

Digitization

Cybercrime: ***Increase in ransomware attacks***

16.10.2025

At a glance

A wave of ransomware from a hacker group is rolling across Switzerland. The federal authorities are issuing an urgent warning about attacks, especially because attacks on companies are on the rise.

- Over 200 companies have been affected since 2023 - with damage running into millions.
- There are currently four to five attacks per week - a sad record for Switzerland.
- No company is too small: cyber criminals are targeting unprotected vulnerabilities.

The federal authorities warn: A hacker group is currently intensifying its activities in Switzerland - the authorities are currently registering 4-5 attacks per week. Around 200 Swiss companies have already fallen victim to these ransomware attacks. The damage amounts to several million Swiss francs - several hundred million worldwide.

Protect yourselves - no one is too small or too big to become a target

This warning concerns us all. Recent developments clearly show that no company is too small to become a target. Cyber criminals make no distinction between large corporations and SMEs. They look for vulnerabilities - and find them where protective measures are lacking or have been neglected.

Since 2023, over 200 Swiss companies have fallen victim to such attacks. Ransomware is no longer a marginal phenomenon. A single attack can bring an entire business activity to a standstill within hours. Production interruptions, loss of business-critical data, threats to supply chains - the effects extend far beyond the IT sector. Cybercrime is therefore not just a technological risk, but also a business and strategic risk.

Company responsibility: Preparation is key

For businesses, one thing is clear: prevention starts within the company itself. Those who do not protect their digital infrastructure are exposed to a growing risk. You don't need a specialist department to take basic measures, but you do need a clear awareness at management level.

Essential elements of cyber resilience are:

- System maintenance and updates - outdated access points are one of the most common gateways.
- Backup and emergency plans - backed up offline, tested and retrievable in an emergency.
- Multi-factor authentication - simple step, big impact.
- Employee awareness - people often remain the weakest link.

Cybercrime is not a technology problem. It is a management task

Those who invest in digital security today will protect their customers, supply chains and reputation tomorrow, as well as Switzerland as a business location as a whole.

For further information on the topic of ransomware incidents and how to protect yourself, the Swiss Insurance Association has published a guide.

Further information from the federal government can be found here.

Angela Anthamatten
Deputy Head of Department Competition & Regulatory Affairs

David Stauffacher
Project Manager infrastructure and digital