Swiss Post Cybersecurity AG
Kasinostr. 30
5001 Aarau

Telefon +41 62 834 00 55
swisspost-cybersecurity.ch

Pressemeldung

Erster Threat Landscape Report von Swiss Post Cybersecurity: vollständige Prävention nicht mehr möglich

Aarau und Morges, 8.7.2026. Die erste Ausgabe des «Swiss Threat Landscape Report» von Swiss Post Cybersecurity kommt zu einer ernüchternden Erkenntnis: Eine vollständige Prävention ist nicht mehr möglich. Organisationen müssen sich auf den nächsten Angriff vorbereiten und darum ihre Fähigkeit stärken, diesen schnell zu erkennen, darauf zu reagieren und sich davon zu erholen. Der Report bietet eine Analyse der sich wandelnden Bedrohungslage und des Zusammenspiels von externem Druck, Regulatorien und internen Anforderungen in der Schweiz.*

Unternehmen erkennen Cyberangriffe als erhebliches Geschäftsrisiko und verstehen, wie wichtig proaktive Sicherheitstests sind. Das Bewusstsein allein reicht jedoch nicht mehr aus; Unternehmen müssen ihre Fähigkeit, komplexe Angriffe zu erkennen, darauf zu reagieren und sich davon zu erholen, kontinuierlich überprüfen, so eine wichtige Erkenntnis des Reports. Die Ergebnisse dieses Berichts verdeutlichen zudem: Eine vollständige Prävention ist nicht mehr möglich. Der nächste Angriff wird kommen.

Die Analyse zeigt, dass 71 % der Befragten bereits einen Cybervorfall erlebt haben. Als am häufigsten auftretende Vorfälle wurden Malware und Ransomware sowie Phishing und Social Engineering Attacken genannt. Der Anteil der Befragten, die angaben, nicht betroffen zu sein (25 %), erscheint vergleichsweise hoch. Angesichts der zunehmenden Häufigkeit von Sicherheitsverletzungen durch Dritte, Datenlecks und ähnlichen Vorfällen ist davon auszugehen, dass einige Vorfälle unbemerkt geblieben sind oder deren Auswirkungen noch nicht erkannt wurden.

Der Bericht zeigt eine eindeutige Veränderung im Verhalten der Angreifer: Moderne Cyberangriffe stützen sich zunehmend auf Identitätsdiebstahl, Social Engineering und auf von Angreifern kontrollierte Infrastruktur statt auf rein technische Exploits. Weiter wird festgestellt, dass Cybersicherheit auf Ebene der Geschäftsführung und des VRs nach wie vor nicht ausreichend verankert ist, was zu einer **Kluft zwischen operativen Cyberrisiken und strategischer Aufsicht** führt. Eine wirksame Cybersicherheits-Governance erfordert die Einbindung in das unternehmensweite Risikomanagement sowie eine solide Grundlage in Form von Transparenz über die Unternehmensressourcen und Risikoerkennung.

Der Report identifizierte fünf oft unterschätzte Herausforderungen für Unternehmen:

1. **Abläufe und Zuständigkeiten:** Bei Vorfällen führen unklare Zuständigkeiten und Verantwortlichkeiten häufig zu Verzögerungen, internen Konflikten und ineffizienten Entscheidungsprozessen. Viele Organisationen erkennen diese Lücken erst, wenn eine Krise bereits bis hin zur Führungsebene eskaliert wurde.

2. **Mangelnde Transparenz bei der IT-Infrastruktur:** Vielen Unternehmen fehlt es an vollständiger Transparenz hinsichtlich ihrer Systeme, Identitäten, Cloud-Dienste und veralteten Geräten. Schatten-IT und nicht verwaltete Konten führen weiterhin zu erheblichen Sicherheitslücken. Unternehmen können Ressourcen, von deren Existenz sie nichts wissen, nicht wirksam schützen.
3. **Zugriffsmanagement für Service Provider:** Drittanbieter verfügen häufig über weitreichende Zugriffsrechte auf interne Systeme, während Zugriffskontrollen und das Life-Cycle-Management nach wie vor unzureichend geregelt sind. Unkontrollierte Zugriffe durch Lieferanten stellen ein wachsendes Risiko dar, insbesondere angesichts der zunehmenden Angriffe auf die Lieferkette.
4. **Angreifer und Datenlecks:** Die Zahl der Angreifer, die versuchen, an Unternehmensdaten zu gelangen, nimmt zu. Unternehmen haben häufig keinen Überblick darüber, welche Daten bei einem Vorfall kompromittiert wurden. Unzureichende Protokollierung und begrenzte Überwachung machen Untersuchungen schwierig, kostspielig und zeitaufwendig. Gleichzeitig werden gestohlene Daten zunehmend auch lange nach dem ursprünglichen Datenleck erneut veröffentlicht oder wiederverwendet.
5. **Unterschätzung des Wiederherstellungsaufwands:** Viele Organisationen unterschätzen die Komplexität und Dauer der Wiederherstellung nach einem Cybervorfall. Aufgrund betrieblicher Abhängigkeiten, forensischer Untersuchungen und Massnahmen zur Systemrestaurierung dauert die Wiederherstellung oft deutlich länger als erwartet. Cyberresilienz hängt nicht nur von der Prävention ab, sondern auch von der Fähigkeit, unter Druck effektiv wiederherzustellen.

Paul Such, CEO von Swiss Post Cybersecurity: *«Cyberbedrohungen entwickeln sich hinsichtlich ihrer Geschwindigkeit, ihres Ausmasses und ihrer Raffinesse ständig weiter. Für Schweizer Organisationen ist Cybersicherheit mittlerweile ein zentraler Bestandteil des Unternehmensrisikomanagements, der Widerstandsfähigkeit und der Führungssteuerung und nicht mehr nur eine rein technische Disziplin.»*

Der Report gibt Auskunft und bietet Einblicke zu: Herausforderungen im Bereich Governance, relevante Cyberbedrohungen für Schweizer Organisationen (siehe Grafik: erwartete Risiken und Angriffsarten), neue Angriffstechniken wie KI-gestütztes Phishing, identitätsbasierte Angriffe und mehr, praktische Empfehlungen zur Stärkung der Cyberresilienz oder auch konkrete operative Erkenntnisse aus dem SOC (Security Operations Center) von Swiss Post Cybersecurity.

Der «Swiss Threat Landscape Report» ist erhältlich unter: https://www.swisspost-cybersecurity.ch/swiss-threat-landscape-report

** Die Umfrage zum «Swiss Threat Landscape Report» wurde im Januar und Februar 2026 von Swiss Post Cybersecurity durchgeführt. Befragt wurden Personen in Führungspositionen im Bereich IT und Cybersecurity. Sie basiert auf 70 anonymisierten Antworten. Die Ergebnisse liefern einen qualitativen Überblick über aktuelle Trends, Risiken und Einschätzungen innerhalb der befragten Branchen: Öffentlicher Sektor/Behörden, Gesundheitswesen, Finanzsektor, Versicherungswesen, Fertigungsindustrie, Einzelhandel und weitere.*

Über Swiss Post Cybersecurity AG

Die Swiss Post Cybersecurity AG bietet Security-Lösungen zum Schutz digitaler Informationen und vertraulicher Daten von Unternehmen und unterstützt diese dabei, die steigenden Sicherheitsanforderungen zu erfüllen. Unsere Lösungen – insbesondere die SOC-Services unseres Cyber Defense Centers – werden in der Schweiz entwickelt und bereitgestellt. Kompetenzen in Governance, Offensive Security, Integration sowie Risk & Compliance ergänzen unser Angebot. Mit rund 150 Mitarbeitenden betreuen wir über 350 Organisationen in Europa. Unser Hauptsitz befindet sich in Aarau, mit weiteren Standorten in Morges und Luxemburg. Die Swiss Post Cybersecurity AG ist eine unabhängige, marktorientierte Tochtergesellschaft der Schweizerischen Post und entstand 2024 durch den Zusammenschluss zweier bekannter Marktführer: terreActive und Hacknowledge.
https://www.swisspost-cybersecurity.ch/de/

Kontakt
Swiss Post Cybersecurity AG
Gabriele Bornemann
Marketing Manager
gabriele.bornemann@swisspost-cybersecurity.ch
+41 62 834 00 55

Jenni Kommunikation AG
Sylvana Zimmermann
sylvana.zimmermann@jeko.com
+41 44 388 60 80