Herding Cats:
Don’t get Cyber-Jacked!

June 2008

BrandenWilliams
SECURE BUSINESS GROWTH

If you had a safe filled with cash in a relatively insecure location (say at a retail back office), would you close the door and lock it when you are not using it? Hundreds of retailers would say, “Absolutely. This safe would be closed and locked when not in use.” Why is this same approach not taken with security?

I’ve worked with companies that take extreme measures to protect their perimeter, but leave the internal network flat (i.e., the Armadillo Model: hard crunchy exterior, soft chewy middle). My intent is not to point out the always-feared-but-rarely-seen Insider Threat, but to frame our thinking around the landscape of Cybercrime Combat.

The rise of cybercrime grabs headlines of major publications every day. So far in 2008, PrivacyRights.org is reporting over ten million records affected by breaches[1], and that number has the potential to more than double before the year is over.

Cybercrime can occur anywhere. It could be perpetrated by the often glorified hacker sitting in a dark room on foreign soil, the overly helpful customer service agent that happily resets a password, or a commercial enterprise that profits from targeted organized crime.

Speaking of organized crime, what a booming enterprise! Compliance initiatives like PCI have succeeded in turning the raging river of stolen data into a babbling brook (with the occasional flash flood). Because the easy score is harder to come by, organized crime units have turned to more sophisticated approaches to increase revenue. For example, it is relatively simple for one of these enterprises to get associates hired at a company and ship skimmed data out the door.

This year we’ve seen a highly publicized breach reportedly caused by credit card stealing malware. We’ve progressed from the rudimentary hacking of Point of Sale (POS) systems to SQL Injection attacks to sophisticated attacks involving massive installations of malware.

This ain’t your daddy’s security incident. You know, the ones caused by accidental malcode[2] or by a programmer paying homage to a stripper[3]. Instead, these are highly organized and targeted attacks that have a remarkable success rate.

What are we to do? Surely there are some “basic” controls that we can put in place to prevent these types of attacks. Quite simply, there are. Unfortunately, without a mature security program in place, the effort required to install these controls could quickly grow from “basic” to “insurmountable.”

The first place to start is revamping your patch management and system hardening process. You should manage a limited number of builds that can be updated as needed to create a “Gold Image.” All new server builds come from it, and all production builds should mirror it. You would need some automation to make it scalable, and there are many products available—both free or open source and commercial—that can do this. You also may need to address that legacy software package that can only run on Windows NT. As Administrator. Without Service Pack 6. Because the guys in finance need it.

Companies that have not gone through a standardization of their IT infrastructure may slide to the insurmountable side of the scale. Months (hopefully not years) of remediation

FOOTNOTES

[1] *http://www.privacyrights.org/ar/ChronDataBreaches.htm*

[2] *The Morris Worm*

[3] *The Melissa Virus*

may need to be done first. Your effort will be rewarded as you save time and money by updating a few builds every time a patch comes out—not hundreds.

The other thing we can do is pump the concept of “least privilege” through the veins of our company. Stores and possibly small satellite offices should not have access to the Internet, nor should they be able to access each other. Network segmentation and secure enclaves should be common, not rare. Users should have all of their rights stripped except for the ones required for their job. Those with elevated privileges should have their access re-evaluated periodically, and their actions logged and analyzed.

These “basic” concepts will work in a mature security program, or they can be seen as part of the To-Be picture. Criminals will continue to improvise as you cut off new revenue streams, but keeping up with security trends will keep you a target—not a victim.

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

About the Author:

Branden R. Williams, CISSP, CISM, CPISA/M, 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 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 at or reach him directly at http://www.brandenwilliams.com/.