Operational technology security: an urgent need for action

March 2024

Annika Nitschke

In recent years, steadily-growing cyber-security threats have been evident, and they are not limited to IT systems. Cyber criminals are increasingly focusing on hacking production systems, which are also referred to as operational technology (OT). For many companies, these systems are often outdated and have low levels of security. While companies worldwide are investing heavily in IT security, many have yet to prioritise OT security. Production systems frequently represent the most critical assets in a company, and an outage could pose consequences that threaten a company's existence. While IT systems can be restored or replaced relatively quickly – assuming proper business continuity management is in place – production systems are often unique, and depending on the extent of the damage, recovery can be a much more onerous process.

IoT and cloud applications increase the need for security in automation

The lack of advanced security technologies and the use of outdated systems have been weak points in OT security for years. The increased networking of these systems is contributing to the elevation of OT security as a potential target for cyber-security threats. IT and OT are no longer areas that operate separately from each other, as was often the case in the past. There are no longer simple or individual points of contact in the modern enterprise architecture. For example, IT-managed corporate internet access is being used for IoT and cloud applications, which are increasingly being used in production and are creating new gateways to access OT systems.

The pressure on companies regarding cyber security is not solely driven by the increasing cyber-security threat to OT systems. In the EU, legislation has adapted to the increased need for cyber security. With the Network and Information Systems Directive 2 (NIS 2) and the Cyber Resilience Act, companies are faced with new requirements for the protection of critical infrastructures and supply chain security. This represents a major challenge, especially for smaller companies, which were not necessarily affected by previous legislation and are often starting from scratch in setting up a security organisation and implementing the required measures.

IT versus OT: security needs to be rethought

Security projects are usually implemented and governed from the perspective of the IT department, which can lead to major challenges for production capability. In IT, the top priority is confidentiality and integrity. In contrast to IT, availability is the top priority in OT, along with safety – the protection of people and the environment – also being particularly relevant. Because of that, the systems in the OT environments often do not fit the traditional approach to IT security, as the strategies, concepts and processes do not apply in the same way. As security measures often cannot be retrofitted, a differentiated approach is required to ensure the right security measures are in place, especially since many OT devices have unique security requirements.

For example, while patching vulnerabilities and regularly updating systems are effective security measures in IT, this is often not possible and sometimes even undesirable in OT due to the requirement for continuous 24/7 operations. OT systems oftentimes face a lack of test systems. Because of this, the effects of regular patches and updates are unpredictable and can potentially cause unwanted problems. Whether or not an update needs to be carried out is therefore a question of necessity and feasibility and must be determined in close co-ordination between IT and OT.

Figure 1: Comparison between the objectives of OT systems and IT systems

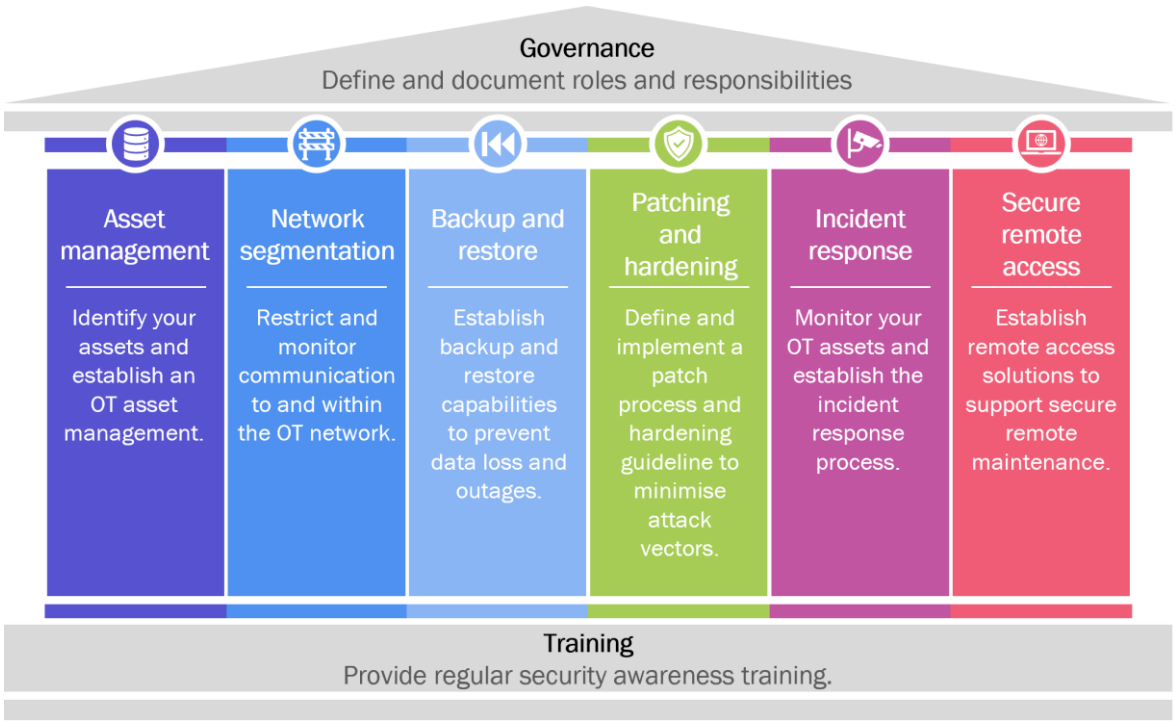
Information technology (IT)		Operational technology (OT)
3–5 years	Lifecycle	5–25 years
Confidentiality and integrity	Security objectives priority	Availability and safety (protection of people and environment)
Hardware and software components used are standardised and specifications for purchasing conditions are known	Standardisation	No consistent standardisation of hardware and software; lack of specifications for both purchasing conditions and integration of IT components in control systems, machines and production facilities
Available	Test environment	Rare
Standard process; critical patches can be applied on short notice	Patch and vulnerability management	Rare, approval from manufacture required and patches can only be applied within maintenance windows
Many custom solutions in place	Security solutions	Rare, unknown process interferences and the expiration of warranty through the installation of security software is possible

Source: Analysys Mason

Effective security starts with the basics

Security vendors are responding to the growing demand for OT security solutions. Some vendors have now developed dedicated OT security software for vulnerability management or endpoint security. However, even without the introduction of such solutions, it is important that companies realise they can raise the security level of their production environments with the implementation of basic technical and organisational measures, which are outlined in Figure 2.

Figure 2: Technical and organisational measures organisations need to adopt to increase the security level within OT environments to lower the risk of cyber attacks



Source: Analysys Mason

Security requires governance

For basic technical and organisational measures to be implemented successfully, companies require an OT organisation within their company that is responsible for the operation of OT assets. Additionally, this OT organisation should serve as a central authority to develop sustainable and operationally viable security concepts together with the IT and the security organisations. In fact, OT must be included in all relevant projects within the IT department to contribute expertise as required and vice versa. However, this relies on the existence and effectiveness of the appropriate underlying processes, often requiring change of mindset.

To implement the requirements effectively, the OT organisation needs to operate within a well-defined management framework. Companies can adopt the IEC 62443 as a guide, which is now recognised as the relevant standard for OT security and is a supplement to the ISO 27000 series of standards relevant to IT security.

Do you need to review your OT security?

We can support clients in all aspects of OT security and help them to build a strong OT organisation. Please do not hesitate to contact us.