MS-ISAC

MS-ISAC Security Primer

General Security Recommendations

March 2017, SP2017-0211

The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides the following general cyber security recommendations to assist state, local, tribal, and territorial (SLTT) governments in preparation, protection, and mitigation of malicious cyber activity.

RECOMMENDATIONS:

Securing Networks and Systems

- Know what is connected to and running on your network. Keep all hardware, operating systems, applications, antivirus software and signatures, content management systems (CMS), and essential software up-to-date to mitigate potential exploitation by malicious actors. This includes third-party applications and plugins. Monitor and take action on new information regarding vulnerabilities, exploits, and attacks
- Continuously conduct vulnerability scans of Internet-facing applications, focusing on identifying and remediating cross site scripting (XSS) and Structured Query Language (SQL) injection (SQLi) vulnerabilities. If a third party hosts the website, ensure that they do the same.
- Ensure that systems and both physical and wireless access points are hardened with industry-accepted guidelines, such as the CIS Security Benchmarks (http://cisecurity.org).
- Implement, monitor, and store logging for at least 90 days to identify unusual or unauthorized modifications and traffic, and to ensure that only authorized users are accessing resources.
- Perform regular backups of all systems to limit the impact of data loss and store the backups offline. Rebuilding or reimaging an infected system from a known good backup or fresh operating system installation is the only known way to guarantee removal of infections.
- Disable or remove software, ports, protocols, and services that are not in use.

Securing the End User

- Passwords should have at least ten characters and include uppercase and lowercase letters, numbers, and symbols. CIS recommends the use of at least 14 characters. Use different passwords for each account you access.
- Use multi-factor authentication consisting of something you know (password) and something you have (mobile phone, physical key, etc.), if it is offered.
- Adhere to the principle of least privilege, whereby a user and/or application only has the rights necessary to carry out their daily activities. If a user has no need for administrative access on a machine, they should not have an administrative account. This will help minimize the damage caused by malicious activity carried out under the user's credentials.
- Provide social engineering and phishing training to employees. Urge them not to open suspicious emails, not to click links contained in such emails, not to post sensitive information online, and to never provide usernames and/or passwords to any unsolicited request.

Responding to a Compromise or Attack

- Develop an incident response plan and ensure that it is always available.
- Establish and maintain effective partnerships with your upstream network service provider and know what assistance they may be able to provide you in the event of an attack.
- If your website is hosted by a third party, do the same with your hosting provider.

The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. More information about this topic, as well as 24x7 cybersecurity assistance for SLTT governments, is available at 866-787-4722, SOC@cisecurity.org, or https://msisac.cisecurity.org/. The MS-ISAC is interested in your comments - an anonymous feedback survey is available at: https://www.surveymonkey.com/r/MSISACProductEvaluation.