OCIO Cybersecurity for Elections

The current and emerging cybersecurity threats to state and local elections infrastructure has made the need for additional cyber defense protection necessary in order to maintain the accuracy and efficiency of the voting process.

In partnership with Iowa Secretary of State's office, the Office of the Chief Information Officer (OCIO) Information Security Division (ISD) has been utilizing cybersecurity tools funded by Iowa's Homeland Security Grant Program to improve the elections infrastructure cybersecurity posture.

Cybersecurity threats are constant. Ransomware, malware, and data breaches are not only very costly and interrupt day-to-day operations, they can also damage the public's trust and confidence. As Iowa's economy is becoming increasingly more reliant on technology, it's more important than ever to take action to secure computer networks and information systems.

Visiting websites infected with malware, opening attachments or following links in phishing emails, and not properly securing sensitive data are some of the ways that users can do harm to the network. Implementing security awareness training can help staff understand the threats and risks of cyber attacks and equip them with the knowledge they need to prevent malicious activity. The ISD has an online security awareness program available that covers these topics and more.

Controlling the infection, spread, and execution of malicious software is critical to protecting IT infrastructure. Malware can steal confidential data, compromise data and system integrity, and cause data and systems to be unaccessible or unavailable. The anti-malware service available from the ISD can help block these attacks and also allows for remote containment to limit the severity of an infection.

Monitoring for and alerting on suspicious network traffic can provide information on malicious content or malicious activity that could not otherwise be examined due to the sheer volume of information. This kind of visibility can be obtained using an intrusion detection system (IDS). An IDS is a vital part of a cyber defense strategy as it contains a database of known attack signatures and compares the network traffic against the database to detect and alert on potential attacks. An intrusion detection system (IDS) is also a cybersecurity service that is available from the ISD.

It is important to mention that the previously discussed cybersecurity tools are not intended to replace any safeguards that may already be in place, rather they can be used to supplement existing information security products such as a firewall or anti-virus.

The established partnerships and distribution of these cybersecurity tools will increase visibility and provide real-time alerting and remote containment of potential cyber attacks. Adding additional layers of protection will provide more support to the security and reliability of the elections infrastructure. We appreciate all of the time and attention that the counties have given to our cybersecurity effort and we look forward to continuing to work with you.

Please reach out to the OCIO Information Security Division for more information or assistance
jesse.martinez4@iowa.gov
https://iso.iowa.gov/