CTSI
TECHNICAL UPDATE
Volume 28 Number 19 | May 7, 2024

CYBERSECURITY CONTROLS: PART TWO

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 largely been brought on by additional cyber threat vectors and growing attacker sophistication. As these incidents continue to rise in both cost and frequency, counties must take steps to address their cyber exposures and bolster their digital security defenses.

CTSI is presenting a three-part series on essential cybersecurity controls. April focused on multifactor authentication, endpoint detection and response, and patch management. June will highlight email authentication technology, secure data backups, and incident response planning. Taking the time to review 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.

NETWORK SEGMENTATION AND SEGREGATION

When organizations' networks lack sufficient access restrictions and are closely interconnected, cybercriminals can cause more widespread operational disruptions and damage. That's where network segmentation and segregation can help.

Network segmentation refers to dividing larger networks into smaller segments through the use of switches and routers, therefore permitting better monitoring and traffic control between segments. Segmentation may boost network performance and help localize technical issues and security threats. Segregation entails isolating crucial networks (i.e., those containing sensitive data and resources) from external networks, such as the internet. Segregation leverages additional security protocols and access restrictions within their most critical networks, making it difficult for cybercriminals to penetrate these networks laterally.

END-OF-LIFE (EOL) SOFTWARE MANAGEMENT

At some point, all software will reach the end of its life. This means manufacturers will discontinue technical support, upgrades, bug fixes, and security improvements. As a result, EOL software will have vulnerabilities that cybercriminals can easily exploit.

Organizations may be hesitant to transition away from EOL software for a number of reasons, such as limited resources or migration challenges. This is especially true when systems are still functioning. However, continuing to use EOL software also comes with risks, including heightened cybersecurity exposures, technology incompatibilities, reduced system performance, and additional data compliance concerns. Organizations should adopt life cycle management plans that outline ways to introduce new software, provide methods for phasing out unsupported software, and utilize device management tools to push software updates.

REMOTE DESK PROTOCOL (RDP) SAFEGUARDS

RDP consists of a digital interface that allows users to connect remotely to other servers or devices from any location. Through RDP ports, employees are permitted to retrieve files and applications stored on their organizations' networks while working outside the office, as well as giving IT departments the ability to identify and fix employees' technical problems remotely.

Unfortunately, RDP ports are also frequently leveraged as a vector for launching ransomware attacks, particularly when these ports are left exposed to the internet. In fact, nearly 1.3 million RDP-based cyber events occur each day, with RDP reigning as the top attack vector for ransomware incidents. To safeguard your RDP ports, it's important for organizations to keep these ports turned off whenever they aren't in use, ensure such ports aren't left open to the internet and promote overall interface security through the use of a virtual private connection (VPN).

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.

County Technical Services, Inc.
Technical Updates are available online at ctsi.org
800 Grant St., Suite 400, Denver, CO 80203
(303) 861-0507 | Fax: (303) 861-2832