Properly securing operation technology (OT) and IoT

Cybersecurity

Cybercriminals have found lucrative targets in IoT and OT. Most companies are not prepared to face this threat. A structured approach helps to minimize risks.

By Christian Koch, NTT Data

Attacks on water supply systems, manipulated mixing ratios of drugs at pharmaceutical companies, outages of public transport display boards: Hackers are increasingly discovering operational technology (OT) and the Internet of Things (IoT) as a lucrative target for attacks. While most people now know that they shouldn't click on dubious emails full of spelling errors, machines and systems are often unprotected.

For a long time, cybercriminals had no interest in OT because production plants or supply systems for electricity, water, and gas were not connected to other IT systems, so they could hardly cause any damage. Most of the time, attacks were just too complex to warrant the effort.

Interconnected production entices criminals

The manufacturing industry is digitizing its business processes along the entire value chain, from virtualization in the product creation process and more flexible service and business models to new manufacturing processes such as additive manufacturing. The risk of malware and cyberattacks is increasing as a result of the interconnectivity of production plants and machines with internal systems for production control or, increasingly often, with the cloud. In the process, cybercriminals try to disrupt a plant and extort a ransom or obtain trade secrets on behalf of mostly foreign competitors or countries. Then, months later, copies of car spare parts turn up that not even a service technician can distinguish from the original.

The fact that OT security lags so far behind security in IT is due to the fact that OT is planned by engineers who have to implement technical production requirements under cost pressure and in a short time, but for whom cybersecurity was rarely an issue in the past. They developed a plant purely according to functional aspects. When new cybersecurity risks arise, the plant's software would have to be patched. But the conditions in OT are less than ideal. Never touch a running system applies even more in OT than in IT. There is usually no time to apply patches either. Even if the update only takes a few minutes, it can bring an entire production line to a standstill and result in a lengthy restart, especially since functional tests are usually also necessary. Consequently, companies have to leverage regularly scheduled maintenance windows, but these are rare. In chemical production plants, for example, it can take several years before the opportunity arises for an update including all functional tests.

What to do

The starting point for better OT security is greater visibility in OT networks. Often, companies don't even know what components they have in the systems, what software versions they use, what data they exchange, and what connections exist to external companies. However, you can't protect what you don't know. Knowing the software versions in use, communication relationships, external access, zoning in the network, and much more is the basis of any cybersecurity strategy.

Network segmentation is often the first recommended measure to take. This involves separating parts of a system from other systems according to risk level and criticality. For this approach to succeed, the detailed structure and communication of the systems must be known. It is also advisable to separate legacy systems, which can sometimes be decades old and for which updates are no longer available, from new parts and to apply separate security strategies. However, it is not only the manufacturer and operator of a system who are required to ensure a high level of security; the maintenance staff must also be on board. In the case of remote maintenance, they usually access a jump server via a VPN connection. From time to time, hackers use such connections to plant malware and spyware that can then infect entire plants and facilities, especially if access to the jump server or VPN authentication is only weakly protected. To mitigate such risks, a better architecture is needed. Some security service providers recommend an audit for this purpose with a penetration test, which should reveal vulnerabilities in the IT and OT infrastructure. You will probably find plenty of vulnerabilities, but the gain in knowledge is low, especially if no security has been implemented in the OT systems. It is much better to implement measures first and then evaluate them with an audit.

Many companies asking for OT security support have already had a security incident or know companies in their industry that have. Awareness has increased in recent years and companies are motivated to do more for security. However, they often feel overwhelmed and don't know where to start. What is needed here is a structured approach that provides the company with orientation.

Christian Koch, Vice President Cybersecurity and Lead of IoT/OT at NTT Data.

Please also have a look at our community info entry

NTT DATA
Trusted Global Innovator