KUDELSKI SECURITY

OT CYBERSECURITY RECOMMENDATIONS

The OT security ecosystem typically lags behind IT by five to 10 years. While current IT controls may not transition to OT networks, the following defense-in-depth mechanisms can act as guidelines for securing OT environments. If a crucial security control cannot be applied, compensatory controls should be identified as appropriate.

Training and Awareness

An effective OT security program depends on the willingness of staff to accept security as an enabler of all computer-oriented activities. Training and awareness programs that improve knowledge and vigilance are critical for securing OT environments.

Security Assessments

Applications and data are critical to the normal functioning of OT devices, so we recommend an initial security assessment of applications for coding errors. Maintain data integrity and authenticity via cryptographic controls where appropriate.

Audits and Assessments

Periodic testing and system verification is key to optimal security, helping to eliminate paths that an attacker could exploit.

Risk Management Programs

Designing an effective OT security architecture requires a risk model that maps to functional system requirements and provides a view of the real-world consequences of compromise.

Supply Chain Management

Establishing a supply chain management program avoids creating weaknesses in the operations chain, especially when third parties need to access the corporate network.

Cyber Incident Response

A comprehensive cyber incident response plan covering proactive and reactive measures will help prevent incidents and better allow the organization to respond when one occurs.

Physical Access Controls

This typically means layered security measures that allow access for users to do their jobs, including key cards, biometric authentication, visitor escort services, fences, etc.

System Monitoring

Securing OT systems with well-planned strategies enables defense teams to detect, counter, and expel adversaries. At a minimum, physically separate IT and OT domains, segment networks, and isolate critical parts of the network. Secure a buffer zone where services and data can be shared between SCADA systems and business networks.

Deploy monitoring tools such as intrusion detection/prevention systems (IDS/IPS), identity awareness systems, and logging on all systems. Lock down unused ports on routers, switches, and network daemons, and ensure default configurations are not used.

Security Controls

Asset inventory helps to identify required security controls. Once assets have been identified, at a minimum implement the security features provided by device/system vendors and complement these with secure configurations (read/write protections, memory protection, etc.). Implement multi-factor authentication whenever possible and establish secure password policies.

Since OT system downtime is unacceptable and intervals between system upgrades can be years, we recommend an effective change management program to identify controls to remediate critical vulnerabilities that cannot be patched immediately, such as a host monitoring system that detects unauthorized changes to the host.

Organizations need to improve their posture by fostering a culture of security, adapting cross-sector mechanisms, and implementing context-based security controls.

However, doing so is not optional or an extra.

Organizations must implement and continually monitor technologies, policies, and procedures to help protect their environment and protect against known and emerging threats.

Kudelski Security, a division of the Kudelski Group (SIX: KUD.S), is an innovative, independent provider of tailored cybersecurity solutions to enterprises and public sector institutions. Kudelski Security is headquartered in Cheseaux-sur-Lausanne, Switzerland, and Phoenix, Arizona, with operations in countries around the world.

info@kudelskisecurity.com | www.kudelskisecurity.com