frogworks
Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

"Rise above the storm and you will find the sunshine."

-Mario Fernández

June 2019

Issue 6, Volume 9

This monthly publication provided courtesy of Alex Bleam, Owner of Frogworks

We are excited and proud to announce that Frogworks has been recognized as one of the world's best MSPs by Channel Futures!

Channel Futures MSP 501 2018 WINNER

THE ULTIMATE GUIDE TO THE WORLD'S BEST MSPs

Five Common Insider Threat Profiles

Insider threats come in many different shapes and forms and can be a frustrating problem to diagnose. Adding to the problem is the fact that even the most reliable and seemingly harmless employees can change in an instant and pose a threat. Protecting your company against these sometimes-unpredictable actors requires an understanding of the various profiles that exist and their motivations. To help, here is a quick look at five of the most common Insider Threats that companies may face, and some quick tips on how you can protect your organization from each of them.

1. Disgruntled Debbie
The disgruntled employee is often the first profile that comes to mind when most people think of Insider Threats. Disgruntled Debbie is the employee who didn't get the performance rating or the raise she wanted and decided to retaliate. While Debbie is a fictional character, this threat is very real. For example, this became a harsh reality for Tesla one summer. An angry employee stole some of the company's proprietary information and began to share it with 3rd parties, compromising the company's most sensitive business assets.

2. Oblivious Oliver
Oblivious Oliver is the employee who has no clue that he is introducing risks to the organization. A large percentage of cyber security incidents start with human error, and Insider Threats are not always malicious in nature. Often, these threats stem from everyday employees who don't know about cyber risk and, equally important, how to protect against them.

We saw a prime example of this in the RSA breach. RSA has been known as a trusted security technology provider for quite a while now, and their compromise was a stark reminder that even large security companies and their employees are not immune to attacks on the unsuspecting or oblivious employee. In this case, a simple click on a phishing email by a gullible employee led to the compromise of approximately 40 million records. The phishing attacks, like most today, were targeted and mimicked trusted contacts.

Curious employees also fall into this category. These are the employees who just want to know "What could happen if..?", "How far might I be able to get with accessing something I shouldn't have access to?", "What might actually happen if I clicked on this suspicious email?". Deep down inside, some employees are just curious kids inside, wondering what the button does.

The best solution for Oblivious Olivers is training and awareness. By helping Oliver understand the risks of clicking on malicious links and encouraging him to approach all emails with caution, attempted phishing attacks against the Oblivious Olivers of this world are less likely to succeed.

3. 3rd Party Patrick
Someone doesn't have to be a full-time employee in your organization to be considered an Insider Threat. Third party contractors and vendors often have the same or very similar access privileges even though they aren't directly employed by the company. Their introduction of risks to the

(Continued on page 2)

company can be intentionally or unintentionally malicious depending on the circumstance.

The list of breaches stemming from third-party errors is unending. A few examples from last year alone include Saks Fifth Ave, Lord and Taylor, Best Buy, Kmart, Delta, Target, Sears, My Fitness Pal, and many, many more. In each of these cases, the company realized significant losses as a result of their partner's actions, or lack thereof. This makes having a strong third-party security program that includes both technology controls and legal controls against a third-party breach imperative to stopping 3rd Party Patrick dead in his tracks.

4. Terminated Tony

Noticing activity from the account of someone who's been recently terminated? As Terminated Tony leaves, he creates back doors and tries to retain access to systems and data for future use. This is an unfortunate and costly mishap that occurs quite frequently. In one real world example, an ex-employee of Allen & Hoshall continued to access the companies files for two years after he left the company. He was able to export intellectual property worth almost half a million dollars – an action that landed him in jail for a year and a half. Ensuring that after an employee is terminated, access to systems throughout the company and network are promptly terminated is an important step to ensuring that Terminated Tony doesn't wreak havoc on your company after he's gone.

5. Malicious Marvin

Unfortunately, some insiders are just downright criminals. Driven by financial hardship, gambling problems, greed, substance abuse and more – employees steal from their employers for numerous reasons. These employees are deliberately looking to breach the company's security and take advantage. One example of this occurred when an employee from Anthem Health caused a breach that resulted in unauthorized disclosure of personal data for 18,000 patients. The file, which contained social security numbers, full names, medical information and more, was sent to the employee's personal email address for access outside of work. It appears that the employee was intentionally stealing and misusing the data, and after the discovery of the breach, was investigated for numerous counts of suspicious activity.

Malicious Marvin is a very real threat. Life happens, and unfortunately, even the best employees make poor choices. It's important to apply the concept of least privileged access and only grant access to users on a need to know basis. Furthermore, having insight into user activity through logging and monitoring, implementing a robust data loss prevention program, and having strong detection and response capabilities can help keep Malicious Marvin at arm's length within your organization.

Conclusion

Protecting your organization against an Insider Threat requires that you first understand what those potential threats might be. Disgruntled Debbie, Oblivious Oliver, 3rd Party Patrick, Terminated Tina, and Malicious Marvin can cost your company millions of dollars if gone unchecked. This list provides insight into some of the most common profiles but remember that there are no limits to the motivations and profiles of Insider Threats. Anyone from business colleagues to your cyber security team could potentially pose a threat. This makes having a robust cyber security program based on the principle of "defense in depth" essential to stopping the insider threat.

Some Dell Systems Are At Risk Of New Hacks

Do you use Dell equipment at home or in your office?

If so, then the recent discovery made by independent security researcher Bill Demirkapi should give you pause.

Recently, Mr. Demrikapi discovered a flaw in the company's SupportAssist utility that comes pre-installed on most Dell systems.

If you have an older Dell, know that SupportAssist was recently re-branded and was formerly known as Dell System Detect, which may be a name you're more familiar with. At the root though, it's the same code and both versions of the code have the same flaw.

The program is designed to interact with Dell's support website. This is where it will scan for service codes and tags that match your system and then automatically download and install driver updates as needed to keep your system up to snuff. It's a good piece of software that performs a valuable function, so it probably comes as no surprise that hackers took note and promptly found a way to take advantage of the code's functionality.

Dell, who has been working with Mr. Demirkapi since he reported the issue to them, explains it thusly:

(Continued on page 3)

(Continued from page 2)

"An unauthenticated attacker, sharing the network access layer with the vulnerable system, can compromise the vulnerable system by tricking a victim user into downloading and executing arbitrary executables via SupportAssist client from attacker hosted sites."

In essence, the hackers use a variety of tricks to fool your system into thinking it's getting updates from Dell, when in fact, it's being fed poisoned files from a site controlled by hackers.

The bug impacts all Dell SupportAssist Client versions prior to version 3.2.0.90. The company has already fixed the issue. The main takeaway here is to check your SupportAssist version number to see if you're in the safe zone, and if not, download the latest version right away.

Chrome Will Offer More Ways To Control Web Tracking

Google announced a pair of important security features of upcoming versions of its Chrome browser at this year's I/O Developer Conference.

Both changes are designed with the same goal in mind:

To give users some additional tools to block or at least mitigate the threat of online tracking.

The first of the two new features is called Improved SameSite Cookies, and as the name suggests, it's an attempt to improve cookie handling. As you probably know, cookies are created when a user visits a particular website. Cookies are the mechanism by which that site remembers information about a user's visit. It stores information such as preferred language, items you may have in your shopping cart (if the site has an eCommerce element), your login information, and the like.

Unfortunately, cookies are often used to identify users and track their movement and activities. That is not only by the owners of the site, but also by any third-party the site shares data with. As an example, cookies are the reason that re-targeting ad strategies work. Worse, there's currently no good way to categorize and identify how websites are using cookies. To every browser in use today, they're all considered to be the same thing. That is why when you go into your browser settings page and clear your cookies, it automatically logs you out of all websites where you've saved your login credentials.

Google's new feature would change that, allowing you to selectively delete cookies based on what they're doing. That means you'd be able to preserve your saved logins while blocking or deleting cookies used for other purposes. In a similar vein, the company's planned Fingerprinting Protection feature seeks to make it harder to fingerprint people that are using the Chrome browser. That is a tactic commonly used to track user activity without their knowledge and consent.

It remains to be seen how robust these new features will be, but if they live up to expectations, they'll be two powerful new additions to Google's growing suite of user controls. That's a very good thing.

Password Policies Getting Update From Microsoft

Industry experts have been predicting the death of the humble password for decades. To date, those predictions have amounted to nothing.

Passwords are still with us, and still serve as the cornerstone of security, even as other measures have arisen alongside them to help better secure your all-important data.

Even though passwords aren't gone, the security landscape is changing. Recently, Microsoft has announced another step down that path of change. They're doing away with the notion of forced password changes.

The logic is hard to argue with. The policy of forced password changes really doesn't offer all that much in the way of protection. It often creates as many headaches and problems as it solves, because users tend to make small, virtually meaningless and easy to predict changes to their passwords. Or, they often forget their new ones anyway.

While Microsoft is no longer forcing password changes at periodic intervals, they are leaving the option available for Enterprise users to establish their own forced password change thresholds if they choose to do so. In tandem with the coming change, they're also recommending that security professionals perform a periodic review of passwords to ensure that the passwords in use aren't on the list of the UK National Cyber Security Centre's list of the 100,000 worst passwords.

One important thing to note is the fact that the company isn't making any changes to its requirements for minimum password length, complexity, or history. That is essential in terms of keeping users from simply recycling the same two or three passwords, switching endlessly back and forth between them.

It's also worth mentioning that these changes could benefit companies that are currently under audit. That is if the auditing agency is using Microsoft's security baseline as a guideline. That makes this seem like a small , but it is more significant than it may first appear.

We now have an E-newsletter!

… but we might not have your email address! If you would like to receive our newsletter though email please visit us at **www.getfrogworks.com/newsletter** and sign up.

Security Is Now A Concern For Open Source Software

This year's Open Source Security and Risk Analysis Report analyzed the anonymized data of more than 1,200 commercial codebases from 2018. According to the report, managing open source risk continues to pose a significant challenge for industry.

The Synopsys Cybersecurity Research Center produces the report, and found that 96 percent of the code bases they analyzed contained open source components.

These were found with an average of 298 open source components per codebase. This is an increase from an average of 257 found in 2017. Disturbingly, the research center found more than 16,500 vulnerabilities over the course of their research, with more than 40 percent of the codebases analyzed having been found to contain at least one high-risk open source vulnerability.

The major problem does not stem from the fact that open source components are more prone to bugs. Rather, it stems from the fact that while companies are often quick to embrace open source software, they tend to do a relatively poor job of keeping it up to date.

The research group summarizes their findings as follows:

"At the end of the day, all software is vulnerable to attack - without exception - and the nature of open source software is to shine a light on the issues it has, leading to increased visibility of bugs, not an increase in bugs.

The security risk is significantly diminished by increasing visibility. If you're not using open source components, you'd be using closed source components - either commercially available or hand-rolled - that have just as high of a likelihood of being vulnerable. Except that you just don't know about the bugs, unlike with open source components."

The group recommends the following actions. First, make regular use of readily available tools that can be used to scan your codebase to identify the open source components and their version numbers. Then check this data against one or more vulnerability databases to be sure you're adequately protected. If you're not currently doing so, the time is now.

Persistent Banking Trojan Virus Launches New Phishing Scam

The venerable banking Trojan known as Q-bot is back in the news, having recently been spotted in the wild as part of a sophisticated new phishing campaign designed to claim a new generation of victims.

Q-bot is one of the oldest banking Trojans still in use, and has a history that stretches back more than a decade.

In this most recent incarnation, the malware is being delivered via an email which appears to be a reply to an existing email chain. The body of the email contains a poisoned link which, if clicked will install the malware in the background.

Once in place, it creates a backdoor to the compromised machine in question, allowing hackers access any time they like. It also serves as a key logger and general spy. It can steal financial data, banking data, other logins, credentials, and of course, makes it possible for the hackers to install additional malware as they see fit.

The reason Q-bot is still enjoying use of stolen data is that it's very good at what it does, and the developers of the code have taken steps to keep it up to date. This, combined with finding new and innovative ways of introducing the Trojan onto target systems has made it as close to a persistent threat as we've seen when it comes to malicious code.

The latest campaign appears to borrow from the success of a similar campaign launched last year involving a Trojan with comparable functionality called Emotet.

This serves as confirmation that different hacking groups around the world are learning from one another, comparing notes, and developing an increasingly robust set of best practices. All this makes it increasingly more difficult to effectively defend against such threats. Stay vigilant and be sure to remind your employees never to open emails or click links inside emails, even if they appear to be from a trusted source.