THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Ransomware - when the whole company grinds to a halt

Ransomware attacks paralyse organizations for days and cost an average of six figures - even without paying the ransom. We show which entry points are most common and why backups alone are not enough.

min read: 9 min **Updated:** 14 March 2026 **Risk:** Very high risk
Source: awareness-as-a-service.com/en/resources/threats/ransomware

What is ransomware?

Ransomware is malicious software that encrypts files or entire systems and supposedly releases them only after payment of a ransom. In practice, the picture is more complex: modern ransomware groups operate so-called **double extortion** - they exfiltrate data before encrypting it, then threaten publication even if the ransom is paid.

Ransomware attacks are not random events. Behind most major campaigns are professional criminal organizations that purchase access to corporate networks from Initial Access Brokers, systematically exploit vulnerabilities, and move undetected through networks for weeks before striking. The encryption itself is often the final link in a long chain.

Consequential costs regularly exceed the ransom by multiples: operational downtime, forensics, system restoration, reputational damage, and regulatory consequences. The BSI estimates that organizations hit by a serious ransomware attack take an average of several weeks to fully restore operations.

At a glance

01

Weeks, not hours

The average recovery time after a full ransomware attack is several weeks - backups alone are rarely sufficient for a rapid return to normal operations.

02

Double extortion is standard

Data is exfiltrated before encryption. Even after paying the ransom, the risk of publication remains.

03

Phishing is the most common entry point

Compromised credentials and phishing emails that download malware are the most frequent initial access routes - ahead of unpatched vulnerabilities and RDP brute-force.

How to recognise ransomware

Ransomware rarely announces itself directly - the preparation phase is almost invisible to users. These signals may indicate an active or imminent attack:

Unusual file operations
Mass renaming or encryption of files by an unknown process - often recognisable by new file extensions (.locked, .encrypted, random characters).

Unknown admin accounts
New local administrator accounts or unfamiliar accounts in Active Directory are a strong indicator of active compromise.

RDP brute-force attempts
Mass failed RDP login attempts in the logs signal access attempts that can precede ransomware deployment.

Database or file server unexpectedly offline
Systems going offline or becoming unreachable without an obvious reason may indicate ongoing encryption.

Security tool disabled
When antivirus, EDR, or firewall logs go silent or services are stopped, an attacker may be clearing obstacles.

Unexpected network traffic
Large volumes of data flowing to external IP addresses at night or over weekends may signal exfiltration.

How to protect yourself

For employees

- **Do not open phishing links or attachments** - ransomware frequently enters the network through a phishing email.
- **No personal USB sticks or storage media** on company computers.
- **Report unusual system behavior immediately:** Processes starting unexpectedly, sudden slowness, unknown file extensions.
- **Do not bypass security warnings:** If a browser or operating system warns about a website or file, take the warning seriously.

For administrators

- **Offline backups (3-2-1 rule):** Three copies, two different media types, one offline/air-gapped. Regularly test backups for recoverability.
- **Network segmentation:** Isolate critical systems (production control, accounting, backups) in separate segments with strict firewall rules.
- **Harden or disable RDP:** No RDP directly exposed to the internet; mandatory MFA; ideally only accessible via VPN or a jump host.
- **Prioritise patch management:** Known, exploited vulnerabilities (CISA KEV list) should be patched within 24–72 hours.
- **Deploy EDR/XDR:** Behaviour-based detection recognises ransomware-typical patterns (mass encryption, LSASS dump) at an early stage.

Real cases

CASE 01 · HOSPITAL · DE · Q3/2025

A ransomware group infiltrated a hospital through an unpatched VPN vulnerability. Three weeks after the initial access, attackers encrypted patient records, laboratory systems, and the PACS. In-patients had to be transferred to other facilities.

Damage: weeks of reduced operations, forensics and restoration cost EUR 1.2 million · **Ransom:** not paid · **Lesson:** VPN appliances are preferred entry points - patches must follow within hours, not weeks.

CASE 02 · FREIGHT FORWARDER · CH · Q4/2025

A phishing email with a fake customs invoice dropped a loader that remained dormant for weeks. After fully mapping the network, LockBit ransomware was deployed. The dispatch system, booking systems, and email server were completely down for three days.

Damage: CHF 320,000 in operational losses, customer attrition · **Ransom:** CHF 180,000 demanded, not paid · **Lesson:** Offline backups ultimately enabled recovery - but the operational disruption was still substantial.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Disconnect affected systems from the network immediately** (unplug cables, disable Wi-Fi) - without shutting them down. Running processes may be forensically valuable.
2. **Do NOT pay without consulting experts.** Payment does not guarantee decryption and funds further attacks. Consult law enforcement and forensic specialists first.
3. **Activate the crisis team:** IT Security, management, legal, and cyber insurance carrier.
4. **Notify authorities:** In Germany, report to BSI (critical infrastructure) and state police; in Switzerland, to the NCSC. Reporting protects against accusations of concealment.
5. **Forensic preservation:** RAM dumps and log preservation before restoration - for law enforcement and insurance claims.
6. **Coordinate communications:** Notify customers, suppliers, and authorities proactively - after legal review. No immediate social media statements.

Frequently asked questions

Should you pay the ransom?

Generally, no. Payment does not guarantee full decryption, can trigger further demands, and funds criminal operations. Exceptions are only conceivable in extreme circumstances (e.g. immediate threat to life) and only after consulting law enforcement. Insurance may cover payment - but that is not a recommendation.

Why are backups alone not enough?

Because restoration takes time - hours to days for a full restore. Because attackers often delete or encrypt backups if they are not cleanly isolated. And because exfiltration remains a problem regardless of backup status.

What are indicators of compromise (IOCs) for ransomware?

New admin accounts, disabled security tools, unusual outbound traffic, LSASS dump activity, unknown processes, Cobalt Strike beacons, lateral movement in Active Directory.

Must I report a ransomware attack?

In the EU, NIS2 reporting obligations apply to critical infrastructure and important entities (72 hours). In Switzerland, sector-specific obligations exist and from 2025 an NCSC reporting obligation applies to critical infrastructure operators. Regardless of legal requirements, early reporting accelerates assistance.

Related topics

Ransomware is frequently the final link in a chain that begins with phishing or compromised credentials. Insider threats and unsecured cloud services create the attack surface that ransomware groups exploit.