CreditUnionTimes

Cyber Risk: The Need to Keep Up as Digital Services Take Off

The future emphasis of cybersecurity must shift from catching the thief to preventing the theft.

By Scott Woepke | August 04, 2023 at 09:00 AM

Fast, roaming internet and smartphone growth has connected people from all over the world, making communication simple and affordable. These developments have made an irreversible imprint on financial services providing instantaneous global connectivity. While online interactions with credit unions have become easier and more convenient for members, they have also made things easier for cyber criminals.

Watch Out for the Bad Actors

A few words of caution: As technology transforms financial services, the criminals are following these developments. Today's most concerning financial crimes are committed by sophisticated cyber criminals who possess technical capabilities that can easily exploit the vulnerabilities in the financial system. They are also attracted to the low-risk, high-reward proposition that exists in their pursuit of valuable assets such as money and personal data. As a result, the entire financial services industry continues to be a prime target for cyberattacks. This includes banks,

credit unions and the entire ecosystem of technology providers supporting the financial ecosystem.

Financial Services Attack Vectors

As the digital transformation of financial services continues, we need to carefully weigh the benefits and risks of the changes taking place. There is no doubt the financial industry will see an acceleration of improvements being made to digital capabilities, but we must keep up with efforts to protect the industry from disruption. Attackers have access to advanced hacking tools, techniques and malware, enabling them to exploit vulnerabilities and breach defenses with precision. They can deploy tactics such as social engineering, phishing and zero-day exploits to gain unauthorized access or manipulate systems. Here are a few areas that represent attack surfaces for the cyber criminals that require attention:

1. Critical infrastructure is at risk. Systems that support clearing, settling or recording of payments, securities, derivatives and other important financial transactions are a target given their systemic importance. In one high profile incident in 2016, the SWIFT network experienced an attack of 35 fraudulent instructions illegally transferring close to $1 billion from the Federal Reserve Bank of New York account belonging to the Central Bank of Bangladesh. Most of the funds were secured; however, a fraudulent transfer of $101 million did take place.

In another case in 2020, the New Zealand Stock Exchange experienced a four day disruption as a result of a foreign distributed-denial-of-service (DDoS) attack. For credit unions, these critical infrastructure risks must be addressed to ensure uninterrupted service and member satisfaction.

2. Today, we have a payments revolution taking place supporting real-time payments for person-to-person, business-to-consumer and business-to-business payments. An unintended consequence of these payment advancements is fraud. Faster payments creates faster fraud. The payments industry is on alert about a rise in cybersecurity incidents. As the popularity of these new payment services grows, so does the criminal activity that attempts to breach networks and scam credit union members. Steps must be taken to ensure the security and safety of these systems to promote trust in these new payment services that credit union members are adopting. Advancements in cybersecurity technology provides protection that provides new strength and resilience with digital security.

3. As more systems and devices are connected and depend on computer software to function, the attack surface expands across a credit union’s supply chain. Credit unions commonly use third-party partners to deliver better services and functionality to members. The attack surface expands as a result of the numerous third-party relationships that exist and

enables cyber criminals' opportunities to access a credit union's network. Managing third-party risk is a significant concern and involves effective third-party and data governance and technical solutions that securely support the flow of personal and financial data.

Looking Ahead: The Importance of Network Security

Financial services technology will continue to advance, and so must the technology and processes needed to prevent cyberattacks. The ever-changing landscape of technology requires the ability to dynamically extend security and compliance across virtual and cloud-based business architectures. These new complexities introduce security blind spots and non-compliant devices into the environment. Dynamically ensuring controlled network access is a critical step to take, and it can be achieved without business interruption by leveraging the latest cybersecurity technologies.

Building a strong defense perimeter enables credit unions to take proactive measures in countering attacks. The strategy of deploying cybersecurity capabilities also needs a paradigm shift. The historical approach of identifying network breaches and then containing them needs to shift to a more proactive stance. The future emphasis of cybersecurity must shift from catching the thief to preventing the theft. This proactive and assertive approach to network protection is designed to prevent cyber criminals from ever entering your network. Not only does it provide greater protection, it eliminates the effort and costs associated with the remediation of cyberattacks.

By elevating our cyber defense through network protection, we can tilt the scales in favor of the defense and protect the valuable assets within the credit union industry.

Scott Woepke is the Chief Commercial Officer for QWERX, a Washington, D.C.-based cybersecurity software provider supporting financial institutions.