Herding Cats:
Get Compliant on the Cheap

April 2009

BrandenWilliams
SECURE BUSINESS GROWTH

This issue is like the current security and compliance landscape in that it is PCI heavy. PCI is not new and it certainly does not seem to go away. With every passing year, we think that PCI's drum beat will become more diminuendo and ritardando. But instead, it just seems to get louder and faster. Announcing a breach in the first two months in each of the last three years might have something to do with keeping it top of mind.

Companies tell me the reason they have not made more progress toward sustainable compliance and improved payment system security usually boils down to money. PCI Compliance can be very costly. As a security professional, we must not look down our nose at the business side of a company and tell them that they should have been doing this all along. Quite frankly, it is OUR fault for letting it get this bad. We didn't do enough of the right things to prevent security from falling so far behind. So, it's time for a bailout.

Unlike governments around the world, businesses cannot simply print more money to pay for the products, services, and people they need to get the job done. Investment from the business side of a company is required to move forward, but the amount of the investment can depend on how savvy you are with the tools you have available at your disposal. Let's explore some of the options as it relates to PCI.

Managed Security Services. There, I said it. And not just because I am affiliated with a company that offers them. When budgets get slashed, sometimes the people do too. This means that you have the same amount of work to do (if not more), but fewer resources to push the work forward. Don't be Atlas. Instead, consider outsourcing some of your operational security tasks. Managing and monitoring firewalls, intrusion detection (wired & wireless), and log management consumes precious resources.

Outsourcing can usually save you significant money over the wide variety of full time, specialized employees you may need to perform the tasks, and get you access to a large network of specialized resources that can help you with all kinds of challenges you face. If you are worried about the human element of a layoff, do your local economy a favor and buy local! Don't import these services; instead, choose a company that has a local presence in your country so that the people you lay off can have a shot at selling their skills to an outsourcer.

Open source software is another tool that can help you become compliant or secure if properly used. Here are some examples of open source tools that can be used to meet specific PCI requirements. This list is not exhaustive, so even if these technologies will not work for you, other technologies might.

IDS: Snort, OSSEC
Wireless Detection: NetStumbler, Airsnort, Kismet
Firewall: Linux IP Tables, BSD's ipfw, NetFilter
Point to Point Encryption: stunnel, ssh tunnels
VPN: OpenVPN
File Encryption: TrueCrypt, FileVault (Mac OS X)
Security Testing: Zenmap, Firewalk, Cain & Abel
Wireless Cracking: Aircrack-ng

On top of all of this, there is a myriad of Live ISO security testing suites available for download that will run on your existing machine without a reformat like Backtrack and Knoppix. The tools mentioned above are included with a slew of others that could be used to test security or enable compliance.

Open source does come with drawbacks to corporations. Many of the applications are coded by people who have day jobs. This is a hobby or research project for them, and they will update it when they have time. For that reason, support may be slow. Most popular tools have a large user community, so there may be tons of support out there if you knew where to look.

One thing to do before deploying any open source tools is to check with your legal department on the licensing. Some companies have specific policies on what kinds of software licenses can be used, and which ones cannot. I have had more than one company tell me that they cannot deploy anything licensed under certain versions of the GNU Public License.

Compliance and security can be had on the cheap. You don't have to buy the Bently to get around town when the Civic works just fine!

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/.

TEL 214 727 8227
FAX 214 432 6174

BLOG brandenwilliams.com

EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH