EU directive NIS2:
Open source is the key to success

The EU is increasing the pressure: With the NIS2 directive, significantly more companies will be included in the area of critical services while at the same time, cybersecurity requirements will increase. Companies should prepare for implementation now. Open source technology can help achieve the cybersecurity goals.

Cyberattacks and business disruptions are among the world's most serious business risks. In response to the rising number of attacks, the European Union has strengthened regulatory requirements for cybersecurity and adopted the NIS2 directive in December 2022.

This framework applies to companies in particularly critical industries and prescribes a strict defense against cyberattacks. Management is explicitly involved in the process.

The member states must have converted the directive into national law by October 2024. Even if companies still have some time left, they should prepare for implementation now, because the regulations are extensive.

Holistic safety required

The first version of the NIS directive was launched in 2016. At that time, the focus was strongly on IT security. But in the meantime, the framework conditions for cybersecurity have changed significantly. With digitalization, many industrial systems have been networked that previously had no connection to the Internet and were not even intended to do so.

Networking opened up these OT systems and now they communicate with each other or with the cloud. Every interface or every Internet-enabled component thus becomes a potential gateway for attackers from the net.

The EU has taken this development into account in NIS2 and created regulations that include the entire company.

Cybersecurity becomes a top priority

A range of technical measures is intended to establish the basis for enhanced cybersecurity. For example, NIS2 requires at least the encryption of data and information, vulnerability management and consistent access control.

However, these tools are not sufficient to achieve an adequate level of security, as attack methods are also becoming more and more sophisticated. The chatbot ChatGPT, for example, can be used to compose texts that are hardly any different from those written by a human. This makes it even harder to detect phishing emails that try to tempt their readers to open an attachment infected with malware.

That‘s why it‘s important to constantly monitor traffic to determine the normal condition. If an attacker has managed to get beyond the firewall, an intrusion detection system (IDS) can detect possible irregularities, such as a higher data transfer. An intrusion prevention system (IPS) can then stop the attack. Deep packet inspection (DPI) is also gaining in importance. This tool analyzes data packets sent over a network, down to the user level, to detect and categorize protocols and applications.

In addition to technical defense mechanisms, a whole range of organizational measures will become mandatory. Companies are required to establish risk management, set up emergency plans and regularly train their employees in IT security. This means that management can no longer assign responsibility for cybersecurity exclusively to the IT department, but will be held accountable itself.

It is also becoming important to include the supply chains, since attacks with serious consequences are possible via suppliers or the systems of other companies. In this context, certifications for the reliability of systems and components will play a central role, and the EU has called the member states to define suitable industry standards for certification.

Which standards exactly will come into question has thus not yet been determined. In automation, component developers and integrators are already successfully using IEC 62443. This series of standards for the safety of industrial communication networks therefore has a good chance of becoming established in the field of automation and can already serve as a guide.

Advantage Open Source Technology

Now that significantly more companies are affected by the NIS2 directive, many have to deal with the extensive regulations for the first time and retrofit existing industrial systems. Since the lifecycle for OT systems is significantly longer than in IT, many companies have a very heterogeneous infrastructure that must be networked and now also secured.

IT security tools based on open source technology have a clear advantage in this situation. Literally, the NIS2 directive states: “Open-source cybersecurity tools and applications can contribute to a higher degree of openness and can have a positive impact on the efficiency of industrial innovation. Open standards facilitate interoperability between security tools, benefitting the security of industrial stakeholders.”

Open source technology makes it possible to use open communication standards and thus offers a good solution for networking and securing heterogeneous infrastructures. This gives companies the necessary flexibility and keeps them open to future innovations without making them dependent on individual manufacturers.

Further, the NIS2 states: “Policies promoting the introduction and sustainable use of open-source cybersecurity tools are of particular importance for small and medium-sized enterprises facing significant costs for implementation, which could be minimized by reducing the need for specific applications or tools.”

Many companies have already purchased new hardware for networking as part of the digitization process. Replacing it completely due to the NIS2 security regulations would be a huge financial burden. Open source technology can help here as well: Endian, for example, offers an IoT security gateway as a software version. With this Endian 4i software, any industrial PC and any IoT gateway (x86) can be turned into a complete security solution. This makes it easy to continue using existing hardware.

Open source also offers advantages beyond cybersecurity: Individual enterprise applications can be used via Docker container technology or third-party applications can be integrated. This allows devices and machines to be monitored and their data analyzed for process optimization.

Significantly more companies affected

Not only the regulations are increasing. Compared with the original directive, the number of companies included in the scope of critical services is also growing. In total, the NIS2 directive covers 18 sectors and distinguishes between “Essential Entities” and “Important Entities.” A complete list can be found here.

Essential Entities include large companies in energy, transportation, banking, finance, healthcare, drinking water, wastewater, digital infrastructure, ICT service management in the B2B sector, aerospace, and public administration sectors.

The important economic sectors (“Important Entities”) are composed of seven areas, which are postal and courier, waste, chemicals, food, manufacturing, digital services and research institutes.

The size regulation is also new: Thus, medium and large companies with 50 or more employees or 10 million euros in sales are affected, regardless of the performance or thresholds of their facilities. For some operators, even company size no longer plays a role, as in parts of the digital infrastructure or public administration.

The fact is that NIS2 includes significantly more companies than the current NIS rules. Estimates put the number of additional companies in Germany alone at up to 40,000.

Severe sanctions

Violations of the guidelines as well as the reporting requirements are subject to severe penalties. Up to 10 million euros or 2 percent of global sales can be due if an organization fails to meet its obligations. This shows that the EU will in future attach the same importance to cyber security as it does to data protection.

Despite the harsh penalties and extensive obligations, the NIS2 represents progress overall. Because only if all companies take cybersecurity seriously can the threat be contained in the future. And ultimately, the companies themselves will benefit from this.