Information Security for Every Technology User

Created to Satisfy HB 3834 for 2020

Course Objectives

1. Learners will understand the following terms in the context of information security:
    - information security
    - threat
    - threat actor(s)
    - risk
2. Learners will understand the types of information that need to be safeguarded online and in computer systems.
3. Learners will be aware of different forms in which that information might exist and different location in which it might be stored.
4. Learners will understand how to prevent the unauthorized access to information, information systems, and secure facilities.
5. Learners will understand how to prevent the unauthorized use of information and systems.
6. Learners will be aware of best practices for secure information storage.
7. Learners will be aware of best practices for securely deleting or otherwise disposing of information and information systems.
8. Learners will be aware of best practices for detecting, assessing, reporting and addressing threats to information security.
9. Learners will be able to describe indicators for common attacks.
10. Learners will understand how to respond to and report detected attacks or suspicious activity.

Modules

1. Introduction
    - Welcome
    - Orientation
    - Introductory Case Study
        - Allentown, PA
        - City of 121K. An employee took a laptop while traveling. While off the network, it missed crucial software updates. He clicked a link in a "phishing" email which installed the malware. On his return to the office, the malware sprea rapidly. No ransom was demanded, but the attack cost about $1 million to clean up and the city also adopted additional defensive measures that cost an additional $420,000 per year. The attack was traced to attackers in the Ukraine. [1]
2. Passwords Matter
    - How Passwords are Used and Stored
    - Common Attacks

- Brute-Force Attacks
- Dictionary Attacks
- Rainbow Tables
- Social Engineering
- Phishing
- Keylogging
- Shoulder Surfing
- Guessing
- Web spiders
- Reused passwords exposed in breaches

3. Choosing and Protecting Strong Passwords

Case Studies

Aug 18, 2019: 20+ Texas towns targeted in ransomware attacks. July 25, 2019: City Power, the electric utility for Johannesburg, South Africa, discloses ransomware attack. June 26, 2019: Lake City, Florida agrees to pay ransomware. June 20, 2019: Riviera Beach, Florida, discloses ransomware attack and payment. May 7, 2019: City of Baltimore hit with ransomware attack. April 2019: Cleveland Hopkins International Airport suffered a ransomware attack. April 2019: Augusta, Maine, suffered a highly targeted malware attack that froze the city's entire network and forced the city center to close. April 2019: Hackers stole roughly $498,000 from the city of Tallahassee. March 2019: Albany, New York, suffered a ransomware attack. March 2019: Jackson County, Georgia officials paid cybercriminals $400,000 after a cyberattack shut down the county's computer systems. March 2018: Atlanta, Georgia suffered a major ransomware attack. February 2018: Colorado Department of Transportation (CDOT) employee computers temporarily were shut down due to a SamSam ransomware virus cyberattack. [2]

Allentown, PA

City of 121K. An employee took a laptop while traveling. While off the network, it missed crucial software updates. He clicked a link in a "phishing" email which installed the malware. On his return to the office, the malware sprea rapidly. No ransom was demanded, but the attack cost about $1 million to clean up and the city also adopted additional defensive measures that cost an additional $420,000 per year. The attack was traced to attackers in the Ukraine. [1]

Kaufman, TX

One of the municipalities targeted in the Aug, 2019 attack on 24 Texas municipalities. Most details are being concealed, but the city was forced to conduct business manually instead of with computers and cellphones were used when the phone system was disabled. [1]

Wilmer, TX

One of the municipalities targeted in the Aug, 2019 attack on 24 Texas municipalities. Public library checking out books on paper. Police dept writing tickets by hand. Population 5000. [1]

Lake City, FL

Paid a ransom of about $460K, using cyberinsurance coverage. [1]

Baltimore, MD

Declined to play ransom of $76K -- incurred estimated costs of 18 million. [1]

Atlanta, GA

Declined to pay ransom of $51k -- estimated costs are $17 million. [1]

Central Platte Natural Resources District in Nebraska

Attackers disabled antivirus software, introduced ransomware that encrypted a key database, and demanded ransom. The district had protected themselves with a backup process that ran every 15 minutes and so declined to pay. [6]

References

1([1], [2], [3], [4], [5], [6], [7]) https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

2 https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/attack-list-cities-government-agencies

3 https://www.jdsupra.com/legalnews/ransomware-attacks-targeting-cities-and-60139/

4 https://www.wired.com/story/ransomware-hits-georgia-courts-municipal-attacks-spread/

5 https://www.cnbc.com/2019/08/22/texas-ransomware-attacks-tell-the-us-cybersecurity-story.html

https://www.scmagazine.com/home/security-news/ransomware/nebraska-irrigation-district-thwarts-ransomware-attack-with-auto

https://www.scmagazine.com/home/security-news/ransomware/survey-48-of-organizations-attacked-by-ransomware-over-12-m