Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

January 26, 2021
CS-02-2021

Security Control Frameworks

OVERVIEW:

Cybercriminals are more likely to target organizations/devices which they consider low hanging fruit, easy targets, or targets of opportunity. This means organizations with no policies or controls in place are typically first to become targets of cybercriminals. To help prevent your organization from becoming a target, there are several frameworks which can be followed. Even though the implementation of all controls may not be possible, the implementation of a select few can offer a low-cost high-reward plan which may elevate the cybersecurity posture enough to no longer be the primary target of malicious actors.

FRAMEWORKS:

Although there are multiple frameworks covering cybersecurity, two of the more well-known are the Center for Internet Security (CIS) Controls Framework and the National Institute of Standard Technology (NIST) Cybersecurity Framework.

The CIS framework focuses on twenty Critical Security Controls (CSC's), which are broken down into three different categories. These categories include basic controls, foundational controls, and organizational controls.

CIS Controls®

cissecurity.org

Basic controls focus on endpoint security such as using tools to identify devices on your network while maintaining a list of these devices and the software they use. These tools could be used to continuously monitor these devices, remove any unauthorized devices from your network, and ensure approved devices and software are up to date. This also includes ensuring administrative accounts are being properly used, security settings are up to date on all devices, and appropriate logging has been implemented.

Foundational controls mostly deal with network and data security, such as; using approved web-browsers with up to date anti-malware software, using only the necessary ports and protocols, maintaining regular backups which are kept off-line, and blocking any known malicious IP addresses. This also includes using tools to monitor for the unauthorized transfer of data, segmenting this data into different categories of classification, maintaining separate networks for personal vs. enterprise devices, and enabling two-factor authentication wherever possible.

Organizational controls are about checking your work to make your cybersecurity more effective. This involves training your workforce to identify social engineering and phishing emails. It also involves the use of penetration testing as a check sum to not only test the security measures put in place, but also to test incident response in the event of a compromise and to ensure best practices are being used.

The NIST cybersecurity framework is designed to be a performance based, flexible, cost-effective approach to cybersecurity. The NIST framework offers a five-step methodical approach to cybersecurity which is to identify, protect, detect, respond, and recover.

The first step is to identify and prioritize by understating what is critical to the business and your vulnerabilities. The second step is to protect yourself by developing and implementing safeguards. These can include data security, training for employees, identity management and access control, employing technology, and ensuring endpoints are up to date with the latest patches. The third step is detection by constantly monitoring your network for anomalies or cybersecurity events. Responding to events, which includes event analysis and mitigation, is the fourth step. A debriefing should also be conducted to discuss what improvements can be made. Communication is key to ensure everyone is on the same page. The final step is recovery, which includes making sure everything is back to normal and any identified improvements are implemented.

KEY TAKEAWAYS:

Although every organization has its own unique cybersecurity challenges, these frameworks are not one size fits all; instead, they are flexible to fit your organization's needs. This includes several controls which can be included with little to no cost, just time and effort. Even if only a few of the recommended measures are implemented, your cybersecurity exposure may rise above the level of becoming targeted by cybercriminals. This means a few low-cost solutions can have a huge return on investment.

CYBERSECURITY ASSESMENT RESOURCES:

CISSA - https://www.cisa.gov/cyber-hygiene-services
Michigan State Police – MC3 offers a free Cybersecurity Assessment. To request an assessment, send an email to MC3@michigan.gov.
MISecure Quick Self Audit - The MC3 collaborated with various groups to create the following document for schools, based off the CIS Controls, but it can be used for any organization. https://misecure.org/wp-content/uploads/2020/12/MiSecure-SelfAudit.pdf

FRAMEWORK RESOURCES:

CIS Controls to protect your organization and data from known cyber-attack vectors - https://www.cisecurity.org/controls/cis-controls-list/
NIST Cybersecurity Framework - https://www.nist.gov/cyberframework