‘Cybersecurity by obscurity’ isn’t good business strategy

09.11.17

This article originally appeared in the September 11, 2017 issue of the North Bay Business Journal.

Until recently, small- and medium-sized businesses have not been specifically targeted by hackers and could avoid cyberattacks by simply employing the concept of “security by obscurity.”

If your business was not large, or in politically charged industry, then it was generally safe from targeted cyberattacks. But those days are over.

Here are a few reasons why size of your organization no longer matters.

First, the prevalence of criminal ransomware attacks (where the attacker encrypts the victim’s data and then extorts a payment to decrypt it and make it accessible again) has proven to be profitable for attackers against businesses of all sizes. In many cases, attackers don’t even know who they’ve successfully encrypted, and they don’t really care. If the cyber criminals can encrypt your hard drive’s contents, and you’re willing to pay to get the drive decrypted, then your business is big enough for them.

Recently, during the course of the well-publicized ransomware attack against Hollywood Presbyterian Medical Center, (see https://www.wired.com/2016/03/ransomware-why-hospitals-are-the-perfect-targets/) it became clear that the bad guys didn’t even know they were attacking a hospital. Many other examples of small to medium-sized ransomware attacks quickly followed. This type of indiscriminate attack undermines the whole concept of small business cybersecurity by obscurity.

Next, foreign nation-state sponsored attackers, e.g. the Syrian Electronic Army or the Digital Caliphate, are targeting absolutely every commercial entity they can identify operating within the United States. Until a few years ago, their efforts primarily focused on government, law enforcement and utilities, but not anymore.

As those primary targets have hardened their cyberdefenses, attackers have moved down the food chain to smaller entities – and these foreign nation-state attacks are often covert. Foreign sponsored entities such as The Lazarus Group, which is believed to be sponsored by the North Korean government, is not interested in holding your company for ransom or monetizing your sensitive data. These types of attackers simply want to place dormant logic bombs on your business network that remain inactive until receiving a “go” sign, at which time all the bombs will all launch at once, with the intention of crippling our nation’s communications infrastructure.

Or maybe a foreign government sponsored entity just wants to enlist your company’s network equipment into their “botnet” army. By turning your network gear into an automated zombie awaiting orders, your company may become part of a much wider attack against a third party, such as a hardened government agency. The fact that your business is small or medium-sized acts as no defense against this type of attack.

Finally, your small to medium-sized business now faces the challenge of attackers with staggering computing resources at their disposal. Until recently, a decent password protecting remote access to your business was sufficient, because cracking passwords requires significant computing power. Attackers wouldn’t bother targeting the small guys, because the cost of all those computers was prohibitively expensive given the limited return on investment.

Now that password-cracking processor cycles can be rented for pennies a minute from Amazon Web Services and similar cloud vendors, attackers can cost-effectively launch password cracking breaches, and similar automated attacks, against business entities of all sizes.

Tactically speaking, avoiding ransomware attacks involves imposing strict prohibitions on inbound email attachments/links and performing frequent, offline backups. Defending against logic bomb and botnet threats requires up-to-date patching of network gear and hardening of weak vendor default configurations.

David Trepp*, partner in BPM’s Information Security Assessment Services Practice, has led over 1,100 information security penetration test engagements for satisfied customers across all major industries throughout the United States and abroad. He has given dozens of presentations to audiences nationwide, on a variety of information security topics. Prior to joining BPM, David was founder and CEO of Info@Risk, a leading comprehensive penetration test firm. David has worked in information security with commercial, healthcare, government, financial, utility, law enforcement and nonprofit organizations since 1998. To learn move, visit bpmcpa.com/cybersecurity or contact David directly at DTrepp@bpmcpa.com.*