

Five Cyber Security Best Practices to Mitigate Remote Access Vulnerabilities

By: Alex Leemon

Recently, I attended several ICS Security and energy sector events. This year's topics revolved around meeting key regulations such as NERC CIP v5 and sharing best practices, lessons learned and emerging security trends. One key point stood out [as the sophistication and number of cyber-attacks on critical infrastructure](#) increases: it's more important than ever to understand the landscape of entry points into your OT networks and industrial control systems. The increased connectivity between IT and OT effectively extends this landscape of entry points to include business users and applications accessing critical assets as well as outside vendors accessing your systems remotely.

The energy sector is leading the way in taking measures to secure critical assets and doing a terrific job at sharing information about remote access best practices and technologies that help to mitigate the impact of a potential cyber-attack. [This is evidenced by the recent revamping of the E-ISAC by the North American Electric Reliability Council \(NERC\)](#). A number of security measures implemented by energy companies can be extended into other industries, and in fact, some of the measures are part of other standards and best practices such as the [NIST 800-82 Revision 2: Industrial Control System \(ICS\) security](#).

Some of these more traditional IT security best practices can be adapted to meet the unique remote access requirements of Industrial Control Systems. Here are five recommended actions:

1. **Identify all remote users, accounts and associated credentials.** Be sure to include SSH keys, hard-coded credentials and passwords to get visibility into who is accessing an organization's critical systems.
2. **Lock down credentials.** Once all remote users, accounts and credentials are identified, it's time to centrally store the credentials in a locked and safe environment where they can be more effectively managed. The users can then securely retrieve the password or SSH key, or request a direct connection to only the accounts they are authorized to access.
3. **Minimize direct connection to critical assets.** Isolating all sessions originating outside of the ICS domain and from unmanaged devices minimizes direct connections to any critical assets and keeps credentials shielded from unauthorized users.
4. **Trust but verify – keep an eye on remote users.** Implementing live monitoring and session recording can facilitate the identification of unauthorized activity. It can also help to confirm that remote users access only those systems they are authorized to see. Session monitoring and logging also supports compliance with industry regulations and standards.
5. **Deploy analytics tools.** To meet high availability requirements, early detection and alerts are key. Analytics tools can identify user and application patterns which in turn can be used to create privileged user and account profiles of normal behavior. When

abnormal activity is detected and alerted, incident response teams can address and disrupt in-progress attacks.

Implementing these five practices will significantly help in addressing the IT/OT connection related vulnerabilities and improve your ICS security posture.

About the Author:

Alex Leemon is a Sr. Product Marketing Manager at CyberArk, focusing on ICS Security Solutions. She has over 15 years of experience in industrial control (DCS) and safety systems. Before joining CyberArk, Alex served in various roles related to the development of Industrial control products. Alex holds a B.Sc. in Management and is currently pursuing an MA in Homeland Security (Cyber).

Some of the content of this article was originally posted on the CyberArk blog on October 29, 2015.

<http://www.cyberark.com/blog/5-it-best-practices-that-also-mitigate-cyber-security-vulnerabilities-in-ot/>