Herding Cats:
"Get a Pizza" Hacking

July 2012

BrandenWilliams
SECURE BUSINESS GROWTH

I may not be like most people, but when I see a topic like the one covered in this issue I get excited. Yes, it is possible to get excited about standards, compliance, and governance, but only if you have the right mindset! When viewed in the right light, these three terms become framework generators, actors in the larger system, and specialized, reportable cross-sections of your information security program. The challenge comes when you use any of those terms to fully define your security program. Doing so removes effectiveness from your program as it doesn’t take into account the types of threats organizations face today.

RSA sponsors a group called the Security for Business Innovation Council (SBIC) that publishes reports twice per year. The last report details a critical finding for security professionals to understand—our security programs are tuned to support compliance, not information security. This means that for every dollar you spend to keep the auditor away, you are letting your information security program get farther from its true goal—protecting information.

Think about how your information security program works today. Chances are, you (or someone before you) spent countless hours trying to justify every dollar allocated toward information security to the executive committee, and you had to constantly fight for more dollars as your responsibilities grew. That battle is neither easy nor quick. Chances are, it is often a losing battle in your eyes as you are constantly denied funding requests. The carrot method simply either didn’t work, or was just too hard to sustain.

Enter compliance, the savior of information security! Now I don’t have to fight for my dollars, I just have to “prove” that whatever I am asking for is required for compliance. Think back to your career during 2002-2008. I would be willing to bet a twelve-pack of your favorite brew that you used SOX, GLBA, HIPAA, or PCI DSS at least once to get a funding request approved—even if it was a stretch to call it part of a compliance requirement. Otherwise, how could you get management to sign off on web-application firewalls and wireless IPS devices? The stick method worked well to get us to a basic state of information security that could ward off unsophisticated attacks by amateur hackers.

But now that we’ve raised the security bar (which depending on who you talk to is either above many company’s internal capabilities, or its so easy to clear you trip over it), the bad guys have raised their abilities as well. Sure, the basic techniques like port mapping, probing, and even vulnerability scanning are still used, but the attack platforms have gotten tremendously better. If you have not tried it, go download Metasploit and check out its automated abilities. You can literally download it, fire off an automated attack, get a pizza, and be into many companies’ networks by the time you sit back down.

Companies today are facing something they have never had to face before—state sponsored actors that go after their intellectual property. This is the equivalent of defending your networks against an organized army of electronic attackers quite like what you might call cyber-warfare. Let’s not delude ourselves to think that this has never happened before, but it is becoming more prevalent then it has in the last five years. Security programs designed to capture and mine information only for compliance purposes will miss these armies breaking into their systems and will only know something bad happened when they get a call from a third party or see their stuff showing up in Pastebin.

The call to action is for you to rethink how your security program is built and center it around intelligence instead of compliance. Intelligence-led security programs are the future of information security in corporations. You must be able to understand and

incorporate relevant intelligence feeds from outside your organization and correlate those with activities happening inside your networks. The days of waiting on a new compliance requirement to drive your security budget are over. We need to take action in our roles as bad guy hunters. After all, we tend to be the scapegoat when things go bump in the night.

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 speaker 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