TATA

TATA ADVANCED SYSTEMS

CYBER SECURITY PRACTICE

Why Organizations are Concerned about the Security of Critical Infrastructures?

The moment since Operational Technology (OT) and Information Technology (IT) have fused, new doors to possibilities have opened. This convergence has added new capabilities to industrial control systems (ICS) and brought several benefits including enhanced productivity, improved system performance, and reduced costs. Along with numerous advantages, it has also generated a new set of vulnerabilities and expanded the attack surface of the critical infrastructures like power generation plants, water treatment plants, oil & gas refining plants, transport systems, etc. As per a recent report[1], 74% of IT security professionals globally are more concerned about a cyber-attack on critical infrastructure compared to an enterprise data breach.

Growing Attacks on Critical Infrastructures

The world has witnessed a lot of devastating cyber-attacks on industrial control systems right from the year 1903 when hackers compromised the Marconi's secure wireless telegraph presentation with Morse code. One of the famous cyber-attacks that holds a special place in the books of history took place in 2010 at Iran's Natanz uranium enrichment facility, where the Stuxnet worm reportedly destroyed numerous centrifuges.

The primary factor behind this rising frequency is the growing reliance on Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs) and distributed control systems for controlling physical devices and monitoring processes.

Now, let's glance through some recent cyber-attacks on critical infrastructures in India and across the globe:

- In May 2020, Taiwan's state-owned energy company, CPC Corp., hit by a massive ransomware attack. Later, in the same month, Israel also reported an attempted cyber-attack on control systems at water facilities.
- In March 2020, the ransomware attack targeted a US-based natural gas compression facility.
- In November 2019, Kudankulam Nuclear Power Plant in Tamil Nadu experienced a major malware attack.
- In May 2019, the computer systems of power distribution companies (Discoms) of Telangana and Andhra Pradesh were hit by a ransomware attack.
- In December 2018, Italian oil firm Saipem suffered from Shamoon malware attack that erased data residing on the company's computers.
- In March 2018, Haryana Power Discom suffered a cyber-attack on its Automatic Meter Reading System (AMR) that encrypted billing data of about 4000 industrial consumers.
- In November 2017, a huge malware attack disrupted operations of THDC Ltd's Tehri dam in Uttarakhand.

Challenges to the Security of Critical Infrastructures

Increased Connectivity

The increasing infiltration of internet-connected devices in OT networks and industrial control systems have provided threat actors with a multitude of entry points to critical infrastructures. Since the OT networks were not primarily designed for exposure to the Internet, the likelihood of cyber-attacks in such environments is constantly growing.

Skill Shortage

Lack of skilled cybersecurity resources is a major challenge faced by organizations across the globe. When it comes to the security of critical infrastructures, businesses need some talent that understands both IT & OT systems and can determine and remediate potential vulnerabilities in both environments. This is why a majority[2] (93%) of cybersecurity professionals believe that OT security should be encompassed into the education and training of IT security practitioners.

Lack of Visibility into the Attack Surface

Lack of detailed visibility does not let security teams to completely defend valuable assets against sophisticated cyber-attacks. It creates blind spots that help attackers to circumvent security controls and breach unsecured elements including IT & OT systems. Thus, it is imperative for security teams to have a clear picture of incoming and outgoing IT traffic and existing anomalies. In a recent survey[3], it was found that only 36% of critical infrastructures have a high level of cyber resilience.

Apart from the above-mentioned major challenges, there are some other factors as well that impact the security of critical infrastructures.

- Growing rate of automation in industrial processes
- Increasing complexity of industrial control systems
- Evolution of cyber threats

Recommendations to Ensure the Security of Critical Infrastructures

Let's go through some useful tips that can help organizations to optimize the security of their critical infrastructures.

- Identify all existing critical assets
- Enhance visibility into the IT & OT networks
- Search proactively for abnormal activities that may cause severe damage
- Maintain backup of system data and configurations
- Disable unnecessary ports and services
- Implement a risk-based approach that incorporates detection, response, and recovery plans as well
- Meet necessary compliance with industry regulations
- Improve collaboration with government bodies, corporate entities, and other institutions
- Conduct OT security training for IT security professionals

Protecting critical infrastructures from the growing threat of cyber-attacks has now become a topic of boardroom discussion for CISOs, CIOs, and business stakeholders. Organizations must adopt a proactive and predictive approach to bridge the widening gap in the security of IT and OT networks.

The Cyber Security Practice of Tata Advanced Systems provides an advanced and comprehensive set of security services for quick threat detection and incident response across IT and OT environments. We help you design an effective OT security program to determine and eliminate potential risks while ensuring business continuity without interruptions.

For more information, connect with us at
contactcs@tataadvancedsystems.com

References:
1, 2 - Global State of Industrial Cybersecurity Report
3 - Greenbone Network Research