CYBERSECURITY 101 · EBUILDER SECURITY

Ransomware

Criminals lock your systems, steal your data and charge you to get your business back. Here is how it happens, and the controls that decide whether you recover.

WHAT IT IS

Ransomware is malicious software that locks an organisation out of its own systems and data, usually by encrypting files, until a ransom is paid. Most modern gangs steal the data first and threaten to publish it, so an attack is an outage, a data breach and a public extortion campaign at once. The note appears in minutes, but the criminals have usually been inside for weeks.

WHY IT MATTERS

44% of breaches

Involved ransomware in 2025, up from 32% the year before. Among small and medium businesses it was 88%.

Verizon DBIR, 2025

1.53 million dollars

Mean cost of recovering from an attack, excluding any ransom paid.

Sophos, 2025

28% paid

The share of victims who paid in 2025, an all-time low. Recovery without paying is the norm.

Chainalysis, 2026

WHAT HAPPENED

In August 2025 attackers hit Miljödata, the HR supplier used by about 80% of Swedish municipalities. Roughly 200 of Sweden's 290 municipalities and regions lost systems in one weekend, and when the 1.5 bitcoin demand was refused, data on more than 1.5 million people was published on the darknet. (Swedish Prosecution Authority, 2025)

RED FLAGS TO WATCH FOR

The ransom note is the end of the attack. The warning signs come in the quiet weeks before it.

- New administrator accounts, or accounts suddenly gaining privileges.
- Security tools switched off, reconfigured or uninstalled.
- Backup jobs failing, or snapshots and shadow copies being deleted.
- Unusually large outbound data transfers to unfamiliar destinations.

> THE ONE RULE THAT STOPS IT
>
> **Keep one tested backup copy offline, out of reach of an attacker with admin rights, and never pay the ransom.**

THEN BUILD THE HABIT AROUND IT

- Patch internet-facing systems, VPNs and backup servers within days, not months.
- Enforce multi-factor authentication on every remote login and admin account.
- Rehearse the incident plan, including manual fallbacks and who notifies MCF, Polisen and IMY.

- Put patching, MFA and breach-notification duties into every supplier contract.

MYTHS AND FACTS

MYTH Ransomware only hits big companies.

FACT Verizon's 2025 report found ransomware in 88% of breaches at small and medium businesses, against 39% at large enterprises. Thinner defences make smaller organisations the easier pick.

MYTH Paying the ransom ends the incident.

FACT CERT-SE warns there is no guarantee systems are restored, files are decrypted or the attacker will not return with new demands. Payment also marks you as a payer.

MYTH Good backups make you immune.

FACT Backups end the outage, not the extortion. Most gangs steal data before encrypting, and they hunt backup servers first, so copies must be offline and tested.

THE LEGAL DUTY

Under NIS2, in force in Sweden as Cybersäkerhetslagen since 15 January 2026, covered organisations must report a significant incident to MCF (formerly MSB) within 24 hours, and boards are personally accountable under Article 20.

GET HELP

eBuilder Security provides managed detection and response and security awareness training from Sweden. Read the full guide at the link below.

ebuildersecurity.com/cybersecurity-101/ransomware-101