2023 ANNUAL THREAT REPORT

As we enter 2023, it is critical for financial institutions (FI) to have a proactive strategy in place for detection, response, recovery, and resilience. Having a cohesive plan with the right components can keep your FI threat ready and prepared to prevent and mitigate an inevitable cyber attack. By implementing the right instrumentation on vital networks combined with expert security and powerful intelligence to hunt for threats, your FI can establish the upper hand in the fight against cyber crime. **From an initial threat perspective for 2023, it's the big THREE: 1. social engineering 2. vulnerability & configuration management 3. credential harvesting.**

Social engineering is a critical issue because it concerns your business's weakest link: humans. According to Security Today, in the article, *Just Why are So Many Cyber Breaches Due to Human Error*, "A joint study by Stanford University Professor, Jeff Hancock, and security firm, Tessian, has found that a whopping 88 percent of data breach incidents are caused by employee mistakes. Similar research by IBM Security puts the number at 95 percent." Cyber criminals have become savvier in their attempts to breach your infrastructure to gain access to sensitive data and assets. It is essential to take proactive measures and educate people about the potential threats. Developing a strong human firewall requires arming individuals with knowledge of malicious emails and other security risks as well as teaching strategies on how they can effectively defend their data. All employees need to understand that they play an important role in creating an effective security program that protects not only themselves, but their coworkers, the customers, and all aspects of your business.

Nurturing a community of trust amongst employees and customers by sharing important information about emerging alerts and threats is one effective way to build knowledge. The "see something, say something" mentality is a productive mindset to combat threats and ultimately builds a culture of peer-to-peer sharing. Additionally, providing continuous training to identify questionable communications, suspicious links, and other possible threats keeps your employees alert and aware. One way we can do this is with phish simulations, using real examples of malicious attempts for educational purposes. Employees are sent a practice phishing email to allow employees an opportunity to identify and report it. These exercises don't have to be limited to phishing - phone calls, sketchy behavior by individuals, unusual texts - really, anything suspicious should be on your employee's radar.

Vulnerability & configuration management are key components for reinforcing your systems against cyber attacks. As technology continues to advance, malicious actors slip undetected into your system by exploiting vulnerabilities and misconfigurations. Evaluating exactly what you have facing the internet and how you are monitoring it is a crucial step in hardening the external infrastructure.

Regular monitoring for vulnerabilities and scanning for misconfigurations helps identify gaps in your defenses. With that information you can prioritize exactly what vulnerabilities need to be addressed. Scanning and change control procedures can be reviewed and validated to avoid egregious errors. Because many financial institutions don't have the manpower to update, maintain, or upgrade these on a regular basis, it is recommended FI's move them to the cloud. While there is hesitation because they are essentially surrendering their ability to regulate it, realistically, a cloud provider can provide improved and optimal protective services in comparison to a smaller business who cannot keep up with the demands. Firewalls, edge routers or an exchange server infrastructure should all be considered when deciding which platform. Ultimately, the right one will streamline the configuration process.

Credential Harvesting is an equally devastating attack on your infrastructure. Cyber criminals exploit vulnerabilities in your defenses through social engineering and other attacks and amass databases of usernames and passwords. When that weakest link we discussed above breaks the cardinal rule to NOT reuse username and passwords across different sites, bad actors take advantage of that error. The stolen usernames and passwords are then used to access platforms and sites that use the same login credentials. Once they've breached your system, your sensitive data and assets are compromised. Consider this: an employee uses the same username and password for their personal and work accounts. They fell victim to an attack and like a disease, the cyber criminals reach has quickly spread and infiltrated your employee's personal accounts and now your company's, which consequently puts your client's data and assets at risk as well.

Best practices to prevent these types of attacks begins with quality instrumentation. It's important to use an Endpoint Detection and Response (EDR) that actually functions efficiently with solid logging and strong security operations support to analyze the alerts that come out of these systems. Implementing technology that is specifically designed for the unique challenges and threats that banks and credit unions encounter daily provides more efficient cyber risk management. The promise of Artificial Intelligence (AI) and Machine Learning (ML) alone has not been able to match the value of a highly trained SO engineer that understands the threats and Indicators of Compromise (IOC) that are presented and how to deal with them. It is the combination of both working in concert that bolsters your protection. Implementing a co-managed approach to your risk management program allows for your FI to remain a part of the process and have a first line of defense to assist in threat detection.

This partnership is beneficial because as your outsourced (Security Operations Center) SOC is identifying vulnerabilities and preventing threats from becoming attacks, your internal team can focus on response, recovery, and resilience to reduce the impact of one.

Resilience is of utmost importance because no matter how much you prepare and proactively plan, it's not a matter of IF a cyber attack will happen - it's WHEN. Nation state actors and cybercriminals have one goal in mind - to infiltrate your system for malicious purposes. They are working to destroy your infrastructure, steal your data, collect a ransom, or simply acquire bragging rights. Is your team prepared in the event of an actual breach? Establishing an effective Incident Response (IR) program is paramount to your response, recovery, and resilience. Table Top simulations are an excellent way to practice incident response so your team stays threat ready. It allows you to see how your team responds to the breach, prevents it from spreading, and reduces the impact. These exercises give insight into your capabilities and deficiencies, which help determine where you need improvement.

Other steps to take are ensuring you have multiple, quality backups for data. Verify your ability to satisfy recovery point objectives and your Recovery Time Objective (RTO) so your business can continue to operate. Also, test the failover between your live and remote sites. Confirm that data loss doesn't occur during the switchover because the secondary site tends to be less capable. Additionally, analyze what the degraded capability would be so your team is cognizant of it.

Entering the new year, FIs must stay alert and proactive in the face of cyber attacks. It's time to evaluate your cyber risk management plan and implement a combination of powerful technology and monitoring support from industry-specific experts. Employ an ally to create a strong, proactive approach for prevention, detection, and response to effectively safeguard your FI. Remember that preparation and awareness is crucial to cybersecurity, so train your employees - all of them. Cyber criminals are only getting zealously more brazen, but if we evolve our security practices with equal fervor, we will prevail.

Bob Thibodeaux
Chief Information Security Officer

Bob has more than 25 years of experience as a senior security expert and highly accomplished IT executive and engineer. Through leadership positions managing IT departments and programs, technology operations and data center operations, Bob has driven innovative process improvements, disaster recovery programs, information security strategies, and audit and compliance improvements. He has been responsible for incident response, risk management and penetration testing for community-focused banks, credit unions and high-tech companies across the United States. Bob is a Certified Information Systems Security Professional, Digital Forensics Examiner and GIAC Penetration Tester. Bob holds a degree in Business and Management from the University of Maryland and is a retired USAF Senior Master Sergeant.

Elizabeth Houser
Director of Cyber Defense

Elizabeth Houser is the Director of Cyber Defense for DefenseStorm and has engaged in roles ranging from security engineer and SOC manager to her current responsibilities for social engineering, vulnerability management, and tabletop services. Prior to joining DefenseStorm, Elizabeth volunteered at King County Sheriff's Office Major Crimes Unit while completing her degree in Information Security and Digital Forensics, being awarded Volunteer of the Year for her service. In addition to earning the CISSP, Elizabeth's certifications include the CISA, CISM, CRISC and CGEIT from ISACA as well as a Master of Library Information Science degree from the University of Washington and an MS in Entomology from the University of Tennessee. Elizabeth currently serves on the Computer Information Systems advisory board for Edmonds College

DefenseStorm ensures cyber risk readiness with a comprehensive system, including cyber security, compliance, and fraud. The only system specifically built for banking, it accounts for all the daunting challenges, regulations, and technology requirements you face as a financial institution. Our intelligent data engine, GRID, delivers real-time access, analysis, and action on all your critical threat data. Our Threat Ready Active Compliance (TRAC) team enables co-managed support 24x7x365, providing the support and expertise you need. Together, we will help you get ahead of the storm of threats.