InfoSight Newsletter

July 19 2024 | Volume 18 | Issue 27

League InfoSight Highlight

Cyber Incidents – Ransomware and Data Breaches

Recent ransomware attacks have been making headlines and raising concerns for credit unions. Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. The Cybersecurity Infrastructure Security Agency (CISA) highlighted that in recent years ransomware incidents have become increasingly prevalent among the Nation's state, local, tribal government entities, and credit infrastructure organizations such as credit unions.

Ransomware follows similar patterns, starting with the initial compromise of the system. Some of the most common infection points are:

- Phishing emails with corrupt attachments or links;
- Weak remote desktop protocols;
- Unpatched systems;
- Extensive reuse of passwords; and
- Lack of multi-factor authentication.

Users often open a corrupt attachment or link which unknowingly installs the malware on their computer. The hacker then will explore the networks looking for vulnerabilities and sensitive data, which often goes undetected. Once they have access, the ransomware will spread through the network and then encrypt material. After which, the hackers will make their ransom demand in exchange for a decryption key.

CISA provides suggestions which may help protect credit unions' networks.

1. **Backups:** Do we backup all critical information? Are the backups stored offline? Have we tested our ability to revert to backups during an incident?

2. **Risk Analysis:** Have we conducted a cybersecurity risk analysis of the organization?
3. **Staff Training:** Have we trained staff on cybersecurity best practices?
4. **Vulnerability Patching:** Have we implemented appropriate patching of known system vulnerabilities?
5. **Application Whitelisting:** Do we allow only approved programs to run on our networks?
6. **Incident Response:** Do we have an incident response plan, and have we exercised it?
7. **Business Continuity:** Are we able to sustain business operations without access to certain systems? For how long? Have we tested this?
8. **Penetration Testing:** Have we attempted to hack into our own systems to test the security of our systems and our ability to defend against attacks?

TruStage shared steps credit unions should take to manage a ransomware incident, which include:

- Do not restore data until images can be collected by the digital forensics team.
- Do a global password reset.
- Disconnect from back-ups.
- Disconnect from the internet.
- Check to see if there are any malicious inbox rules.
- Obtain the ransom demand to share with the legal and forensics vendors.
- Contact your insurance carrier immediately to report an incident.

Cyber Incident Reporting

The NCUA has the **Cyber Incident Notification Requirements rule** which states that NCUA must receive notification as soon as possible but no later than 72 hours after a credit union reasonably believes that it has experienced a reportable cyber incident. A reportable cyber incident is any substantial cyber incident that leads to one or more of the following:

1. A substantial loss of confidentially, integrity, or availability of a network or member information system that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services or has serious impact on the safety and resiliency of operational systems and processes;
2. A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities; or
3. A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of a credit union

service organization, cloud servicer provider, or other third-party data hosting provider or by a supply chain compromise.

In addition, CISA recommends contacting law enforcement immediately. They encourage contacting a local FBI or Secret Service field office to report a ransomware event and request assistance.
https://www.fbi.gov/contact-us/field-offices
https://www.secretservice.gov/contact

Resources
InfoSight -

- Cybersecurity

- Data Breach
  - Member Notification and Content Notice
  - Media Response Components
  - State Considerations

- Security Program for Credit Unions
  - NCUA Notification Requirements
  - Information Security Program Requirements

CU PolicyPro

- Policy 4120 – Information Security
- Policy 4125 – Incident Response

RecoveryPro

- Section 1600: Cyber Incident Response Process
  - Procedures for detecting, containing, and recovering from Cyber Attacks
  - Cyber Incident Reporting
  - Member Notifications and Communications Templates
  - Cyber Incident Planning Recommendations
  - Cyber Event - Threat Assessment

CISA Ransomware Guide
CISA How to Protect Your Networks from Ransomware
NCUA Cybersecurity Resources
NCUA - Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice

David Curtis

Director, Compliance Services, GoWest Credit Union Association

LIS Webinar: Cyber Incident Content Review

Join us on **Tuesday, July 30, 2024 at 2pm ET** for our upcoming webinar where we will dive into the latest content updates for RecoveryPro! New content includes procedures for detecting, containing, and recovering from cyberattacks, along with communication strategies for notifying key stakeholders. You do not need to be a RecoveryPro client to attend!

Register now to reserve your spot!

News and Alerts!

OFAC Basics Video Series - My Funds are Blocked, Now What?

The Department of the Treasury's Office of Foreign Assets Control (OFAC) is releasing the second video in its “OFAC Basics” video series, **"My Funds Are Blocked, Now What?"** This video provides viewers with guidance on what it means when funds are blocked in connection with OFAC sanctions, as well as recommended steps for what to do if your funds have been blocked.

Read More

NCUA: FFIEC Publishes 2023 Data on Mortgage Lending

The Federal Financial Institutions Examination Council (FFIEC) published data on 2023 mortgage lending transactions reported under the Home Mortgage Disclosure Act (HMDA) by 5,113 U.S. financial institutions, including banks, savings associations, credit unions, and mortgage companies.

Read More

NCUA: Agencies Issue Final Rule to Help Ensure Credibility and Integrity of Automated Valuation Models

Six federal regulatory agencies issued a final rule pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act, designed to help ensure the

credibility and integrity of models used in valuations for certain mortgages secured by a consumer's principal dwelling. In particular, the rule will implement quality control standards for automated valuation models (AVMs) used by mortgage originators and secondary market issuers in valuing those homes. The final rule is substantially similar to **the proposal issued in June 2023**.

Read More

CFPB Blog: How to recover financially after Hurricane Beryl

In early July, Hurricane Beryl hit the coast of Texas, causing extensive damage and flooding before bringing extreme weather into other parts of the country. The Federal Emergency Management Agency (FEMA) urges Texans and other affected residents to take care when you are outside assessing damage to your property from the storm, and to find a community cooling center if your home doesn't have air conditioning. Once you are physically safe, there are steps you can take to help ensure your finances are secure.

Read More

Questions, Comments, Concerns? We are here to help! Email us at **info@leagueinfosight.com**