materials supply chain. Because it is easy to get people to click links, your systems are only as secure as your partners. If a partner is infiltrated and bad guys can masquerade as them, imagine how much more believable that email might be to Sally in Accounting or Bob in Marketing!

We can't wait for these attacks to happen, we have to rapidly advance our defenses to be able to detect and repel attacks that come our way. We can't wait for the call that says "You've had a breach." We must hunt for the bad guys before they make themselves widely known. In order to do this, we have to stop thinking of Information Security and the tools included under that domain solely as a support structure for audit functions.

FOOTNOTES

[1] *See what I did there? None of that Consumerization phrase.*

Security systems today tend to be tuned for compliance, not for security[2]; thus the alarms that should be going off when bad things are happening rarely do. I'm not saying we have to throw compliance out the window, I'm saying that information security systems must support compliance—that's table stakes—as well as support the hunt for advanced attacks that your business will face when the bulls-eye lands on you.

FOOTNOTES

[2] *See the latest SBIC report (check your search engine of choice for a link) for details on this.*

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/.

TEL 214 727 8227
FAX 214 432 6174

BLOG brandenwilliams.com

EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH