CTSI

TECHNICAL UPDATE

Volume 28 Number 23 | June 4, 2024

CYBERSECURITY CONTROLS: PART THREE

Cyber incidents—including data breaches, ransomware attacks, and social engineering scams—have become increasingly prevalent, impacting organizations of all sizes and industries. Such incidents have been mainly brought on by additional cyber threat vectors and growing attacker sophistication. As these incidents continue to rise in cost and frequency, counties must address their cyber exposures and bolster their digital security defenses.

CTSI presented a three-part series on essential cybersecurity controls. April focused on multifactor authentication, endpoint detection and response, and patch management. June highlighted email authentication technology, secure data backups, and incident response planning. Reviewing these risks and liabilities helps counties prevent cyber incidents and associated insurance claims from happening. It can also help secure adequate cyber coverage in the first place.

EMAIL AUTHENTICATION TECHNOLOGY/SENDER POLICY FRAMEWORK (SPF)

Many ransomware attacks start with employees receiving deceiving emails, such as those from fraudulent senders claiming to be trustworthy parties and providing malicious attachments or asking for sensitive information. It's paramount that organizations utilize email authentication technology to monitor incoming emails and determine the validity of these messages based on specific sender verification standards that organizations have in place. Organizations can choose from several different verification standards, but the most common is SPF—which focuses on verifying senders' IP addresses and domains.

Upon authenticating emails, this technology permits them to pass through organizations' IT infrastructures and into employees' inboxes. When emails can't be authenticated, they will either appear as flagged in employees' inboxes or blocked from reaching inboxes. With SPF, unauthenticated emails may even be filtered directly into employees' spam folders. Ultimately, email authentication technology can make all the difference in keeping dangerous emails out of employees' inboxes and putting a stop to cybercriminals' tactics before they can begin.

SECURE DATA BACKUPS

One of the best ways for organizations to protect their sensitive information and data from cybercriminals is by conducting frequent and secure backups. First and foremost, organizations should determine safe locations to store critical data, whether within cloud-based applications, on-site hard drives, or external data centers. From there, organizations should establish concrete schedules for backing up this information and outline data recovery procedures to ensure swift restoration amid possible cyber events.

INCIDENT RESPONSE PLANNING

Cyber incident response plans can help organizations establish protocols for detecting and containing digital threats, remaining operational, and mitigating losses in a timely manner amid cyber events. Successful incident response plans should outline potential attack scenarios, ways to identify signs of such scenarios, methods for maintaining or restoring key functions during these scenarios, and the individuals responsible for doing so.

These plans should be routinely reviewed through penetration testing and tabletop exercises, to ensure effectiveness and identify ongoing security gaps. Penetration testing refers to the simulation of attacks that target specific workplace technology or digital assets to analyze organizations' cybersecurity strengths and weaknesses. In contrast, tabletop exercises are drills that allow organizations to utilize mock scenarios to walk through and test the efficiency of their cyber incident response plans.

WHAT THIS MEANS FOR COUNTIES

CTSI recommends counties implement these essential cybersecurity controls to help manage their cyber exposures. Not only will it help safeguard and reduce digital vulnerabilities at the county level, but it will also assist in obtaining coverage with higher limits and lower premiums for CAPP. For more information, contact CTSI at (303) 861-0507.