Topic 5 Discussion 1

Research and describe 2-3 intrusions that have occurred in alternative environments (SCADA, real time systems, critical infrastructures). Explain how and why the intrusions occurred. What can organizations do to prevent such threats?

Hello Class,

Stuxnet (2010) - SCADA Systems

Overview:

Stuxnet is one of the most infamous cyberattacks targeting SCADA systems, specifically designed to disrupt Iran's nuclear program.

How and Why It Occurred:

Stuxnet was a sophisticated worm that exploited multiple zero-day vulnerabilities in Windows systems. It specifically targeted Siemens PLCs (Programmable Logic Controllers) used in industrial environments. The attack was believed to be a state-sponsored effort to sabotage Iran's nuclear capabilities without resorting to military action.

Prevention:

Isolate critical systems from general IT networks to limit exposure. Ensure all software and systems are up-to-date to mitigate vulnerabilities. Implement IDS tailored for industrial control systems to detect unusual activities.

Target Data Breach (2013) - Critical Infrastructure

Overview:

The Target data breach involved the compromise of credit and debit card information of millions of customers, impacting the retail sector's critical infrastructure.

How and Why It Occurred:

Attackers gained access through a third-party vendor's credentials, exploiting weak security practices. They installed malware on point-of-sale systems to capture card data. The goal was financial gain through the theft of sensitive customer information.

Prevention:

Strengthen security protocols for third-party vendors and conduct regular audits. Implement MFA for accessing sensitive systems to enhance security. Regularly train employees on cybersecurity best practices to recognize phishing attempts and other threats.

Ukrainian Power Grid Attack (2015) - Critical Infrastructure

Overview:

This cyberattack caused widespread power outages in Ukraine, affecting hundreds of thousands of residents.

How and Why It Occurred:

Attackers used spear-phishing emails to gain access to the network, followed by the deployment of malware that targeted SCADA systems controlling the power grid. The attack was politically motivated, aimed at destabilizing the region.

Prevention:

Implement strong password policies and regular system audits to identify vulnerabilities. Develop and regularly update incident response plans to ensure quick recovery from attacks. Establish backup systems and redundancy in critical infrastructure to maintain operations during an attack.

References:

Dong, Y., Wang, R., & He, J. (2019). Real-Time Network Intrusion Detection System Based on Deep Learning. *2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS)*. https://doi.org/10.1109/icsess47205.2019.9040718

Erickson, A. (2021, December 23). *14 Major SCADA Hacks*. Www.dpstele.com. https://www.dpstele.com/blog/major-scada-hacks.php

Kostadinov, D. (2020, April 28). *Intrusion Detection and Prevention for ICS/SCADA Environments | Infosec*. Www.infosecinstitute.com. https://www.infosecinstitute.com/resources/scada-ics-security/intrusion-detection-and-prevention-for-ics-scada-environments/

Maglaras, L. A., & Jiang, J. (2014). Intrusion detection in SCADA systems using machine learning techniques. *2014 Science and Information Conference*. https://doi.org/10.1109/sai.2014.6918252

*NEW: House Homeland Releases “Cyber Threat Snapshot” Highlighting Rising Threats to US Networks, Critical Infrastructure – Committee on Homeland Security*. (2024). House.gov. https://homeland.house.gov/2024/11/12/new-house-homeland-releases-cyber-threat-snapshot-highlighting-rising-threats-to-us-networks-critical-infrastructure/

Sheng, C., Yao, Y., Fu, Q., & Yang, W. (2021). A cyber-physical model for SCADA system and its intrusion detection. *Computer Networks*, *185*, 107677. https://doi.org/10.1016/j.comnet.2020.107677