NCUA
National Credit Union Administration

Office of Examination and Insurance
Office of Business Innovation

Cybersecurity Update

October 2022

Cybersecurity Threat Landscape

- Cybersecurity remains a significant risk
- Geopolitical issues continue to influence cyber risks
- Credit union risk exposure changes frequently
- Risk management needs to be continuous to protect against evolving cyber threats
- Specific cyber threats
  - Ransomware & Cloud Migration
  - Evolving DDOS Attack Vectors
  - Cryptocurrency/Decentralized Finance (De-Fi) Risks
- Cyber hygiene & the basics

Ransomware & Cloud Migration

- Remains a considerable threat
- Credit unions should use penetration testing to confirm defenses and security against threats
- Prevention Best Practices
  - Enforce multi-factor authentication
  - Store any relevant secrets and keys offline
  - Create redundant backups
  - Encrypt backup data in transit and at rest
  - Store backups offsite and offline

Resource: CISA

CISA.gov/stopransomware

Evolution of DDoS Tactics and Techniques

- Shift to targeting small and medium size businesses
- DDoS tactics and techniques evolved
  - DDoS extortion
  - Application assaults
  - Attacks targeting internet-facing infrastructure
- Credit unions need to:
  - Maintain cyber security preparedness
  - Monitor internet traffic and firewall security
  - Be prepared to mitigate an attack if it happens

Decentralized Finance (De-Fi)

- Use outlined in Letter to Credit Unions
  - 22-CU-07 - Federally Insured Credit Union Use of Distributed Ledger Technologies
- Technology being exploited by bad actors
  - Blockchain savvy hackers motivated by financial gain
  - Exploiting internet and application protocol weaknesses along with security and authentication weaknesses
- Credit unions considering these and other emerging technology should:
  - Perform thorough third-party due diligence and conduct risk assessments
  - Ensure De-Fi platform addresses security, authentication, and other risks

Cyber Hygiene

- Goal – keep sensitive data secure and protect it from theft or attack
- Benefits – minimize risk of operational interruption, data compromise, and data loss
- Common challenges
  - Breadth/complexity of IT environments
  - Monotony
  - User buy-in

Best practices include:

- Single sign-on
- Endpoint protection
- Patch management
- Ongoing user education and security awareness training
- Encryption
- Backups
- Firewalls
- Password hygiene
- Muti-factor authentication (MFA)

Cyber Incident Notification

- Law requires CISA to implement regulations with established reporting framework
  - 72 hours – report major cyber attack
  - 24 hours – report ransomware attacks
- NCUA issued a proposed cyber incident reporting rule in July 2022
  - Notify NCUA no later than 72 hours after forming a "reasonable belief" an incident occurred
  - Structured to align with CISA reporting
  - Comment period ended September 26, 2022
- DHS Cyber Incident Reporting Council – government and regulatory agencies collaborating to create harmonized reporting structure

Updates to ISE Program

- Pilot testing completed September 30, 2022
- Program is scalable for credit unions of all sizes and complexity
- New ISE program aligns with ACET toolbox – means no surprises for credit unions
- New ISE planned for deployment by end of Q4 2022

Partner & Engagement

- Raise awareness of cybersecurity risk to credit union industry by
  - Supporting outreach events
  - Providing training and speaking at events and roundtables
  - Providing assessment tools and other resources on the NCUA's Cybersecurity Resources webpage
  - Publishing Cyber Alerts and Notifications to credit unions
  - Participating in industry tabletop exercises to test cyber preparedness
- CISA hosting discussions on potential risks of Post Quantum Cryptography – credit unions invited to participate
  - https://www.cisa.gov/quantum

Cybersecurity Awareness Month

- See Yourself in Cyber!
- Focus on key action steps
  - Enabling multifactor authentication
  - Using strong passwords
  - Recognizing and reporting phishing
- Industry Webinar - Ransomware in the Financial Sector
- People, systems and controls
- Shields Up!

Office Contact Page

Office of Examination and Insurance

eimail@ncua.gov

(703) 518-6360

Office of Business Innovation

bimail@ncua.gov