Herding Cats:
Do it Differently

May 2011

BRANDENWILLIAMS
SECURE BUSINESS GROWTH

When I first read the theme for this month, I though about how circular the theme sounds. Is it changing or is it not? Because either things change, or they remain constant. I'm going to interpret it as "recurring themes in security," meaning that over time as business and technology change, many times the underlying themes stay the same which could be both to the benefit and detriment of our security posture.

Two months ago I wrote about "The New Network Security Paradigm" in the Journal, whereby we explored the changing nature of information technology in the workplace. Moving computing resources into handheld devices might be as dramatic of a paradigm shift as computer networks in the workplace, client-to-site VPNs for remote access, and wireless networking. Yet, for the most part companies have not changed much in their approach to protecting themselves. VLANs separate and segment traffic[1], firewalls protect us from the bad guys, internet facing servers get a special area of the network, and our mobile workforce can connect back into the corporate office over virtual private networks.

Attackers are much more creative and destructive than they were fifteen years ago. Code Red wreaked havoc on organizations in the early 2000s, but Code Red and it's kin were pretty broadly distributed and not really designed to compromise or extract information from a single target. What's the solution there? Lots of patching, email filtering, and added firewall rules. Targeted attacks today take on a much different look and feel and typically require some kind of human element to successfully complete. The human element could be social engineering, spear phishing, or collusion from an insider. But what happens when a company today is breached?

Lots of patching, email filtering, and added firewall rules.

Doesn't that sound a bit familiar? It should.

Security is often referred to as a mixture of people, process, and technology. More than ten years ago, the inherent security around many internet facing technology solutions was soft. You didn't need to worry about the people preventing an information security breach[2] because the technology had enough holes in it that an attacker could find one large enough to squeeze their way through. Many hackers and security professionals today may even debate that the security around some of the technology we deploy and rely on is still quite soft, but now focused on mobile computing and application weaknesses.

Social engineering is a completely different game that is tremendously effective, and the only way to protect your organization is through training first and then potentially the deployment of advanced monitoring and detection technologies. No, I'm not talking about a SIEM. I'm talking about advanced, real-time visibility into your systems with the ability to act and react to stop and remedy a security breach. Very few organizations either feel this type of protection is required, or their risk models show the benefits do not outweigh the costs.

We're entering an era of dramatically reduced trust in our systems and networks, but we haven't changed what we do in response. Most companies I visit still view their internal networks as trusted, and make the assumption that they are not compromised. In my March column, I made the following statement: "You can't trust the LAN anymore, and

FOOTNOTES

[1] *CAREFUL with how you use the term "segment" in this context.*

[2] *Though you did need to, and often saw it, when physical security breaches occurred.*

you probably never should have.” It’s just too easy to connect a device to most LANs. Larger companies typically lack the ability to monitor on such a small scale to detect a device operating discreetly on the network, and smaller companies don’t have resources paying attention to something like this. So why would we use the same methods to protect our networks even though our usage of information technology in business is evolving?

As security professionals, it is our jobs to accurately reflect operating risk back to the business, and speak to our executives in a way that allows us to move our agendas forward—namely protecting the business against information security threats. We have to evolve our thinking, our interaction with the business, and our approach to protecting the enterprise.

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, buy his book, or reach him directly at http://www.brandenwilliams.com/.