Important Cybersecurity Tips for ASHRAE Pros

BY ECTON ENGLISH, MEMBER ASHRAE

"Shields Up!" is the slogan the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has adopted to bring attention to critical infrastructure cybersecurity. Recently, an increasing number of companies, small municipalities and government entities have been victims of various cybersecurity attacks. Some are indiscriminate malware and ransomware attacks while others are much more sophisticated and targeted toward specific entities.[1] The most important trend for awareness is that these types of cybersecurity incidents are only going to increase in the future. As ASHRAE professionals, this is an important time to increase cybersecurity awareness among HVAC professionals and take steps to improve our cybersecurity posture. The intention of this column is to help novice ASHRAE professionals take low-cost, basic steps to significantly improve their cybersecurity practices. The following are five considerations that can improve cybersecurity for you, industry partners and customers.

User Access

User access to a system is a key weakness often exploited in any cybersecurity incident. Users are often unwittingly the gateway for a cyber intrusion into a network that enables an attack to wreak havoc. These types of cyberattacks usually implement a click that leads to a malicious website where credentials are stolen or malware is loaded onto the victim's computer. Mitigations to limit this type of attack include:

- Providing basic cybersecurity education to all users. An educated user is a strong defense mechanism against malware introduction and social engineering, also known as social hacking.
- Providing users the minimum amount of privileges needed to perform their duties. Users with administrative or power-user accounts should only use those accounts when needed and use their general non-administrative accounts for normal duties. This practice can limit what an attacker can do with a compromised, non-privileged user account.
- Using multifactor authentication (MFA)[2] to limit the effect of stolen credentials. This technology requires users to have two forms of credentials, such as a password and a fingerprint, for system access. For additional security, use a time-based one-time password (TOTP) MFA solution, which generates a temporary code that can only be used for a limited time for system access. TOTP and MFA solutions can often be deployed to end users via a free cell phone application or key fob.

Ecton English is a subject matter expert for industrial control systems/supervisory control and data acquisition (ICS/SCADA) and the technical director for the facilities operations organization at the National Security Agency (NSA), Ft. Meade, Md.

Malware Detection and Prevention

Malware is a term that's used to describe any type of software that causes intentional disruption or harm to a computer or system.[3] Malware such as viruses and trojans are quite common, but many anti-malware tools are available to detect, quarantine and ultimately eradicate them. Newer malware, categorized as "ransomware," tends to be harder to detect, although modern anti-malware tools have been fine-tuned to guard against this attack vector. Ransomware is a sophisticated type of malware that encrypts an entire user's system, or multiple systems on a network, to prevent access until a ransom is paid. The encryption used is typically hard to break and, in many cases, companies and municipalities have paid these ransoms to cybercriminals to regain access to their information. Given the recent emergence and relative popularity of ransomware as a form of cyberattack, it's especially important that organizations take appropriate steps to mitigate this threat. Mitigations to help prevent the infection and spread of malware include:

- Using anti-malware software on all systems and keeping it updated. Even the most basic types of anti-malware tools can prevent a large number of viruses and trojans. Many free options are available; for example, currently all new Microsoft Windows Operations System installations (i.e., Windows 11) include a built-in anti-malware tool called Microsoft Defender. It is imperative to ensure that anti-malware tools are updated frequently so new malware can be detected and mitigated.
- Separating critical systems from each other to isolate the spread of malware. Determine if infrastructure control systems need to be connected to corporate business systems, and if so, only use well-defined and managed mechanisms such as a firewall.

Internet Connectivity

The advent of the Internet and its ability to connect service providers, industry partners, consumers, etc., has been revolutionary in the HVAC industry. However, cybersecurity has often been an afterthought. Many devices that are used to connect to the Internet are often vulnerable and easily exploitable. It is challenging to keep systems maintained, and with the proliferation of zero day attacks,[4] it is more critical than ever to mitigate their potential exposure, also known as the "attack surface" in cybersecurity parlance. To mitigate these vulnerabilities, organizations should consider:

- Disconnecting critical infrastructure control systems from any other systems to limit the spread of malware or successful network intrusion. This prevents an attacker from leveraging access across multiple connected systems.
- Using a virtual private network (VPN) or other secure mechanism for remote access. Using a VPN can help protect the communications channel from cybersecurity attacks and help limit who has remote access to the control system.
- Using a professional hosting service that can leverage sophisticated cybersecurity expertise and resources. Outsourcing is often a cost-effective measure to gain significant protections without having to hire and maintain a staff of cybersecurity professionals.
- Determining if Internet connectivity is absolutely needed. Eliminating the connection to the Internet greatly reduces the attack surface area. Often, islanding a system, known as "air-gapping," is an effective measure to reduce a system's attack surface. However, it by

no means is a cure-all and is not a substitute for good cybersecurity practices within an air-gapped system.[5]

Backups

Maintaining backups of critical control system software and information in a secure manner is an important strategy if one is subject to a cyberattack. Many smaller-scale control systems run on a local workstation or small server located in small utility rooms and are not interconnected with other systems. This can be very beneficial from a network security perspective, making it much less vulnerable to network attacks.

However, the systems that reside in these environments often do not get operating system, anti-malware and other critical patches and updates. A stray, infected USB drive or an unprotected vendor's laptop can introduce malware that could destroy thousands, if not hundreds of thousands, of dollars in control programming. System owners have invested significant funds in the design, construction and operations of control systems to enhance their building operations, and backups are a low-cost insurance policy. Consider the following to help protect these investments:

- Using external storage for offline backups. Very low-cost, high-performance external storage systems can be used to back up critical software and programming. This can save substantial amounts of money and time recovering from a catastrophic cybersecurity event.
- Leveraging vendor-hosted environments. Many control system vendors have the ability to both remotely host control system operations and the backups of critical programming in a 24/7 cloud environment. A vendor can also physically store the backup of systems at their facility as another option. Either way, in the event of a cybersecurity incident, recovery can be facilitated in a low-cost and time-effective manner that protects the owner's investment.

Leverage Free or Low-Cost Resources

Here are resources that can be used to help improve your organization's cybersecurity posture.

Free Resources

- **U.S. National Institute of Standards and Technology (NIST) Cybersecurity Resource Center.** NIST serves as a technological center for many cybersecurity-related documentation, guidance and best practices. https://csrc.nist.gov. NIST also has a dedicated sub-site dedicated to helping the cybersecurity of small businesses: http://www.nist.gov/itl/smallbusinesscyber
- **U.S. Cybersecurity and Infrastructure Security Agency (CISA).** CISA is a U.S. federal agency that works with businesses, communities and government to help make critical infrastructure more resilient to cyber threats. https://www.cisa.gov/infrastructure-security. One of the most valuable services CISA offers is tuition-free cybersecurity training that ASHRAE professionals can leverage. https://www.cisa.gov/uscert/ics/Training-Available-Through-CISA
- **Massive Open Online Courses.** These are free online courses produced by companies and universities providing education on various subject matter. Many basic cybersecurity offerings can be provided to system users to improve their cybersecurity awareness. https://www.mooc.org/

Vulnerability Information

- **CISA Known Exploited Vulnerability Catalog.** This is a database of known exploited vulnerabilities across a variety of hardware and software used on multiple platforms including control systems. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **Common Vulnerability and Exposures (CVE) Database.** An alternate name for this database is Common Vulnerability Enumeration (CVE). This website hosts a database of all past and currently known common vulnerabilities and exposures that have been reported. https://www.cve.org.
- **U.S. National Security Agency Cybersecurity Advisories & Guidance.** This website hosts a list of advisories and mitigations on evolving cybersecurity threats. https://www.nsa.gov/Press-Room/Cyberscurity-Advisories-Guidance

References

1. Slowik, J. 2019. "Evolution of ICS Attacks and the Prospects for Future Disruptive Events." Dragos, Inc. https://tinyurl.com/2kmw8vs4
2. NIST. 2022. "Multi-Factor Authentication." National Institute of Standards and Technology. https://tinyurl.com/4x23ar9e
3. NIST. 2022. "Malware." National Institute of Standards and Technology. https://tinyurl.com/zy9ya92r
4. Bogna, J. 2022. "What Are Zero Day Exploits and Attacks?" PCMag, Inc. https://tinyurl.com/3jhhkuhz
5. Wall, T. 2022. "Throwback Attack: An Indian Nuclear Power Plant Falls Victim to Outdated Policies." Industrial Cybersecurity Pulse. https://tinyurl.com/mr29bp68 ■