CYBERSECURITY 101 · eBuilder Security

NIS2

NIS2 is the EU cybersecurity law now in force in Sweden as Cybersäkerhetslagen. Here is who it covers, what it requires and the one habit that keeps you ready.

WHAT IT IS

NIS2 is the European Union's main cybersecurity law, Directive (EU) 2022/2555. It sets a common baseline of security measures and incident-reporting duties for organisations that run important services across 18 sectors. In Sweden it applies as Cybersäkerhetslagen, and it now carries real fines and personal accountability for company boards.

WHY IT MATTERS

€10M or 2%

Maximum fine for an essential entity, of global annual turnover, whichever is higher.

NIS2 Directive, Article 34

24 hours

To file an early warning with the authority after becoming aware of a significant incident.

NIS2 Directive, Article 23

164 municipalities

Directly hit through one HR-software supplier in the 2025 Miljödata attack, out of Sweden's 290.

Swedish authorities, 2025

WHAT HAPPENED

In January 2024 the Akira ransomware group hit a Swedish datacentre run by the IT supplier Tietoevry. The outage took down the Primula payroll system used by most Swedish universities and more than 30 government authorities, and knocked the cinema chain Filmstaden and the retailer Rusta offline for days. One supplier failing rippled across the country. (Tietoevry, 2024)

RED FLAGS TO WATCH FOR

NIS2 exposure usually shows up as gaps in ownership and preparation.

- No one at board level owns NIS2 or has had the training Article 20 requires.
- You cannot quickly list the suppliers your critical services depend on.
- You have no tested process for filing an incident report within 24 hours.
- Backups and recovery have never been tested against a real outage.

THE ONE RULE THAT STOPS IT

Give NIS2 a named owner on the board and run it as a continuous programme, keeping scope, measures and reporting current between audits.

THEN BUILD THE HABIT AROUND IT

- Confirm your scope and whether you are an essential or important entity, then register with MCF.
- Run a gap assessment against the ten Article 21 measure areas.

- Map your critical suppliers and add security terms to their contracts.
- Rehearse a 24-hour incident-reporting runbook with a named owner and a deputy.

MYTHS AND FACTS

MYTH

NIS2 is only for big utilities and national infrastructure.

FACT

It covers medium-sized and larger organisations across 18 sectors, and reaches their suppliers through contracts.

MYTH

Cybersecurity is an IT problem the board can delegate.

FACT

Article 20 makes the board approve and oversee the measures, take training and accept personal liability.

MYTH

ISO 27001 certification means we already meet NIS2.

FACT

It helps a great deal but is not equivalent. NIS2 still checks your scope, reporting readiness and board involvement.

THE LEGAL DUTY

NIS2 is now law in Sweden as Cybersäkerhetslagen (2025:1506), in force since 15 January 2026. Boards are personally accountable under Article 20, and fines reach €10 million or 2% of global turnover.

GET HELP

eBuilder Security helps Swedish organisations turn NIS2 duties into working controls, from board readiness to incident response and training. Read the full guide below.

Read the Full Article →