NCUA
National Credit Union Administration

Office of Examination and Insurance

Cybersecurity Update

April 2023

Overview

Key Threats to the Credit Union Ecosystem & Financial Sector

1. Ransomware & Extortion Operations
2. Social Engineering & OpenAI Platforms
3. External-Facing Application Vulnerabilities
4. Misconfigurations in Cloud Environments
5. Distributed Denial of Service Attacks
6. Geopolitical Issues

Overview

NCUA Cybersecurity Policy & Programs

- NCUA Information Security Exam Program
- White House National Cybersecurity Strategy
- Partnership & Engagement
- NCUA Cybersecurity Resources

Ransomware & Extortion Operations

- Cybercriminals Earned Less Money on Ransomware Attacks in 2022
  - Increased Law Enforcement Activity
  - Government Sanctions & Advisories
  - Prioritization of Ransomware Investigations
- Extortion Operations in 2023 more prevalent
  - Threatens to release data publicly
  - Less risky to adversary than ransomware
- Measures to protect
  - Segmenting networks
  - Implementing tighter access controls
  - Backups (protects from ransomware only)
- Ransomware/Extortion significant in coming years

Resource: CISA

CISA.gov/stopransomware

Social Engineering & OpenAI Platforms

- Remains a considerable threat
- Threat Actors traditionally use:
  - Spear Phishing
  - False Job Offers
  - Fake Credit Union & Banking Websites
- Threat Actors Now Leveraging Artificial Intelligence
  - Generate Malicious Content
  - Creating Personalized Phishing Emails
  - Improving Malware Source Code
  - Phone Verification to Authenticate
- Mitigate using AI Cybersecurity Products - $139B (CY2030)

Resource: Trend Micro

Trend Micro. (2020). The State of Cybersecurity and Digital Trust 2020.

Externally Facing App Vulnerabilities

- External facing applications exposed to unauthorized access threats
- Impacts
  - Online Banking Portals
  - Mobile Banking Apps
  - Payment Systems
- Mitigation best practices
  - Regularly conducting vulnerability assessments and penetration tests
  - Implementing Multi-Factor Authentication for sensitive data access
  - Ensuring software applications are updated
  - Implementing strong passwords

Misconfigurations - Cloud Environment

- Misconfigurations can lead to:
  - Data Breaches
  - Theft and Exploitation
  - Fines for Non-Compliance
- High Profile Breaches
- Credit unions should implement these best practices
  - Ensure training and expertise to securely and properly configure
  - Regularly audit and monitor cloud infrastructure
  - Implement proper access controls

Resource
Dataconomy. (2022, May 16). 16 Dangerous Cloud Computing Vulnerabilities, Concerns, and Threats.

Distributed Denial of Service Attacks

- Pose a serious threat to Credit Unions
- Typically carried out by botnets
- May be used as a smokescreen for stealing data and installing malware, among other things
- Prevention best practices
  - Strong and well-tested response plan
  - Implement redundancy and failover mechanisms
  - Providing employee education & training

Geopolitical Issues

- Russia – a Top Risk
- Other Issues impacting the geopolitical environment
  - Inflation Risks
  - Iran
  - Energy Crunch
- Recent Advances in AI – Larger Challenges

Resource:
Eurasia Group. (2023). Top risks 2023. Retrieved February 12, 2023

Updates to ISE Program

- ISE Officially Deployed
- Three Types of Exam Level Statements
  - SCUEP
  - Core
  - Core+
- Facilitates Tailored Examinations (Asset Size & Complexity)

National Cybersecurity Strategy

- Focus on regulation could spur innovation
- Emphasis on public-private partnerships
- Significant shift in governmental approach to cybersecurity

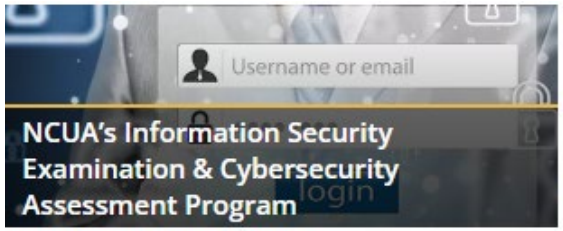
Partner & Engagement

- 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

NCUA's Cybersecurity Resources

Cybersecurity Resources

- NCUA's Information Security Examination and Cybersecurity Assessment Program
- ACET and Other Assessment Tools
- Supply Chain Risk Management (SCRM)
- Catastrophic and Incident Reporting
- NCUA's Regulations and Guidance
- References & Resources



QUESTIONS

Office Contact Page

Office of Examination and Insurance

eimail@ncua.gov

(703) 518-6360