SECUINFRA
Cyber Defense. Made in Germany.

Professional article

Operational Technology (OT) Security today and tomorrow:

Manufacturing and industrial facilities need to be ready for cyberattacks now!

Companies are aware of their vulnerability to cyber attacks. However, they often do not focus on the security of their operational technology (OT), i.e. their manufacturing plants or infrastructure facilities. Yet it is precisely here that the potential for damage can be enormous - and even lead to danger to life and limb. Operational technology (OT) security must therefore be an essential part of a company's IT security concept, but it must also take into account the special challenges such as outdated systems or harsh, industrial operating environments - for example, exposure to high temperatures or dust. Companies should choose a step-by-step approach for an introduction and rely on up-to-date security procedures.

Reports of cyber attacks on companies are ubiquitous in the media - companies such as large electronics chains are just as affected as public administrations. Attackers (groups) are characterized by a high level of criminal energy - they are highly motivated in their actions, well networked and have commercial or political interests in spying on their target company, blackmailing it and damaging it financially or in terms of its reputation.

A large number of companies therefore strive to achieve and maintain an appropriate level of IT security. However, limited IT security budgets and a lack of time and personnel resources often limit their options. In addition, operational technology (OT) security - i.e., the protection of operational technology such as manufacturing and industrial plants or infrastructure facilities - is often not even a focus of security concepts in companies. Yet the damage can be immense: The consequences of malfunctions and failures can range from lost sales to danger to life and limb or even the environment.

However, companies are often unable to identify potential threats to their OT in time or to continuously monitor suspicious data traffic. They lack controls to manage and monitor the security and risks posed by IoT (Internet of Things). Yet the integration of IoT with artificial intelligence, machine learning, automated processes and cloud technologies is still in its infancy. At the same time, the "never change a running system" paradigm is still too often applied. This is fatal, because in the dynamic age of digitization, not only should one's own IT strategy and infrastructure be regularly scrutinized with regard to their security, but fundamental system decisions should also be put to the test.

Despite some overlap between OT and IT, such as the use of identical operating systems, infrastructure or network components, there are fundamental aspects in OT that must be taken into account:

- Safety First: An OT system must run safely and stably, because in the worst case, malfunctions can endanger life and limb.

- No interruptions to control operation: Shutting down and starting up the system involves a great deal of effort.

- OT often still uses old hardware with operating systems that no longer receive manufacturer support and security patches.

- The use of solutions from non-IT, often medium-sized system manufacturers, is also still widespread.

- Many components and devices are only available to a small number of personnel.

- Protocols used are different from those used in IT (ICCP, Modbus or DNP3).

- The operating environments of industrial plants are challenging and harsh, for example in terms of prevailing temperatures, mechanical impacts such as vibrations, or dust and dirt loads.

For Operational Technology (OT) Security, systems from two worlds must therefore be connected with each other; however, these systems can sometimes have been in operation for decades and be poorly documented. This is another reason why OT security is not a quick win, but rather complex and laborious. For this reason, a step-by-step approach is recommended to raise the security level at OT level in the long term and sustainably.

1. Inventory of assets

This is where the inventory of assets is recorded (asset inventory). This means researching and analyzing what the OT system landscape looks like, how it is integrated in the network and which data, software, systems, devices and processes need to be protected. A vulnerability analysis is performed in conjunction with possible patches. It is critical not to overlook blind spots that attackers can exploit.

2. Risk analysis

Inventory and vulnerability analysis provide the necessary information for risk analysis. For example, sometimes it may be safer to work with an older system version without patches and mitigate a potential security problem through targeted monitoring: One then accepts or mitigates a risk, rather than potentially crashing the system by making changes whose complexity

and dependencies cannot be predicted to their full extent. For risk analysis, the MITRE ATT&CK Framework for Industrial Control Systems (ICS) provides appropriate guidance.

3. Central logging

Cyber attacks, or even a malfunction of a system or component, leave their traces in log files. The central collection of these log files is therefore the basic requirement for analysis, alerting and automated containment of an attack. It is crucial that the log data of the most diverse, sometimes old subsystems are stored in a normalized format: Performant analysis methods and machine learning require clean data.

OT Security gets to work

Once these foundations have been laid, the work of establishing OT Security can begin. It consists primarily of the ongoing analysis of log data to detect and defend against attacks in a timely manner. Two methods that have proven themselves in IT security are used here: real-time correlation and user and entity behavior analytics (UEBA), i.e., unsupervised machine learning.

In the Realtime Correlation method, log data is analyzed using defined correlation rules. The decisive factor for the effectiveness is the performance of the analysis. The goal is to reduce the "Detection Time" and the "Reaction Time". To ensure that the relevant spectrum of possible attacks is covered, the MITRE&ATT&CK framework for ICS provides a useful framework here as well. It allows possible attack vectors to be included in the security analysis in a structured manner.

The UEBA method, on the other hand, unlike Realtime Correlation, relies on establishing a baseline. This baseline consists of a statistically determined representation of the OT system, the behavior and the interaction of the components in normal operation. It is important for detecting deviations from normal operation. UEBA has two advantages: First, the system learns independently and can therefore react to attacks that are not yet stored in correlation rules. On the other hand, attacks on OT systems can also involve system interactions that are not problematic in themselves. UEBA recognizes these in their time or frequency as a deviation from the baseline. UEBA is a relatively new approach in IT security, which companies often tackle as the next evolutionary step after real-time analysis. For OT security, however, the opposite approach is recommended: OT systems are designed to repeat activities, production or process steps. This makes it easier to find anomalies, i.e. deviations from the baseline. The basic prerequisite for UEBA - based on machine learning - is cleansed data.

Solutions for OT security monitoring

Detecting cyberattacks in real time requires security software backed by strong security analytics: ArcSight, for example, has the connectors to connect OT systems - both modern log sources and aged subsystems. All connectors bring data to a consistent format as a basis for further analysis. Log data is stored in a log database with built-in analytics; both forensics and real-time correlation and UEBA can then be performed on a common, consistent database. A solution such as ArcSight Intelligence, through the use of machine learning, enables the detection of deviations from regular operations, thus securing OT after only a few days of independent learning. Targeted analysis of attack vectors can be performed with ArcSight Detect; here, the tactics and methods documented in the MITRE&ATT&CK-ICS framework are applied.

As a result, the OT system is sustainably protected against cyberattacks. Since the data is now available in a consistent and cleansed form, it can also be used for other purposes, such as predictive maintenance or optimization of the overall system. After all, not every deviation indicates a cyberattack; in isolated cases, it may also be evidence of the failure of individual components. If you do not have the capacity to manage OT security monitoring yourself, you can also use a SaaS solution or have OT security provided as a managed service.

Conclusion

OT Security is becoming more and more complex due to new technologies, Internet 4.0 and Machine Learning. This makes it necessary to network systems that originate from different times and to standardize data in order to be able to perform systematic monitoring. The prerequisites are asset inventory, risk analysis and central logging. Procedures such as real-time correlation and UEBA can then be used to ensure the highest possible OT security level for manufacturing plants and infrastructure components, for example.

Authors: Felix Gutjahr, Cyber Defense Consultant SECUINFRA

Marcel Röhrl, Portfolio Sales Specialist - NextGen Security Operations, MicroFocus

Further Information: https://www.secuinfra.com/en/techtalk/ot-security-today-and-in-the-future-how-to-secure-kritis/

Press contact:

SECUINFRA GmbH
Svenja Koch
Stefan-Heym-Platz 1
10367 Berlin
Deutschland
Tel. +49 (0) 160 921 633 44
svenja.koch@secuinfra.com