Top 5 Cybersecurity Threats Facing Title Industry in 2018 – Part 3

Overview

In part 1, we examined business email compromise, which occurs when a hacker gains access to a corporate email account and assumes the identity of the corporate user in order to defraud the company, employees, customers, or partners. In part 2, we looked at some of the ways that hackers obtain and use stolen credentials in order to take over an account.

In this post, we'll talk about other ways that systems get hacked and data gets exfiltrated.

Threat #3 – Hacking / Data Breach

The Problem

The term hacking can be defined as an unauthorized intrusion into a network or a computer. 48% of all breaches in 2017 featured hacking as the main tactic used.

The motives of hackers can vary widely, and can include data theft, intellectual property theft, disruption of business operations, ransom, wire fraud, or other types of monetization. With 73% of all hacks perpetrated by outside actors and 76% financially motivated, it is clear that an outside actor wants your money, and these actors are increasingly sophisticated. The image of a hacker wearing a hoodie in his mother's basement couldn't be farther from the truth – in fact, 50% of all breaches in 2017 were carried out by organized criminal groups and another 14% were carried out by state-affiliated or nation-state actors.

Title companies are wrong to think that they are too small to hack, or that they can fly under the radar. 58% of all breaches in 2017 occurred in small businesses.

Regardless of motive or tactics, it is safe to say that you do not want an unauthorized intrusion into your business network. Equally alarming is the fact that in 68% of all breaches, it took months or longer to discover the breach. Meanwhile, it only takes a hacker hours to exfiltrate the data they want, making them long gone by the time you discover anything ever happened.

How It Works

I like to think of hackers like electricity – they are looking for the fastest way to get to ground (i.e. the fastest way to get into your network and get out with some money). I have heard many title industry executives say "I'm just a little old title company, who's going to target me or even

know I exist?" Unfortunately, this sentiment is altogether incorrect – hackers are targeting title companies because they facilitate the transactions, but hackers don't even need to know you exist. With automated hacking tools, bots can do the dirty work for them.

Everything that runs software has vulnerabilities that can be exploited, and exploiting these has never been easier. Automated bots scan every device on the Internet, looking for vulnerabilities to exploit or open doors into a network. Chances are your title company gets scanned dozens, if not hundreds of times per month. These are not targeted attacks against your company, but when a bot finds an open hole in your network, the human hacker will begin their dirty work.

Malware is another common way into a network, and is quite simple. A user is tricked into installing malware, which then provides the hacker with a tunnel into the network from which they can stage their attack. Malware can be used to log every keystroke, steal information, encrypt files for ransom, or spread to other parts of the network.

How to Protect Your Organization

1. Reduce your attack surface

Don't be an easy target. Understand which of your systems are open to the outside world and the reasons they need to be. Reduce the overall number of systems that are accessible from outside. This can be done by reviewing your firewall rules.

Implement a vulnerability management practice in which you regularly discover the vulnerabilities on all of your systems and ensure that those get patched or otherwise mitigated.

2. Implement next-gen antivirus

Traditional antivirus is no longer effective, as it relies on signature-based detection, meaning it only detects what it knows. That leaves your company vulnerable to fileless malware, zero-day attacks, and non-malware attacks. Non-malware attacks use legitimate software, such as PDF's, Word documents, macros, and PowerShell to infect a computer without alerting antivirus solutions.

With over 53% of breaches utilizing non-malware, it is clear that a new approach is needed. Next-generation antivirus solutions are able to use behavior analysis and machine learning to analyze the behavior of the software running on your computer and are able to detect malicious processes without the need for signatures. This means they can detect malware, non-malware, zero-day, and fileless malware where traditional antivirus can't.

3. Prevent malicious downloads

Run all internet traffic through a secure internet gateway, which will block phishing websites, malware downloads, command and control communication, and other malicious internet

traffic. These systems are very effective and are probably the easiest security layer to implement. By capturing all outbound requests, these systems can also alert you to possible compromise or data exfiltration.

4. Detection is just as important as prevention

Many organizations are searching for a silver bullet solution to prevent hackers from getting into their network. Unfortunately, that solution just doesn't exist yet. Firewalls and antivirus alone are not enough. That's why it is imperative that your organization have the ability to detect threats as they occur and shut them down before damage can be done.

The statistics are clear that it only takes hackers minutes to get into your network and hours to get out with all of your data. Meanwhile, most companies don't even know about it until months later. Today's detection systems can alert you to malicious behavior in real-time, allowing you to shut down the threat quickly and minimize damage. Unfortunately, these systems are very noisy, and to be effective they require full-time monitoring by either an in-house security analyst or an outsourced service provider.

Next Time…

In the next post, we'll go deeper into today's malware and ways to prevent and detect infections.

Drew Bradford is a TLTA member and President of Sigma InfoSec, a company that provides enterprise-class cybersecurity solutions to the title industry.