TAI ENGINEERS • MANAGERS • TECHNICAL SERVICES

QUARTERLY JOURNAL

OPERATIONAL TECHNOLOGY IMPLEMENTATION

ISSUE 01 MAR 2023

this issue

SECURING YOUR OPERATIONS

Segregating the control network

TAI typically proposeds separating the control network from the company's corporate network. This would helps to limit easier routes of unauthorized access to the control systems and minimize the risk of cyberattacks.

Implementing intrusion detection systems

TAI recommendeds implementing intrusion detection systems to monitor network traffic and detect potential attacks on the control systems.

Conducting regular security audits

The IT team recommended conducting regular security audits to identify new vulnerabilities and assess the effectiveness of the security measures.

Strengthening Cybersecurity in Life Science

A life science company that specializes in developing medical devices and pharmaceuticals recognized the need to enhance its cybersecurity posture. The company had experienced several cyber incidents in the past, including data breaches and ransomware attacks, which had resulted in financial losses and reputational damage. The company's management realized that the life science industry is highly regulated, and any cyber incident could have serious consequences for patient safety and regulatory compliance.

The company's IT team identified that its operational technology infrastructure was vulnerable to cyberattacks, and a breach could compromise the confidentiality, integrity, and availability of critical data and systems. The company needed to take measures to secure its operational technology infrastructure, which included Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and Human-Machine Interfaces (HMIs).

The company implemented TAI recommended cybersecurity measures, which resulted in a significant improvement in its cybersecurity posture. The implementation of the measures has led to enhanced protection of critical systems and data, minimized the risk of cyber incidents, and ensured compliance with industry regulations and standards. The company continues to conduct regular risk assessments and security audits to identify new vulnerabilities and assess the effectiveness of the security measures.

The life science industry is highly regulated, and any cyber incident could have serious consequences for product safety and regulatory compliance. This case study highlights the importance of implementing a comprehensive cybersecurity plan to secure operational technology infrastructure in the life science industry. By investing in cybersecurity measures, the company was able to protect critical systems and data, maintain regulatory compliance, and mitigate the risk of reputational damage and financial losses.

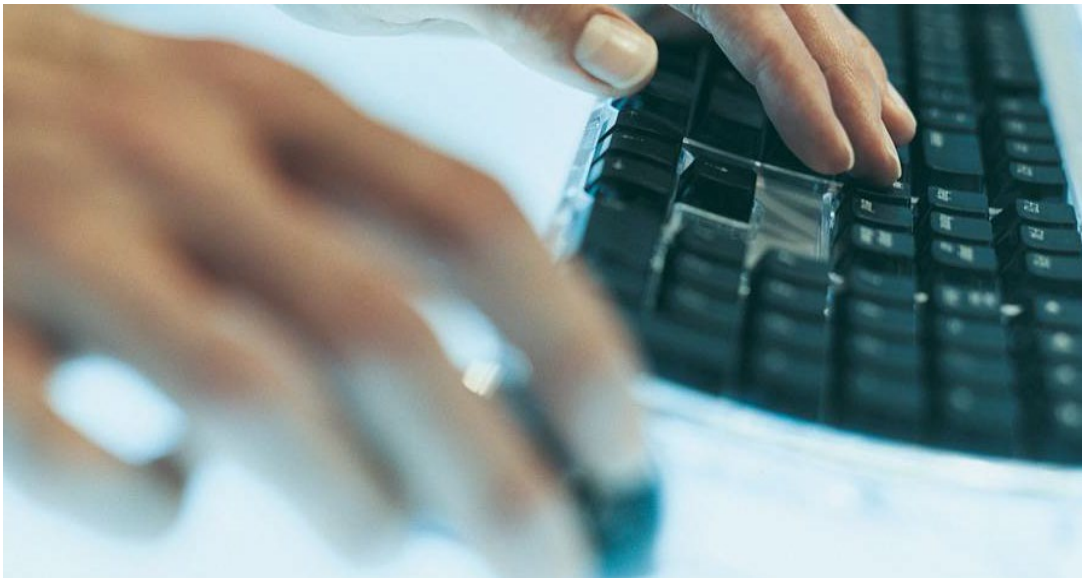
Cybersecurity Planning: What OT Managers Really Need to Know

An operational technology cybersecurity plan is essential for any organization relying on industrial control systems.

An operational technology (OT) cybersecurity plan is a comprehensive set of strategies, policies, and procedures designed to protect the OT infrastructure of an organization from cyber threats. Operational technology refers to the hardware and software systems that control physical processes, such as manufacturing, energy production, or transportation.
The goal of an OT cybersecurity plan is to safeguard the industrial control systems (ICS) and SCADA (Supervisory Control and Data Acquisition) systems that are used to monitor and control critical processes. These systems are often connected to the internet, making them vulnerable to cyber attacks, such as malware, phishing, and hacking.

TAI's OT team proposes a comprehensive cybersecurity plan that include the following measures:

1. Risk assessment and compliance: The IT team conducted a risk assessment to identify vulnerabilities in the company's operational technology infrastructure. Based on the assessment, the team identified areas of non-compliance with industry regulations and standards, such as FDA guidelines, NIST, and ISO. The team then developed a roadmap to address the compliance gaps and mitigate risks.
2. Threat analysis: Analyzing the various types of cyber threats that may target the OT infrastructure.
3. Access control: Implementing strong access controls and authentication mechanisms to prevent unauthorized access.
4. Segregation of networks: The IT team proposed segregating the company's operational technology network from the corporate network to prevent unauthorized access to critical systems and data. The team also recommended implementing firewalls and access controls to limit network access to authorized personnel.
5. Incident response: Establishing standard operating procedures for detecting, responding to, and recovering from cyber incidents.
6. Hardening of PLCs and SCADA systems: The IT team proposed implementing measures to harden PLCs and SCADA systems, including disabling unused ports and services, changing default passwords, and applying firmware updates to address known vulnerabilities. The team also recommended implementing intrusion detection and prevention systems to monitor network traffic and detect potential attacks on the control systems.
7. Employee training and awareness: The IT team proposed conducting regular employee training and awareness sessions to educate personnel on the importance of cybersecurity and how to identify and report potential cyber threats.
8. Continuous monitoring: Regularly monitoring the OT infrastructure for vulnerabilities, anomalies, and suspicious activity.



Segmenting Your OT Network

Virtual Local Area Networks (VLANs) are a fundamental component of modern network design. VLANs allow network administrators to logically partition a physical network into smaller, isolated, and independent segments that operate as individual networks. These logical networks can then be configured with their own unique network settings, including IP addresses, subnets, and access controls, providing a higher level of security and flexibility to the network. VLANs are important for both security and scalability, and are used in a variety of applications across various industries.

One of the key advantages of VLANs is improved security. By isolating traffic within specific VLANs, network administrators can limit the potential damage caused by security breaches or network attacks. For example, if a device within a VLAN is compromised, the attack is limited to the devices within that VLAN and is prevented from spreading to other VLANs. This helps to minimize the impact of security incidents, making it easier to detect, contain, and remediate security threats.

Another important aspect of VLANs is scalability. As networks grow, managing and organizing devices and users becomes increasingly complex. For example, VLANs can be used to separate different departments within an organization, such as accounting or HR, into their own logical networks. This makes it easier to apply different access controls and policies to each group, improving overall network performance and efficiency.

In conclusion, VLANs are an important component of modern network design, providing enhanced security, flexibility, and scalability. By isolating traffic and grouping devices into logical networks, VLANs enable network administrators to create a more secure and efficient network environment.

SOFTWARE

Symantec Endpoint Protection

(SEP) is a security software solution that can help secure workstations in your organization. using SEP to secure workstations involves installing and configuring the software, enabling key security features such as firewall and intrusion prevention, controlling access to external devices and applications, using reporting and alerting features to monitor for suspicious activity, and keeping the software up to date. By following these steps, you can help protect your organization's workstations from a wide range of security threats.

Ensure that SEP is installed on all workstations in your organization and that it is properly configured. This includes setting up policies, schedules, and alerts. SEP can also be used to control which applications are allowed to run on workstations. This can help prevent the execution of malicious or unauthorized software. It can also detect and block known vulnerabilities and attacks. Enable intrusion prevention and configure it to protect against the latest threats.

Centralized Reporting

Centralized reporting ensures that everyone in the organization is working with the same information and data. This promotes consistency in reporting and reduces the risk of errors or discrepancies. With a centralized reporting system, data is stored in one location, which makes it easier to access and share across the organization. This can help save time and resources, as employees don't have to search for the information they need. Centralized reporting can also help ensure that reports are standardized across the organization, with consistent formats, templates, and styles. This can improve the readability and usability of reports.

600 Red Brook Blvd
Suite 300
Owings Mills, MD 21117
410.356.3108
taiengineering.com

Q&A TECHNOLOGY TIPS

Q: User Management: Why Have Unique Access Control Logins to Equipment?

A: By requiring unique user logins, you can ensure that only authorized users are able to access your system or application. This can help prevent unauthorized access, data breaches, and other security issues.

Unique user logins also allow you to track individual user activity and determine who has accessed or modified data. This can help you hold users accountable for their actions and identify any potential issues or suspicious activity.

Edge Computing to Revolutionize the Way Data is Processed

Edge computing is a rapidly evolving technology that is transforming the way data is processed and analyzed. With increased adoption, focus on security, integration with cloud computing, and advancements in edge AI, edge computing is set to play a key role in the future of technology across various industries.

- Increased adoption of edge computing: The adoption of edge computing is rapidly increasing across various industries, including manufacturing, healthcare, transportation, and retail. Edge computing is being used to process and analyze data closer to the source, which reduces latency and enables real-time decision-making.
- Growth in edge devices: The growth of IoT devices has led to a significant increase in the number of edge devices. These devices include sensors, cameras, and other connected devices that collect and transmit data. Edge computing enables these devices to process data locally, reducing the amount of data that needs to be transmitted to the cloud or data center.
- Focus on edge security: With the increasing adoption of edge computing, there is a growing concern about the security of edge devices and networks. The industry is focusing on developing secure edge devices and networks that can protect against cyber threats and ensure data privacy.
- Edge-to-cloud integration: Edge computing is not intended to replace cloud computing but rather to complement it. Many organizations are now integrating edge computing with cloud computing to create a hybrid environment that enables real-time data processing at the edge while still leveraging the scalability and flexibility of the cloud.
- Advancements in edge AI: Edge AI is an emerging trend in the industry, where AI algorithms are run on edge devices to enable real-time decision-making. Edge AI is being used in applications such as autonomous vehicles, predictive maintenance, and smart homes. With the growth of edge devices and advancements in AI, edge computing is expected to become an increasingly important technology in the years to come.