WIPFLI

Cybersecurity Hot Topics: The Latest Trends
Webinar Questions
March 30, 2022

1. How, exactly, should backup air gapping be performed?
   a. *Through network segmentation. You should not be able to access your production network and your backup data from the same system. Ransomware gangs, after getting into your system, will target your backups. There are many solutions that allow you to take the backup offline to mitigate the risk of ransomware encrypting the backup.*

2. What about privileged access management similar to MFA?
   a. *Privileged access management (PAM) is a great complement to multi-factor authentication (MFA). MFA ensures you are who you say you are. PAM ensures you don't have more administrative privileges to the various systems than needed to perform your duties. (There is more to PAM, but that is beyond the scope of this presentation).*

3. Do you have example scenarios of tabletop testing?
   a. *There is an FDIC site that provides some great tabletop testing scenarios, and you don't have to be a financial institution to take advantage of these.*
   https://www.fdic.gov/regulations/resources/director/technical/cyber/purpose.html
   We recommend testing one or two of these scenarios at least annually.

4. Password Manager — which two would you recommend for a company?
   a. *There are many great password managers – Keeper, 1Password, and LastPass are just a few. We recommend if this is for your business, using an enterprise version. Also, many have trial versions, so you can find out what you like.*

5. As the U.S. government moves to be more secure by implementing NIST/CMMC, do you foresee financial institutions moving down this route? The Cyber Assessment Tool to me looks almost exactly like NIST 800-171.
   a. *We don't see banks being required to use a specific framework such as NIST, but they should understand what framework is used by those auditing and testing their IT controls. There are so many frameworks, and they each have their advantages. A framework that has been getting a lot of attention is the CIS Top 18 controls.*

6. Is there a way to easily determine if a QR code is a bad one?
   a. *You can't determine whether a QR code is a phishing scam just by looking at it. QR codes should be treated the same way as URL links in emails. We recommend using a known and trusted app or typing in the web address into the browser address bar rather than using a QR code when asked to enter personal information.*

7. Hypothetical question: A bad actor has created an impostor/fake website of a bank's website. The bank is pursuing takedown options via DMCA provisions, but the hosting company has yet to respond. What do you recommend the bank does to get the site taken down? What do regulators expect regarding actions banks should take in this type situation?
   a. *We are not familiar with DMCA, but thanks, we will research this. We recommend contacting the FBI and a vendor that is familiar with fraud and forensics. They have experience in these types of situations.*