Attacks/Breaches | 3 MIN READ | COMMENTARY

To Safeguard Critical Infrastructure, Go Back to Basics

CISA's recently released cybersecurity performance goals can help lower risk and thwart the impact of cyberattacks.


Bruce Matthews
Director, Cyber Programs, Maximus
February 24, 2023

Source: Andrii Yalanskyi via Alamy Stock Photo

The message is simple, but important: Cover the basics.

In its recently released cybersecurity performance goals, the Cybersecurity and Infrastructure Security Agency (CISA) stressed the importance of taking steps to maintain computer system health and improve online security. The goals are important reminders of risk in the sectors the agency defines as critical infrastructure, because cyberattacks can disrupt and even shut down services that impact daily life. This occurred in the energy sector when Colonial Pipeline was attacked, and in the utility sector with an attack on a dam in New York.

The agency's goals, designed to supplement the NIST Cybersecurity Framework, establish a common set of fundamental cybersecurity practices that lower risk and thwart the impact of cyberattacks on critical infrastructure organizations. For example, there must be an acceptable level of security for customers' accounts so that unsuccessful logins are detected, future attempts are prevented, and suspicious activity is reported.

Another goal, device security, advocates an approval process before new hardware or software can be installed on a system; it also advises managing the inventory of system assets so administrators can detect and respond to vulnerabilities. Related to device security is the data security goal, which stresses the importance of collecting log data and securing sensitive information with encryption.

Individual Users Represent the Greatest Vulnerability

While these basic best practices are familiar to all practitioners in the cybersecurity industry, CISA elevated them because it recognizes that individual users represent the greatest vulnerability to networks. One lapse in cyber hygiene can have a lasting impact and cripple citizen services. Even though cyber threats are invisible, they can noticeably disrupt the food supply, water systems, healthcare, and financial systems with long-term consequences. CISA's promotion of the guidelines shows the need for continuous awareness of the threats in cyberspace, and the importance of avoiding the complacency that can lead to an operational shutdown.

Attackers employ social engineering scams to manipulate individual users into clicking suspicious links, as happened with the Operation Sharpshooter attack that infected 87 critical infrastructure organizations. Through these infected devices, hackers could have gained access to Internet-enabled industrial control systems (ICS) at manufacturing facilities or wastewater treatment plants, causing further disruption. Unlike home or enterprise networks in which restoring the network will usually put you back in operation, an interruption of a wastewater treatment plant may involve days or weeks of work to clean filters and incrementally bring operational functions back online.

In addition to the disruption to operations, there is the financial cost that bears consideration: In 2022, 28% of critical infrastructure organizations experienced a destructive or ransomware attack, costing an average of $4.82 million per incident.

CISA recognizes the state of ICS vulnerabilities, and it has performance goals for protecting those systems, too. Because many critical infrastructure facilities are privately owned, government and industry are working together to coordinate improvements in the security posture, and CISA has a leading role. ICS represents a particular challenge due to the complexity and age of many ICS systems and the underlying operational technology, however, it underscores the importance of overall cybersecurity with four reasons to embrace its guidelines:

- Many organizations have not adopted fundamental security protections
- Small and medium-sized organizations are left behind
- Lack of consistent standards and cyber maturity across critical infrastructure sectors
- Cybersecurity often remains overlooked and under resourced

As the Internet of Things (IoT) connects more devices, the attack surface of critical infrastructure will increase, likely raising the cost of successful attacks. In health care, which CISA considers critical infrastructure, Internet-enabled equipment poses a risk. If a hospital's systems are well protected, but a supplier didn't secure the code in its dialysis or magnetic resonance imaging machines, the hospital becomes vulnerable.

Implementing CISA's new cybersecurity goals takes a dedicated investment, business process improvement, and regular audit to improve cyber defenses. As attacks on hardware, software, and data become more sophisticated, so too must the defenses with continuous modernization of cyber technology. It requires collaboration between CISA and infrastructure providers that will benefit from the agency's mission of promoting cybersecurity awareness, defending against threats, and striving for a more secure and resilient infrastructure. CISA's emphasis on foundational steps to take for cybersecurity are foundational. It may seem like a step backward, but it's actually a consequential leap forward.