Herding Cats:
Is there an App for This?

November 2010

BrandenWilliams
SECURE BUSINESS GROWTH

Take a brief look at your mobile phone. Is it a smart phone? Does it have web access or an application store? Chances are, not only is it a smart phone with some kind of application store[1], but you are probably using more data services now than you did one year ago. It's not by accident either, these devices are becoming more powerful, the apps more user friendly and numerous, and the multitude of ways to get data typically includes both cellular data and Wi-Fi. At any rate, the device will most likely have some kind of IP address on it, making it reachable by other devices.

When you are using cellular data, your device may be more protected from the internet and bad guys, but if you pop on Wi-Fi at your local cafe, anyone else on that network can interact with your device. Many smart phones store much more data than you might expect, which really makes the most serious vulnerability the theft or loss of the device itself. "So what?" someone might say. "I don't care if someone can see what apps I have on there or answer my phone." But what if those apps are mobile banking applications that are storing your credentials instead of purging them?

Hopefully the red lights and sirens are at full tilt now.

Businesses are pushing more and more customer interactions to self-service models like web and mobile applications. If you told me three years ago that I would be able to pay a bill from my smart phone using my bank's free application I would have called you a delusional optimist. If you told me that ten years ago, I would have called you a nutjob. But it's a reality, isn't it? Even smaller banks and credit unions[2] have joined the ranks of the big banks to provide this level of customer interaction. Not that I trust a big bank any more than I would a small bank when it comes to my security, but I do know that big banks have more staff and manpower to watch over these applications when compared to a small bank. And yet I am positive that even apps from small banks have been installed on more than one smart phone, and are probably in use daily.

How long will we have to wait before we see targeted attacks against certain applications? Every major mobile platform has lived through a severe vulnerability exposure over the last two years, so we know that the bad guys have started to look at them.

And companies are paying attention.

My company was recently hired to do an analysis and penetration test against an application for a popular mobile platform. Three years ago, an expense like this showing up on a P&L might cause someone to undergo a forced career change. But today, it's seen as part of the due care that a company takes for legal defensibility.

If you went to BlackHat this year, you probably noticed attacks focusing on applications, browsers, and mobile devices. If you didn't, you missed some cool and some scary attacks. Now when I hear people telling me that they do all their web browsing in destructible virtual machine appliances, I don't see them as paranoid. Well, ok, maybe a little paranoid, but also taking responsibility for their credentials in a way that would help prevent bad things from happening.

FOOTNOTES

[1] Or marketplace, I love you too Droid.

[2] Fun experiment, take your device and search for "credit union" in your application store/marketplace.

Remember, as security professionals, it is OUR JOB to make sure that the business understands and addresses the risks associated with using technology as a medium for customer interaction. Be it regular testing of controls[3], code reviews, secure code training, or spreading liability around through contracts, we must ensure that we protect our stakeholders. Is a Draconian approach to security required to make this a reality? No, and it wouldn't help our overall charge of securing the enterprise. But a meaningful approach, commensurate with the risk of loss or breach of the data, is what we must drive forward.

FOOTNOTES

[3] *And GOOD testing here, folks. Not checkbox audit testing.*

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/.

TEL 214 727 8227
FAX 214 432 6174
BLOG brandenwilliams.com
EMAIL brw@brandenwilliams.com

brandenwilliams
SECURE BUSINESS GROWTH