Tabletop Exercise #4

Cyber Incidents: Phishing and Malware

Working in K-12 schools can bring with it a bevy of challenges. Effective emergency planning can help your team operate efficiently no matter what happens throughout the year. Tabletop Exercises help you ensure healthy operations by bringing together key stakeholders to test your emergency management plans. CSDSIP is back with another scenario-based tabletop exercise based on real life incidents to test your school's emergency response skills. Each exercise is intended to improve your team's critical thinking abilities in realistic scenarios, help coordinate the right people to assist in an emergency and provide knowledge and tools to build confidence handling emergency scenarios.

Tabletop Exercise 4

A nefarious enterprise launches a phishing and malware attack in your community, leading to encrypted files and huge headaches. What are your next steps?

When: June, Thursday evening

Where: Administrative office

Scenario 1 | Phishing Incident: After receiving several angry phone calls following payday, business office staff discovered that multiple district employees had fallen victim to a phishing scheme that redirected their direct deposit paychecks.
Several weeks earlier, an email was sent out to all district employee email addresses directing employees to click on a link to update their payroll passwords or they would lose access to their accounts. The email used the district's logo and appeared to come from the IT department. Multiple employees clicked the link in the email and changed their passwords.
Unfortunately, this email was a phishing scheme that tricks employees into clicking on a link that prompts them to enter their password, update their account information, or resetting a password about to expire. In many cases, both the initial email and the website the link leads to are designed to look legitimate. Once the cybercriminals have the employee's real password, they login to the self-serve portal and change the employees direct deposit account to one they have access to. Many employees only learn that they were tricked once their paychecks fail to show up in their accounts on the next payday. What are your next steps?

Scenario 2 | Ransomware Incident: At around 4:00 PM the special education director's laptop suddenly displays a message that states all files have been encrypted and demands payment in exchange for the decryption key. The message states that the ransom, currently $5,000, will double to $10,000 if payment is not sent in bitcoin in the next 48 hours. If you refuse to send payment after 96 hours all the encrypted files will be deleted and therefore become completely unrecoverable. The laptop contains evaluation and progress monitoring data on numerous students as well as the evaluations of several employees. How would you proceed?

Critical Thinking:

1. What current policies and procedures are necessary in this scenario?
    a. Was the response adequate to the magnitude of the incident?
2. Are all staff trained on who to report to in a similar scenario?
3. Can one or more operational changes be made to mitigate the risk or damage in the future?
4. What lessons can be learned from this scenario?

Recommendations

Cyber Incidents Exercise

Recommendations:

Before the attack:

- Have established safety protocols.
- Train all employees on the cyber safety protocols and best practices.
- Be aware. If you are unsure who an email is from, do not respond!
- Double check before you act. Reach out to the sender in person or by telephone to verify the legitimacy of the email if personal information is being requested.
- Protect your personal information. Social engineering can use publicly available information to try to manipulate you into skipping normal security protocols.
- When possible, double your login protection. Enable multi-factor authentication to ensure that the only person who has access to your account is you.
- Shake up your passwords! Use complex passwords and avoid reusing passwords between websites.
- Ensure servers, personal devices, and network appliances are kept up to date with software patches and security updates. Use anti-virus software.
- Ensure that critical systems are regularly backed up.
- Restrict users to the lowest level of access necessary to perform their tasks.

During the attack:

- Contact CSDSIP immediately upon discovery of any cyber breach. Failing to immediately contact CSDSIP can result in diminished coverage.
    - A data breach coach will be in contact to walk you through next steps.

After the attack:

- Retrain employees on safety protocols and best practices.
- Review technological firewalls to ensure optimum protection.
- Revise and implement policies to prevent future cyber incidents.

Resources

Cyber Incidents Exercise

Resources:

Watch CSDSIP's Cyber Deception and Data Protection training here.

The K-12 Cybersecurity Resource Center

REMS Cyber Security Considerations for K-12 and School Districts

CoSN Cyber Security Tools and Resources

NIST Standards, Guideline & Best Practices

Stop Ransomware

The list below outlines the government organizations that you can file a complaint with if you are a victim of cybercrime.

- **US-CERT.gov**
  Report computer or network vulnerabilities to US-CERT via the hotline: 1-888-282-0870 or www.us-cert.gov.
- IC3.gov
  File a complaint with the Internet Crime Compliant Center (IC3), a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C), at www.IC3.gov.
- FTC.gov
  If you think your computer or mobile device has been infected with malware, report it to the Federal Trade Commission at www.ftc.gov/complaint.
- SSA.gov
  If you believe someone is using your Social Security number, contact the Social Security Administration's (SSA) fraud hotline at 1-800-269-0271. For additional resources, visit the SSA at http://oig.ssa.gov/report-fraud-waste-or-abuse.

Conclusion: Cybercrimes can be devastating to any district and recovery can be difficult. Having an effective plan in place can drastically change the outcome of a situation. Please reach out to CSDSIP to talk through this tabletop exercise or to answer any questions that may arise out of the completing this exercise.

Join us next time for another tabletop exercise.