IT/OT system related challenges from supply security perspective

ERRA Workshop Cybersecurity of Energy Infrastructure

Perry Pederson

Nuclear Security IT Specialist

IT & OT Defined

- **IT Systems:**
  - Information Technology systems manage data, information, and communications within an organization.
- **OT Systems:**
  - Operational Technology systems control and monitor physical devices and industrial processes in various environments.

IT Concerns

IT primarily deals with computers, storage, networking devices, and other physical devices, infrastructure, and processes to create, process, store, secure, and exchange all forms of electronic data.

- Data management
- Business operations
- Computers, servers, networking devices
- Data breaches, malware, phishing
- Regular updates and patches
- Standard IT protocols (e.g., TCP/IP)
- Financial loss, productivity impact
- Often integrated with business applications

OT Concerns

OT primarily refers to hardware and software that monitor and control physical devices, processes, and events in industrial environments

- Control and monitoring of physical processes
- Programmable Logic Controllers (PLC)
- Sensors and actuators
- Safety, reliability, and availability of physical processes
- Infrequent updates due to critical nature of operations
- Industrial protocols
- Safety hazards, operational disruptions
- Often isolated, but increasingly integrated with IT systems

IT Versus OT

Aspect	IT Systems	OT Systems
Purpose	Manages data, information, and communications	Controls and monitors physical processes and systems
Environment	Offices, data centers, cloud	Industrial settings, such as factories, power plants
Security Focus	Confidentiality, integrity, availability	Safety, reliability, availability
Main Protocols	HTTP, HTTPS, TCP/IP	Modbus, DNP_3, BACnet, OPC
Update Cycle	Regular updates, patches	Infrequent updates, due to potential disruptions
Downtime	Tolerable for scheduled maintenance	Minimal downtime, critical for continuous operations
Examples	Email systems, databases, web servers	SCADA systems, PLCs, DCS

Offshoring versus Onshoring

Offshoring

- **Cost Efficiency:** Offshoring can significantly reduce operational costs due to lower labor rates in other countries.
- **Access to Global Talent:** It provides access to a diverse pool of skilled professionals worldwide.
- **Potential Risks:** Increased vulnerability to cyber-attacks and data breaches due to varying international cybersecurity standards.
- **Supply Chain Complexity:** Managing and coordinating across different time zones and regulatory environments can complicate supply chain logistics.

Onshoring

Enhanced Security: Onshoring can offer better control over cybersecurity measures and compliance with local regulations.

Faster Response Times: Proximity allows for quicker issue resolution and real-time collaboration.

Higher Costs: Generally involves higher operational costs due to local labor rates.

Limited Talent Pool: May restrict access to a global talent pool, potentially limiting innovation and expertise

Vendor Dependence versus Independence

Vendor Dependence

- **Single Point of Failure:** Relying heavily on a single vendor can create a vulnerability. If the vendor experiences issues or security breaches, the entire system could be compromised.
- **Cost Efficiency**: Often, long-term contracts with a single vendor can lead to cost savings due to bulk purchasing and standardized training.
- **Streamlined Support and Maintenance:** A single vendor relationship can simplify support and maintenance processes.
- **Limited Flexibility:** Dependence on a single vendor might limit the ability to quickly adapt to new technologies or switch to better solutions.

Vendor Independence

- **Enhanced Security:** Using multiple vendors reduces the risk of a single point of failure, thereby improving overall system resilience.
- **Innovation and Flexibility:** Independence encourages competition among vendors, leading to more innovative solutions and the ability to adapt quickly.
- **Higher Costs:** Managing relationships with multiple vendors can increase administrative and operational costs.
- **Complexity in Integration:** Ensuring compatibility and seamless integration between different vendors' systems can be challenging and may require additional resources.

Open Source versus Closed Source

Open Source

- Transparency: Open source software allows for complete visibility into the source code, enabling thorough security audits and vulnerability assessments.
- Community Support: A broad community of developers contributes to identifying and fixing bugs, which can lead to rapid improvements and updates.
- Flexibility: Users can modify the software to meet specific needs, providing a high degree of customization and adaptability.
- Security Risks: While transparency is a strength, it also means that potential vulnerabilities are visible to malicious actors, requiring rigorous and continuous security monitoring.

Closed Source

- Proprietary Control: Closed source software is developed and maintained by a single company, providing a controlled and managed development environment.
- Security through Obscurity: The source code is not publicly available, which can deter some types of attacks but also limits the ability to independently verify security measures.
- Vendor Dependence: Users rely on the vendor for updates, support, and security patches, potentially leading to slower response times if the vendor is unresponsive.
- Consistency: Closed source software often provides a more consistent and polished user experience, as it is designed and maintained by a single entity.

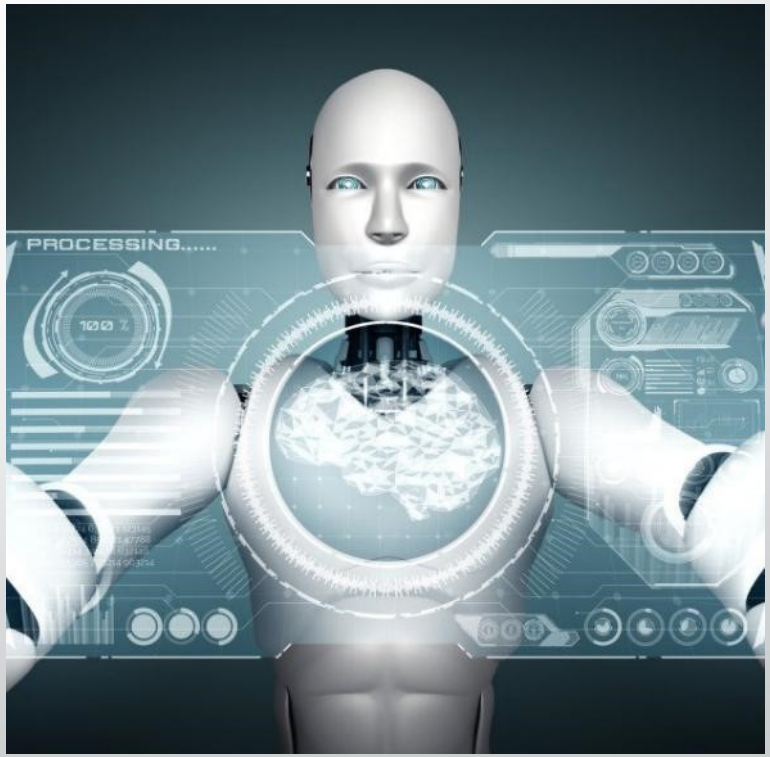
Impact of New Technology (AI)

AI is the latest technology that can enhance attacker's capability.

- Automated Vulnerability Scanning: AI can continuously scan networks and systems for vulnerabilities, identifying potential entry points for attackers.
- Sophisticated Phishing Attacks: AI can analyze vast amounts of data to create highly personalized and convincing phishing messages.
- Adaptive Malware: AI can develop malware that can change its behavior to evade detection by antivirus software.

Autonomous Goal Oriented AI Agents

- Autonomous AI agents represents a more advanced and potentially more dangerous approach to cyber attacks, as it reduces the need for human intervention and increases the ability to adapt and persist in the face of defenses.
- Autonomous AI agents are capable of executing more complex and adaptive attack strategies compared to AI-enhanced hacking, which relies on human creativity and human decision-making.



Supply Chain Risk Management (SCRM)

Information Technology (IT) and Operational Technology (OT) systems are critical to ensuring the resilience of supply chains and industrial operations. As supply chains become increasingly digitized and interconnected, the risks posed by cyber threats to IT and OT systems have grown significantly.

Supply Chain Risk Management (SCRM)

Lack of Supply Chain Risk Management (SCRM) transparency allows adversaries to remotely access and manipulate critical electric power infrastructure, posing risks to national security and Bulk Power System (BPS) reliability.

- Transparency in process (open source)
- Opaqueness in content (CIA)

General Goals to Improve SCRM

- Enhance national security by supporting critical industry-specific vendors.
- Incentivize domestic manufacturing to reduce reliance on foreign-owned, controlled, or influenced suppliers.
- Leverage Power Marketing Administrations (PMAs) and National Laboratories as pilot programs for SCRM improvements.
- Encourage private sector adoption of SCRM recommendations.
- Promote regulatory changes to support SCRM transparency and accountability.

Improving SCRM Through Regulation

Develop a Notice of Proposed Rule Making (NOPR):

- Require use of an Acquisition Resource Center (ARC) and attestation ecosystem for BPS asset owners and operators.
- Ensure regulatory underpinnings for Defense Critical Electric Infrastructure (DCEI) and Made-in-America (MnA) compliance.

Improve SCRM at the Secretariat-Level

- Establish Acquisition Resource Centers (ARCs) to centralize procurement and collaboration.
- Develop an Attestation Ecosystem (Nodes and Channels) for supply chain transparency, enabling real-time access to asset information.

Improve SCRM at the Program-Level

- Conduct holistic threat assessments to track evolving risks.
- Develop a Design Basis Threat (DBT) profile to identify adversary capabilities and pathways.
- Implement a Kill Chain Methodology to detect and prevent adversary actions.
- Build a proactive defense model to increase adversary costs and improve infrastructure resilience.
- Enhance reactive defense capabilities, including rapid response and recovery plans for BPS attacks.

Unified National SCRM Implementation

- Foster public-private partnerships to manage SCRM complexities.
- Leverage existing standards like ISA/IEC 62443 for cybersecurity assurance.
- Establish a task force to coordinate SCRM efforts across federal agencies, industry, and regulatory bodies.

Software Bill of Materials (SBOM)

An inventory that outlines all the components, libraries, and dependencies included in a piece of software. It provides detailed information about each component's version, license, and origin.

- Enhanced Security
  - Identifies vulnerable components and ensures timely updates or patches, reducing the risk of security breaches.
- Compliance and Transparency
  - Helps meet regulatory requirements and provides transparency about software composition, ensuring adherence to licensing and security standards.
- Efficient Risk Management
  - Allows organizations to assess and manage risks associated with third-party components, improving overall software quality and reliability.

SBOM Video: SBOM

SBOM Terminology

- **SBOM Author:** Creates an SBOM.
- **SBOM Consumer:** Receives the transferred SBOM.
- **SBOM Distributor:** Receives SBOMs for the purpose of sharing them with SBOM Consumers or other Distributors
- **Discovery:** Mechanism used by the consumer to know the SBOM exists and how to access it.
- **Access:** Access control mechanisms used by the author or [distributor] to regulate who can view or use an SBOM.
- **Transport:** Mechanism provided by the author or provider to transfer an SBOM.

Progress Toward SCRM Adoption

- Executive Order 14017 on Securing America's Supply Chains, issued in February 2021, directed federal agencies to assess and strengthen the resilience of critical supply chains. This includes sectors such as information and communications technology (ICT), pharmaceuticals, and critical minerals.
- The Department of Defense has its own SCRM policies to manage risks throughout the supply chain, from initial production to disposal. This includes cybersecurity, software assurance, and protection against counterfeit parts.

Progress Toward SBOM Adoption

- Executive Order 14028 on Improving the Nation's Cybersecurity, issued in May 2021, mandates that federal agencies and their software suppliers provide an SBOM for each product sold to federal government agencies.
- The National Telecommunications and Information Administration (NTIA) has outlined the "Minimum Elements for an SBOM," which include data fields like component name, version, supplier, and automation support for machine-readable formats.
- The U.S. Food and Drug Administration (FDA) requires manufacturers of certain medical devices to submit an SBOM during the premarket review process.

Conclusions

- A transparent, attestable SCRM and SBOM process is essential to secure the BPS against evolving threats.
- Collaboration between government, industry, and regulatory bodies is critical to achieving a resilient and secure energy infrastructure.

Köszönöm

Van valakinek kérdése?