Herding Cats:
The New Network Security Paradigm

March 2011

BrandenWilliams
SECURE BUSINESS GROWTH

This month’s theme is near and dear to me working for a company that is generally friendly toward non-company owned devices. It’s wasn’t long before the first production iPad made its way onto the corporate network and emails began arriving with the “Sent from my iPad” signature.

It seems that the line between personal and work-issued devices doesn’t really exist anymore. Maybe it’s a suggestion or guideline now. Take a serious look at your electronic activities over the last month. How much work did you do on a personal device and how many personal activities crept onto your work machines? Everyone here is guilty of taking a work call or answering a work email on their personal device, and I can imagine that every once in a while a stock trade, fantasy football lineup[1], or a last minute gift purchase might be made on a work machine.

Webmail and smartphones in the workplace helped make this more prevalent.

“Thanks”[2] to webmail, I don’t need my work machine, I just need a machine. Thanks to smartphones, I don’t need my personal music device, I just need earbuds. In fact, in my world my personal machine IS my work machine. Our company drinks our own champagne, which means (among other things) I have an on-demand virtual desktop with all my productivity applications ready for me to use. I supplied my machine, purchased all of my own software licenses for my part, and use my company’s licenses for some of the more advanced tools that live in my virtual desktop.

I believe this is the beginning of a trend that will continue over the next several years. Workers will be expected to show up with their own gear or be given a periodic allocation of funds to procure one. Most kids going through college today have their own laptop—granted, in varying degrees of disrepair—and smartphone. What does this mean for security professionals? Quite a bit actually.

For years, the general paradigm for network security has been that if a device is on the LAN, it should be trusted. Therefore, we must put controls in place to prevent devices from joining the LAN. Insert VPNs and a remote or traveling workforce and we have another issue to consider… should these remote devices trusted? Devices that we cannot physically secure and control? Now include on-site visitors that need network access. Finally, add users bringing their own machines to the table.

You can’t trust the LAN anymore, and you probably never should have.

It’s time to re-think the models we use to deploy security inside of our companies. If you assumed the bad guys were on the LAN, how would that change your strategy for keeping data secure? If you were forced to allow non-corporate owned and operated devices on your network, how would you build controls to do this in a secure way?

It is possible, you just have to think creatively.

And with the economics of cloud computing, you better believe that your company’s next IT transformation is going to take concepts like this into account when allocating budgets and strategy. Imagine how much money your company could save without asset tracking, device procurement and management, and even facilities to house carbon-based life

FOOTNOTES

[1] *I am missing the NFL already. LEsigh.*

[2] *You see what I did there? It’s like “Congrats on being Executive Platinum again!”*

forms! I certainly would not want to be in commercial real estate when companies start sending large parts of their workforce home as opposed to keeping them in high rises.

Pop quiz, hot shot. Assume that your network has already been compromised and that bad guys are present. Assume that you will not be able to control (and thus won't have to support) every single device on your network. Assume that you will have multiple points of entry from the outside, which can be somewhat controlled, but must support workers in the field. What do you do?

What do you do?

Now that you have broken the traditional paradigm, take those assumptions and architect a solution that meets the goals of your company while keeping you in check with the various types of security and compliance initiatives you handle on a daily basis. It's not impossible, and you will have to compromise in some areas while investing in others.

It's going to happen, will you be ready?

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/.