CYBERSECURITY 101 · eBuilder Security

Cybersäkerhetslagen

Sweden's NIS2 law has been in force since 15 January 2026. Here is who it covers, what it asks of you and where to start.

WHAT IT IS

Cybersäkerhetslagen is the Swedish law that puts the EU NIS2 directive into force. It sets binding cybersecurity duties for organisations that run important services and makes the board answerable for meeting them. It reaches far more organisations than the old NIS law, and public bodies are firmly in scope.

WHY IT MATTERS

15 Jan 2026

The date Cybersäkerhetslagen (SFS 2025:1506) came into force in Sweden.

Regeringskansliet, 2025

18 sectors

Now in scope, up from 7 under the old NIS law, from energy to public administration.

NCSC, 2026

10M euro or 2%

Maximum fine for an essential operator, the higher of the two. Public bodies up to 10M kronor.

Cybersäkerhetslagen 10 §

WHAT HAPPENED

In August 2025 a ransomware group hit Miljödata, a supplier whose HR systems are used by around 80 percent of Sweden's municipalities. Around 200 of Sweden's 290 municipalities and regions were affected and sensitive HR and health data was exposed. One shared supplier became a national incident. (SVT, 2025)

RED FLAGS TO WATCH FOR

Non-compliance is not only about incidents. Watch for these gaps.

- No clear owner for cybersecurity on the board.
- No incident-reporting runbook mapped to the 24-hour and 72-hour deadlines.
- Suppliers with no security requirements in their contracts.
- Backups that have never been tested.
- No record that you have registered with the supervisory authority.

> THE ONE RULE THAT STOPS IT
>
> **Treat the Article 21 security measures and the 24-hour reporting duty as live obligations now, not a project for later.**

THEN BUILD THE HABIT AROUND IT

- Run a gap assessment against the Article 21 measures.

- Give the board a named owner for cybersecurity.
- Write and rehearse an incident-reporting runbook.
- Add security requirements to every supplier contract.
- Train management and staff, and keep the evidence.

MYTHS AND FACTS

MYTH

Cybersäkerhetslagen only applies to big companies.

FACT

It also covers municipalities, regions and most public authorities regardless of size, and private firms from 50 staff or 10 million euro in turnover.

MYTH

Cybersecurity is the IT department's problem.

FACT

The law puts approval and oversight on the board, and senior managers can be held personally accountable.

MYTH

We still report incidents to MCF.

FACT

Since 1 July 2026 significant incidents go to NCSC through CERT-SE. MCF's cyber functions moved to NCSC within FRA.

THE LEGAL DUTY

Cybersäkerhetslagen (SFS 2025:1506) put the EU NIS2 directive into force in Sweden on 15 January 2026. The board is accountable, and fines reach the higher of 2 percent of global turnover or 10 million euro for essential operators.

GET HELP

eBuilder Security helps Swedish organisations prepare for Cybersäkerhetslagen, from risk-management measures and incident-reporting readiness to security awareness training.

Read the Full Article →