Top 5 Cybersecurity Threats Facing Title Industry in 2018 – Part 1

Overview

Title companies provide vital services to customers during what can be one of the most stressful times in their lives. Title companies diligently work to protect home owners and lenders from lawsuits or other claims that may arise over title disputes. Additionally, title companies often maintain escrow accounts and facilitate the closing of properties. In carrying out this work, title companies often collect sensitive non-public personal information about their customers and facilitate large volumes of high dollar transactions.

Unfortunately, these factors make title companies a high priority target for hackers who would seek to steal, defraud, or disrupt their organizations. Title companies are often the target of phishing schemes, wire fraud, account takeover attacks, and ransomware, among other threats. Small businesses are no longer able to “fly under the radar” of hackers, as over two thirds of all breaches occur in organizations sized between 11-100 employees.

Title companies rely on their reputation to gain new and repeat business and must diligently defend their reputation and protect their brand. Real estate closings are time-sensitive and therefore title companies cannot afford to miss mortgage-related transactions due to ransomware or other system outages.

Threat #1 – Business Email Compromise / Wire Fraud

The Problem

Business email compromise (BEC) 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.

According to the FBI, participants involved in real estate transactions are particularly targeted in such attacks. Real estate transactions are complex, time-sensitive, stressful, and involve multiple parties. This is the perfect storm for hackers, and it pays off, big time.

The average successful wire fraud amounts to $140,000 compared to the average successful bank robbery of $6,500. The real estate sector alone had more than 9,600 victims and lost over $56 million in 2017, according to the FBI.

BEC is a particularly dangerous problem for companies whose data resides in the cloud because stolen credentials allow hackers to access not only email, but also other resources such as files, chat, calendaring, VOIP systems, and more.

How It Works

After gaining access to a corporate mailbox, the attacker first searches for low-hanging fruit, such as employee W-2's, credentials saved in emails/notes, banking information, intellectual property, or other valuable data.

Often times, the attacker will create mailbox rules to automatically forward new emails to an external mailbox which can continue to receive mail even after their access to the mailbox has been closed.

Next, the hacker will study the contents of the mailbox, identifying key employees, customers, or partners on which to perpetrate their next scam. They then target those individuals using the compromised corporate identity by requesting money transfers, changes to payee information, altering wire transfer information, sending false invoices to customers, or other tactics.

How to Protect Your Organization

There are many ways in which an attacker can gain access to corporate credentials, including malware, phishing, social engineering, or other methods of account takeover. Therefore, as with any other cybersecurity problem, a layered approach is critical to counter the sources of the problem.

1. Implement Email Security Best Practices

Start by ensuring you are using best practices to secure your email environment. This means utilizing the built-in security features of your email provider, such as dual-factor authentication, spam filtering, and data loss prevention. Make sure you turn audit logging on – countless companies find themselves unable to investigate the source of a breach simply because they didn't have logging properly configured.

2. Prevent Phishing and Account Takeover

BEC often begins with a phish or other common account takeover methods. Focus on preventing these and you will go a long way toward preventing BEC. Implement advanced email protection with effective spam/phishing detection. Run all internet traffic through a secure internet gateway to block phishing sites, malware, and other malicious communication. Invest in next-gen endpoint protection that does not rely solely on signature detection. Monitor the dark web so you can be alerted when employee credentials are stolen from other sources.

Finally, implement a security training and phishing simulation program to educate and you're your employees. We'll go into greater detail on these items in Part 2.

3. Monitor Your Environment

You need the ability to detect malicious activity against your critical assets. If someone were to log into your CEO's email account from an IP in Africa, would you even know about it? A monitored detection system that can extend into your cloud providers and is backed by the latest threat intelligence is critical to uncovering ongoing breaches and shutting down threats before they can cause damage.

4. Create Policies

Implement a wire policy that is enforced and communicated to all parties. Employees and clients need to know to never send a wire based solely on an email and should verify the accuracy of all wire transfers in person or over the phone. Transfers should only be performed by select personnel on dedicated computers that are known to be malware-free.

Next Time…

In the next post, we'll talk about ways that hackers are able to take over corporate accounts and the steps you should be taking to prevent them.

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