Ready for the NIS2? Deadlines are set in Hungary

Hungary has fully implemented the EU NIS2 Directive (2022/2555) through its Cybersecurity Act (Act LXIX/2024), which came into force on January 1, 2025. For manufacturers, this marks a turning point: cybersecurity is no longer optional—it's a legal obligation.

And it's not just about traditional IT. Full auditability is now required across your entire digital infrastructure—including operational technology (OT) like SCADA and PLC systems. The NIS2 Directive aims to significantly strengthen cybersecurity in critical and important sectors, and manufacturing is front and center.

NIS2 Audit Timeline in Hungary

Registered by 2024

- First mandatory cybersecurity audit must be completed by December 31, 2025.

Registered from 2025

- A contract with an accredited auditor must be signed within 120 days of registration.

Hungary expanded NIS2's scope from 600 to over 7,500 companies—yet over 70% still lack a dedicated implementation budget.

2016	2018	2020	2022	2023	2024	2025
NIS resolution	NIS became effective	NIS2 proposed	NIS2 resolution	NIS2 in force	Transposition into national law	Hungary: NIS2 fully implemented. > First audits by 31 Dec 2025.

Companies in manufacturing will be audited in the following areas:

1. **System classification:** IT and OT systems must be categorized in security classes (basic, significant, high).
2. **Risk management:** Existence of security measures, risk analyses, emergency plans.
3. **OT security:** Protection of SCADA, PLC and ICS systems is explicitly checked.
4. **Incident response:** Reporting processes and ability to respond to security incidents.
5. **Governance:** Appointment of a qualified security officer, involvement of management.
6. **Audit verification:** Performance of a certified audit every two years—with report to the SZTFH.

What are the Consequences of Non-Compliance?

Fines up to HUF 15 million

Per violation. Repeated or systemic failures may lead to even harsher penalties.

Operational shutdowns

Authorities can partially or fully suspend operations if critical vulnerabilities are not addressed.

Forced system shutdowns

IT and OT systems can be taken offline immediately by regulatory order if deemed insecure.

Reputational damage

Violations may be made public. The resulting loss of trust from customers and partners can be irreversible.

Executive liability

Even in cases of ignorance. In severe cases, executives may face a professional ban of up to 5 years.

NIS2 is now in full effect, and manufacturers in Hungary must act without delay. Begin by registering properly, appointing a cybersecurity officer, and implementing a risk management system for OT environments and OT related IT equipment. Don't wait—discover how octoplant and AMDT can help you stay compliant, resilient, and audit-ready.

AMDT is the global market and technology leader for versioning and backup solutions in industrial automation. With its octoplant software platform, the company secures the automation of production processes through strong end-point management, where it consistently records and monitors changes to configurations, programming and project statuses in production. This minimizes downtime, increases efficiency, quality and safety standards, and saves costs as well as resources. As a modular solution, octoplant can be linked to different automation technologies and devices, regardless of the manufacturer.

More Information at: amdt.com