SOPHOS

RANSOMWARE-REPORT SCHWEIZ 2026

Ergebnisse einer unabhängigen Befragung von 79 Schweizer Unternehmen, die im vergangenen Jahr von Ransomware betroffen waren.

SOPHOS-WHITEPAPER – JULI 2026

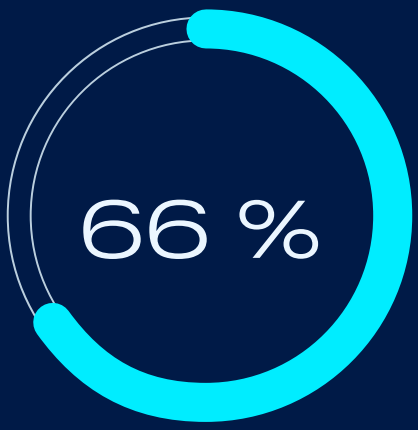
Über den Report

Der State of Ransomware Report, der nun im siebten Jahr erscheint, basiert auf den Ergebnissen einer unabhängigen Studie, die von Sophos in Auftrag gegeben wurde. Der diesjährige globale Report beruht auf den Erfahrungen von 2.158 IT- und Cybersecurity-Führungskräften, deren Unternehmen im vergangenen Jahr von Ransomware betroffen waren, darunter 79 aus der Schweiz.

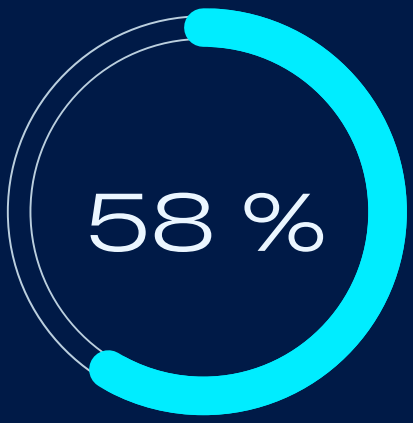
Die Umfrage wurde zwischen Januar und März 2026 durchgeführt. Die Befragten arbeiten alle in Unternehmen mit 100 bis 5.000 Mitarbeitenden und wurden gebeten, die Fragen basierend auf ihren Erfahrungen der letzten 12 Monate zu beantworten. Alle Finanzdaten sind in US-Dollar angegeben. Ausreißerwerte bei den Lösegeldforderungen ab 40 Mio. US$ wurden aus diesen Daten entfernt.

Erfahrungen von 79

IT-/Cybersecurity-Entscheider aus der Schweiz, deren Unternehmen im vergangenen Jahr von Ransomware betroffen waren



Prozentsatz der Angriffe, die zur Verschlüsselung von Daten führten.



Bestätigten, dass der Ransomware-Vorfall des vergangenen Jahres ihr bedeutendster Identitätsangriff war.

Durchschnittliche Wiederherstellungskosten nach einem Ransomware-Angriff

Gründe, warum Schweizer Unternehmen Opfer von Ransomware werden

- **Schädliche E-Mails waren die häufigste technische Angriffsursache** und wurden bei 29 % der Angriffe eingesetzt, gefolgt von kompromittierten Anmeldedaten (24 %) und ausgenutzten Schwachstellen (22 %). Der Prozentsatz ging bei ausgenutzten Schwachstellen deutlich zurück und sank im Bericht von 2025 von 31 % auf 22 %.
- **Bekannte Sicherheitslücken (44 %) gehörten zu den häufigsten operativen Angriffsursachen** und traten am häufigsten in allen befragten Ländern auf, gefolgt von einem Mangel an Personal/Kapazitäten (43 %) und einem fehlenden Schutz (38 %).
- **(NEU) Offengelegte Anwendungen und Systeme waren der häufigste Einstiegspunkt für Angriffe (40 %)** bei Ursachen, die nicht mit E-Mails oder Phishing zusammenhängen, gefolgt von Benutzergeräten (30 %) und Firewalls (28 %).
- **(NEU) 58 % bestätigten, dass der Ransomware-Vorfall des vergangenen Jahres der bedeutendste Identitätsangriff auf ihr Unternehmen war.**

Auswirkungen auf Daten

- **66 % der Angriffe führten zu einer Verschlüsselung von Daten.** Dies liegt über dem globalen Durchschnitt von 56 % und ist ein Anstieg gegenüber den 53 %, die von Schweizer Befragten im Report von 2025 angegeben wurden.
- **60 % der Schweizer Unternehmen zahlten das Lösegeld und erhielten ihre Daten zurück.** Dies ist ein Anstieg gegenüber dem Vorjahreswert von 54 % im Report von 2025 – und der höchste Wert aller untersuchten Länder.
- **100 % der Schweizer Unternehmen, deren Daten verschlüsselt wurden, konnten sie wiederherstellen,** was dem weltweiten Durchschnitt entspricht.
- **Bei 23 % der Angriffe, bei denen die Daten verschlüsselt waren, wurden auch Daten gestohlen.** Dies ist ein Anstieg gegenüber dem Vorjahreswert von 10 % im Report von 2025.
- **77 % der Schweizer Unternehmen nutzten Backups zur Wiederherstellung verschlüsselter Daten,** ein deutlicher Anstieg gegenüber den im Report von 2025 gemeldeten 56 %.

Lösegeldforderungen

- **Die Lösegeldforderungen bei Schweizer Unternehmen lagen bei durchschnittlich 1,29 Mio. USD,** ein sehr großer Anstieg gegenüber den 328.748 USD im Report von 2025.
- **63 % der Lösegeldforderungen beliefen sich auf 1 Mio. USD oder mehr,** was ein Anstieg von 46 % gegenüber dem Report von 2025 ist.

Durchschnittliche Lösegeldforderung in der Schweiz.

Geschäftliche Folgen von Ransomware

- Ohne Berücksichtigung von Lösegeldzahlungen **beliefen sich die durchschnittlichen Bereinigungskosten für Schweizer Unternehmen nach einem Ransomware-Angriff auf 2,21 Mio. US-Dollar,** was ein deutlicher Anstieg gegenüber dem Durchschnitt von 1,04 Mio. USD im Report von 2025 ist. Dazu zählen Ausfallzeiten, Arbeitsstunden, Geräte- und Netzwerkkosten, entgangene Geschäftschancen etc.
- **59 % der Schweizer Unternehmen konnten ihr System innerhalb von bis zu einer Woche nach einem Ransomware-Angriff wiederherstellen,** was ein leichter Anstieg gegenüber den im Report von 2025 gemeldeten 58 % ist. 24 % benötigten zwischen einem und sechs Monaten zur Wiederherstellung, was ein erheblicher Anstieg gegenüber den 9 % im Report von 2025 ist – der höchste Wert aller untersuchten Länder.

Auswirkungen von Ransomware auf Mitarbeitende in IT-/Cybersecurity-Teams von Unternehmen, in denen Daten verschlüsselt wurden

44 % berichten von mehr Stress oder Angst vor künftigen Angriffen. Steigerung gegenüber 28 % im Jahr 2025.

37 % berichten von erhöhter Anerkennung aus der Führungsetage.

37 % berichten von Schuldgefühlen, weil der Angriff nicht gestoppt wurde.

37 % berichten von Fehlzeiten aufgrund von Stress/psychischen Gesundheitsproblemen.

13 % berichten, dass die Teamführung ausgetauscht wurde.

Empfehlungen

Stärken Sie die Identitätssicherheit zum Schutz vor Ransomware. Mehr als die Hälfte der von Ransomware betroffenen Unternehmen aus der Schweiz bestätigten, dass der Ransomware-Vorfall auch ihr bedeutendster Identitätsangriff war. Unternehmen und Organisationen sollten Identity Threat Detection and Response (ITDR) priorisieren, Multi-Faktor-Authentifizierung über alle Zugangspunkte hinweg durchsetzen und regelmäßig sowohl menschliche als auch nicht-menschliche Zugangsdaten prüfen.

Verstärken Sie den Endpoint-Schutz für innovative KI-Modelle. Frontier AI beschleunigt die Erkennung und Ausnutzung von Schwachstellen. Eine starke Endpoint-Abwehr, die Exploit-basierte Angriffe automatisch stoppt, ist unerlässlich.

Priorisieren Sie E-Mail-Sicherheit. Da Phishing und Schad-E-Mails beinahe die Hälfte der Ursachen für Ransomware in der Schweiz ausmachen, sollten Unternehmen und Organisationen moderne E-Mail-Filter einsetzen, DMARC-/DKIM-/SPF-Protokolle implementieren und in regelmäßige Phishing-Awareness-Trainings investieren.

Investieren Sie in Backup- und Wiederherstellungsinfrastrukturen. Unternehmen und Organisationen, die robuste Backup-Systeme unterhalten, konnten verschlüsselte Daten im vergangenen Jahr mit nahezu Rekordraten wiederherstellen. Backups sollten regelmäßig getestet, offline oder in unveränderlichen Formaten gespeichert und in einen dokumentierten Incident-Response-Plan integriert werden, der unter Druck ausgeführt werden kann.

Sie möchten mehr darüber erfahren, wie Sophos Sie bei der Optimierung Ihrer Ransomware-Abwehr unterstützen kann? Sprechen Sie mit einem unserer Ansprechpartner oder besuchen Sie **sophos.com/ransomware2026**.

Sophos bietet branchenführende Cybersecurity-Lösungen für Unternehmen jeder Größe und schützt Kunden in Echtzeit vor komplexen Bedrohungen wie Malware, Ransomware und Phishing. Bewährte Next-Gen-Funktionen mit der Power von Machine Learning und künstlicher Intelligenz sichern Unternehmensdaten effektiv.

2026-08-05 SW-WP (TA) CRE-6104