Cybersecurity in the Financial Sector

March 1, 2022

Cyber incidents have impacted many sectors of U.S. commercial life, and banks are not exempt. Developing and practicing an effective Cyber Incident Response Plan is a vital component of risk management for any business, and especially for a retail bank.

Norwich University Applied Research Institutes (NUARI) provides technologies and services that enhance organizational cyber incident response capabilities and critical infrastructure security. One very successful approach in the development and practice of cyber incident response plans is the use of wargame exercises facilitated by the DECIDE® Platform.

DECIDE® is a web-based tool that provides exercise participants with a carefully paced flow of information tailored to their roles within the organization, which allows them to recognize the business impacts of a cyberattack and to respond with actions that will limit the damage. DECIDE® is designed for distributed exercises in which participants can join from any convenient location, but it can also be effectively used when participants are brought together in a single location to enhance communication.

The DECIDE® Platform was developed with funding from the Department of Homeland Security and is a trusted cybersecurity exercise and training solution for the financial sector. Since its inception, DECIDE® has provided an unmatched experience in simulating an array of cyberthreats and incident scenarios to participants located around the world. This ability has been proven in a series of large-scale exercises, including three Quantum Dawn events sponsored by the Securities Industry and Financial Markets Association (SIFMA). These exercises convened international stakeholders from the largest financial organizations and major government institutions. DECIDE® has also been proven, time and again, in exercises for individual organizations.

Retail banks are vulnerable to cyberattacks in many ways. By the nature of their operations, retail banks must provide their customers with internet access to account details and transactions. The five biggest cyber threats for financial services in 2022 are:

- Distributed Denial of Service (DDoS) attacks where the bank's server is overloaded by spurious traffic blocking legitimate transactions.
- Phishing attacks, a variant of social engineering, trick users into divulging credentials to gain access to bank accounts or internal networks.

nuariinfo@norwich.edu
nuari.org
P.O. Box 30
Northfield, VT 05663
+802.485.2213

- Ransomware attacks use extortion to pressure organizations into paying a ransom and are effective against financial services due to the heavy regulations which require exceptional cyber and data breach resilience.
- Supply chain attacks make it possible for cyber attackers to circumvent a bank's security controls by accessing resources through a third-party vendor where a single compromise could impact hundreds of companies.

Much greater damage can occur if an attacker gains access to the internal servers that manage accounts and process payments. In a process called "spear-phishing", the attacker conducts research against targeted individuals who have access to the bank's internal system, and uses the information gained to send emails that appear innocent, even familiar, but provide access to install malware when the employee downloads an attachment or clicks a link. Even well-trained employees may fall victim to this scam when distracted by competing demands during periods of stress and pressure.

Once the malware is installed, criminals are able to monitor the institution's network and record keystrokes to obtain even more sensitive employee login credentials. With this enhanced access and the knowledge gained of the bank's data exchanges, the criminals are able to initiate a wide range of actions designed to steal from the bank's customers and the bank itself. Recorded cases include:

- ATM fraud against transactions at other banks
- ACH funds transfers or SWIFT message redirection to transfer money from customer accounts to accounts controlled by the criminal
- Fraudulent credit or debit card charges.

Exercises on the DECIDE® Platform allow your team to practice the decisions and actions needed to contain the damage to your bank's reputation and the bottom line.

nuariinfo@norwich.edu
nuari.org
P.O. Box 30
Northfield, VT 05663
+802.485.2213