COMPLIANCE SPOTLIGHT

Volume 2 / Issue 2 June 2023

DID YOU KNOW…

Currently, ransomware attacks are estimated to occur every 19 seconds. Statistics show ransomware attacks will occur every 2 seconds by 2031.

COMPLIANCE REMINDER

NCUA Cyber Incident Reporting Requirements take effect September 1st, 2023. Ensure your Incident Response Plans are updated accordingly.

Contact Us

Buckley Technology Group
P.O. Box 530, Norwell, MA 02061
(800) 355-4550
sales@buckleytechgroup.com

www.buckleytechgroup.com

RANSOMWARE ATTACKS: THE BASICS

Although ransomware attacks have been getting increased attention within the last few years, hackers have used extortion attempts for financial gain and political motives for quite some time. In fact, ransomware attacks have been a critical cybersecurity threat for over three decades. The first documented ransomware attack, known as the PC Cyborg virus or AIDS Trojan, occurred in 1989 using floppy disks.

Today's cyber climate and global events warrant the need to implement evolving and sophisticated mitigation steps to counteract ransomware attacks. Before cybersecurity practices can be matured, it is best to revisit the basics in ransomware risk management and response:

1. How does a ransomware attack work?

   A computer is first infected by the malware, which can result from a phishing email or malicious attachment. Next, the computer and its files are encrypted and inaccessible to the victim. Followed by extortion, in which payment is demanded to decrypt the system or threats are made to destroy and/or release the data.

2. What are signs of a ransomware infection?

   Pay attention if your network or computer is running unusually slow, or if there are files saved with odd names and extensions. Obvious signs include being locked out of your network or blocked from accessing files, with receipt of intimidating messages (i.e., click on a link to resolve the issue or you have a certain amount of time to pay a fine to regain access).

3. What are ransomware risk management essential controls?

   Backup your data offsite/offline. Ensure all systems have up-to-date patches and are running supported software. Put in place multi-layered security controls (i.e., antivirus, data leak protection, multifactor authentication, restricted access permissions, etc.). Test your Incident Response Plan through tabletop exercises, simulated phishing tests, and red team/blue team penetration testing.

4. What should I do if I fall victim to a ransomware attack?

   Isolate and power off the affected computer. Follow your Incident Response Plan. Escalate to the IT Department or IT Service Provider. Contact law enforcement. Check and secure offsite/offline data. Immediately change all passwords to critical systems. Engage with cyber forensics experts.

BTG provides managed Information Security & Cybersecurity services helping credit unions develop and test Incident Response Plans through Social Engineering Testing and Penetration Testing. Contact us for more information.

Elisabeth N. Esposito