SYNOPSIS OF TECHNICAL PAPER ON

How and why to protect Operational Technology systems

As cybersecurity breaches of industrial control systems (ICS) continue to increase, two things are clear. Firstly, information technology (IT) is converging with operational technology (OT) – hardware or software that monitors or controls physical devices and processes. Secondly, while most companies now take IT cybersecurity seriously, many underestimate security risks from the OT in their industrial control systems.

The consequences of inadequate protection are significant. A malfunction in the production chain may cause financial loss, injury or environmental damage. However, ICS are often considered safe as they are "not connected to the internet" or "not based on vulnerable technologies". For this reason, they are not subject to regular updates or security assessments. For operational reasons, though, systems are occasionally connected to a company network or to a standalone PC. If these are not fully secure, opportunistic malware can easily penetrate the ICS and damage or block the system. A deliberate targeted attack, perhaps designed to steal data or blackmail a company, would be child's play.

There are four key elements:

1) **OT cyber threats increasingly resemble those of IT systems.** They are dynamic, constantly renewed during the life of the system, and exploit vulnerabilities in individual components;
2) **Vulnerabilities may derive from interdependencies** and interfacing systems or from operational changes. Initial checks and certifications do not ensure security during the system's entire life cycle;
3) **Continuous system security management is essential** due to the complexity and distribution of OT systems. Staff should be trained to maintain and improve system security;
4) **No single security measure can protect an OT system.** A series of measures must work in combination to increase the system's resilience and protect critical components.

These four elements point to one clear conclusion: when planning security measures for industrial control systems, we need to consider the system throughout its life. When advising on IT and OT cybersecurity at RINA, we focus on developing a cost-effective approach that is tailored to our client's specific needs and covers the control system's entire life cycle.

1. Ensure that everyone involved in the system life cycle, including component manufacturers, integrators and end users, contributes to managing system security;
2. Extend security assessments beyond the initial system release phase;
3. Insist the supplier remains responsible for continually assessing cyber risks to the system or components and informing the customer of new potential vulnerabilities;
4. Develop a robust cyber risk analysis process;
5. Conduct regular staff training and checks;
6. Carry out regular assessments of cyber risks for producers, integrators and users to verify the system's protection and resilience;
7. Implement a two-way process for recording incidents and sharing information between the contractor and the client.

DETAILS OF AUTHOR

Name : Antonio Mario Durante
Designation : Head of Space & Defence Develoment Support Services
Company : RINA Services S.p.A
Address : Via Renata Bianchi, 38, Genova, Italy 16152
Phone : +39 010 6021306
Email : antonio.durante@rina.org