

Digitalisierung

Cyberkriminalität: ***Zunahme von Ransomware-Angriffen***

16.10.2025

Auf einen Blick

Eine Ransomware-Welle einer Hackergruppe rollt über die Schweiz. Die Bundesbehörden warnen eindringlich vor Angriffen, vor allem weil Angriffe auf Unternehmen zunehmen.

- Über 200 Unternehmen sind seit 2023 betroffen – mit Schäden in Millionenhöhe.
- Derzeit gibt es vier bis fünf Attacken pro Woche – ein trauriger Rekord für die Schweiz.
- Kein Unternehmen ist zu klein: Cyberkriminelle zielen auf ungeschützte Schwachstellen.

Die Bundesbehörden warnen: Derzeit intensiviert eine Hackergruppe ihre Aktivitäten in der Schweiz –die Behörden registrieren im Moment 4-5 Angriffe pro Woche. Bisher sind bereits rund 200 Schweizer Unternehmen Opfer dieser Ransomware-Angriffe geworden. Der Schaden beläuft sich auf mehrere Millionen Schweizer Franken – weltweit auf mehrere hundert Millionen.

Schützt euch – niemand ist zu klein oder zu gross, um Ziel zu werden

Diese Warnung betrifft uns alle. Die jüngsten Entwicklungen zeigen klar: Kein Unternehmen ist zu klein, um Ziel zu werden. Cyberkriminelle machen keinen Unterschied zwischen Grosskonzernen und KMU. Sie suchen nach Schwachstellen – und finden sie dort, wo Schutzmassnahmen fehlen oder vernachlässigt wurden.

Seit 2023 wurden über 200 Schweizer Unternehmen Opfer solcher Angriffe. Ransomware ist längst kein Randphänomen mehr. Ein einziger Angriff kann innert Stunden die gesamte Geschäftstätigkeit zum Stillstand bringen. Produktionsunterbrüche, Verlust geschäftskritischer Daten, Gefährdung von Lieferketten – die Auswirkungen reichen weit über den IT-Bereich hinaus. Cyberkriminalität ist damit nicht nur ein technologisches, sondern ein betriebswirtschaftliches und strategisches Risiko.

Verantwortung der Unternehmen: Vorbereitung entscheidet

Für die Wirtschaft ist klar: Prävention beginnt im Unternehmen selbst. Wer seine digitale Infrastruktur nicht schützt, ist einem wachsenden Risiko ausgesetzt. Es braucht keine Spezialabteilung, um grundlegende Massnahmen zu ergreifen, wohl aber ein klares Bewusstsein auf Führungsebene.

Wesentliche Elemente der Cyber-Resilienz sind:

- Systempflege und Updates – veraltete Zugänge sind eines der häufigsten Einfallstore.
- Backup- und Notfallpläne – offline gesichert, getestet und im Ernstfall abrufbar.

- Multi-Faktor-Authentifizierung – einfacher Schritt, grosse Wirkung.
- Sensibilisierung der Mitarbeitenden – der Mensch bleibt oft das schwächste Glied.

Cyberkriminalität ist kein Technologieproblem. Es ist eine Führungsaufgabe

Wer heute in digitale Sicherheit investiert, schützt morgen Kunden, Lieferketten und Reputation sowie den Wirtschaftsstandort Schweiz insgesamt.

Für weitergehende Informationen rund um das Thema Ransomware Vorfällen und wie man sich schützen kann, hat der Schweizerische Versicherungsverband einen Leitfaden publiziert.

Weiterführende Informationen des Bundes finden sich hier.

Angela Anthamatten
Stv. Bereichsleiterin Wettbewerb & Regulatorisches

David Stauffacher
Projektleiter Infrastruktur und Digitales