Herding Cats:
Act Like an Army

November 2012

BrandenWilliams
SECURE BUSINESS GROWTH

The information security landscape has never been quite as exciting as it is today. My dad often joked about me when I was a teenager saying that my interest in technology and then information security would keep me employed forever. Indeed, with the rapid rate of business digitization and the inherent information value creation, he might be right. The last twenty years has seen the Internet change from that thing that academics use to exchange information, to the nice-to-have slow e-connection to the outside world whereby you can order pizza and books in your PJs, to the yelling of executives when email is down, to the absolute critical nature it is in today as a central cog in our value chains. Twenty years ago it was rare to see businesses embracing digital technology just like today its rare to see a business NOT using said technology.

With value creation comes opportunity for abuse. Malware is rampant and the kits used to create many variants of it are open source. It's such a big problem that the average effectiveness of anti-virus software is now so low it's hard to see one vendor outperform another—including the free ones. According to Vikram Phatak, CEO of NSS Labs, many anti-virus vendors offer zero protection against some of the common attack vectors[1]. The bad guys know this and often use it in their attacks because malware is such an effective way to bypass traditional security controls.

Our profession is changing, and frankly I'm ecstatic! The last several years of compliance has certainly raised the bar—albeit its new height is merely knee high vs ankle high in many cases—but I think most of us would put major head-sized dents in our desks if compliance was the future of information security. Compliance has an important role in information security, but it should be a byproduct of security. With compliance driving security we have a horse/cart order problem. It's not sustainable, and ultimately weakens our posture over time as compliance drags its feet behind the types of attacks we face today. So if we're not policy monkeys or compliance wonks, what are we becoming?

The information security professional of the future will need to be more intelligence driven and defense focused to survive. Indeed, our three-letter-agencies in the US (and comparable organizations globally) are teaching the mindset we need in the private sector today. We must be able to expand beyond the "defend everything from everyone" mentality to truly understanding our adversaries, fully understanding how our businesses operate digitally[2], and having both comprehensive visibility into our infrastructures (or ones we leverage) and actionable intelligence about threats and adversaries to deploy our limited resources in ways that maximize our defense capabilities. That's really a long way of saying that we have to act like an army if we are to ward off attacks by an army.

Private sector enterprises are now faced with fighting the equivalent of electronic armies, and according to many intelligence professionals that I interact with there appears to be cooperation and sharing of resources between organized crime and nation states—collectively sharing information and resources to achieve their goals faster than we can defend against them. Never before have companies in the private sector faced attacks of this this sophistication and kind, and as of today there is little they can do from a retaliation standpoint. Couple that with things like cloud adoption, mobility, and Bring Your Own Device programs and we're truly in a losing battle unless we change our ways. In today's world we are expected to keep the enterprise safe without controlling the infrastructure, network, or devices that may interact with our systems.

FOOTNOTES

[1] *Personal email, 12 October 2012.*

[2] *Like knowing what information is used in the business, how it uses it, how its obtained and stored, how it is disposed of, and everywhere it lives and moves.*

Your mission, and you better accept it, is to rethink how you deploy your limited set of resources to defend your companies from these electronic armies. Blanket protection is inefficient, and traditional security controls are not nearly as effective as they once were. We have to be able to analyze behaviors to catch bad guys hiding in plain sight. We have to think about authenticating individuals and sessions, not devices and networks. And all of that starts with a good understanding of the business and its digital footprint.

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