Herding Cats:
Vulnerability in Numbers

December 2008

BrandenWilliams
SECURE BUSINESS GROWTH

The phrase “safety in numbers” is a rationale used by people everywhere. If you walk down a dark alley in a sketchy neighborhood at night by yourself, you are much more likely to be mugged than if you happened down that same alleyway with Tony and ten of your friends ready for a rumble. The phrase is not always life saving. If you are the one person needing help in a crowd, the mentality for most is “Well, at least he’s in a crowd. SOMEONE will call.”

If everyone has that same thought, then no one calls. What if we take the theory and try to apply it to information security?

Corporations store trillions of bytes of data, employ thousands of workers, and manage tens of thousands of devices. How can you be sure that you address the few critical vulnerabilities that could easily be lost in the masses?

A colleague of mine recently described this problem, and I’m going to coin it Hizver’s Insecurity in Large Numbers Theorum. Her basic thesis is that information technologists are small number thinkers when in contrast, successful attacks tend to be performed against large populations where hackers are betting on one of the million to make a mistake.

Information security differs from man other types of business functions. When banks issue lines of credit, they expect that some of the people they originally deemed as credit worthy will default on their loans. This is an acceptable risk that banks work hard to minimize such that one bad loan won’t put them out of business.

In the information security world, one mistake can put you out of business as we have seen in the past.

For example, many companies use formulas for creating new customer account numbers. One reason for this is to prevent someone from just adding or subtracting one number from their account number to instantly gain access to another’s account information. If a breach of a significant set of these numbers occurs, a savvy observer may be able to detect a pattern. With some applied mathematics, he could reverse engineer the process to predict numbers he does not have. Depending on what additional information an account number will produce, that same observer could potentially compromise a significant amount of customer data. What is impossible with small subsets becomes possible and even probable with large sets of data.

Powerful technology is becoming more compact, and users are becoming more savvy. Consider a campus where a few thousand employees work every day. Chances are that one of them might go purchase a wireless access point so they can work outdoors on a pretty day. Or better yet, if the corporation offers an open wireless network for vendors, chances are high that someone with a new iPhone might associate with it and log into their corporate email, potentially allowing a hacker to capture their domain credentials.

Maybe the best and most likely example would be a hacker that targets one particular corporation, offering free WiFi[1] in the area of their campus, hoping that one of the employees decides to work outside of the office. Once the victim joins, the hacker either quietly sits and captures traffic waiting for the victim to slip-up, or the hacker may launch an attack against the device itself.

FOOTNOTES

[1] Sometimes “Free” WiFi is not always “free.”

One of the reasons that Phishing is so successful is based on this theorum[2]. If a hacker sets up a false banking website and blasts an "Account Update" email to ten million email addresses, you are guaranteed to get at least ONE set of valid credentials to commit fraud. Or if you send enough "You just won the lottery!" emails out, you are guaranteed to find one unlucky bloke that will give you his banking information.

Whether the theorum is applied to end users or corporations, the attacks will be successful. The significance of the attack's success depends solely on how significant that "one" account or user is.

What's the moral of this tragedy?

Large numbers work against us in this industry[3]. In order for us to prevent that big event from happening on our watch, we must be diligent to remove the vulnerabilities present when working with large numbers. This means building more intelligence into both your infrastructure and your people[4].

FOOTNOTES

[2] The others being that people want something for nothing, and whiz-bang technology baffles many of us.

[3] Except when factoring them of course!

[4] Keep in mind that this is mostly a people problem that is expensive to solve with technology.

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