Bedrohungslage 2026

Jede Zahl aus einer Primärquelle. Herausgeber, Datum und Fundstelle im Quellenverzeichnis auf Seite 2.

48.167	31 %	2.692	62.328
NEUE SCHWACHSTELLEN	**HÄUFIGSTER ERSTZUGANG**	**OFFENE RDP-ZUGÄNGE**	**ANZEIGEN IN ÖSTERREICH**
2025, rund 132 pro Tag	Ausnutzung von Schwachstellen	IP-Adressen in Österreich	Internetkriminalität 2024

1 Die Menge ist nicht mehr manuell zu überblicken

2025 wurden **48.167 neue Schwachstellen** veröffentlicht, rund 20 Prozent mehr als im Jahr davor und im Schnitt **mehr als 130 pro Tag**. Kein Betrieb kann das laufend verfolgen. Entscheidend ist, welche davon auf Ihren Systemen tatsächlich vorhanden sind.

Quelle [1]: NIST National Vulnerability Database, eigene Auswertung, abgefragt am 13.07.2026.

2 Die Suche nach Schwachstellen wird automatisiert

Bei der **AI Cyber Challenge der DARPA** fanden KI-Systeme 2025 **18 echte, bisher unbekannte Schwachstellen** in verbreiteter Software. Dieselbe Technik nutzen auch Angreifer: Google beschreibt einen **gereiften Untergrundmarkt für KI-Werkzeuge**, der die Einstiegshürde senkt.

Quellen [2] DARPA, AIxCC Results, 08.08.2025. [3] Google Project Zero, 01.11.2024. [4] Google Threat Intelligence Group, 05.11.2025.

3 Angreifer müssen Sie nicht suchen, Sie sind bereits erfasst

Alles, was aus dem Internet erreichbar ist, wird laufend gescannt und ist durchsuchbar, das **gesamte IPv4-Internet 42-mal täglich**. CISA und FBI belegen, dass Täter mit Diensten wie Shodan **gezielt verwundbare Systeme ermitteln**. Am 12. Juli 2026 wiesen **2.692 IP-Adressen in Österreich** einen offen erreichbaren Fernwartungszugang (RDP) aus.

Quellen [5] CISA, 04.06.2025. [6] CISA und FBI, Advisory AA24-241A, 28.08.2024. [7] Shadowserver Foundation, Datenstand 12.07.2026. Gezählt werden IP-Adressen, nicht Betriebe.

4 Zwischen Veröffentlichung und Angriff liegt wenig Zeit

Die **Ausnutzung von Schwachstellen ist erstmals der häufigste Erstzugang** bei Sicherheitsverletzungen (**31 Prozent**, Vorjahr 20). Geschlossen wird gleichzeitig zu langsam: Von den nachweislich angegriffenen Schwachstellen im CISA-Katalog waren nur **26 Prozent vollständig behoben**.

Quellen [8] Verizon, 2026 Data Breach Investigations Report, Mai 2026. [9] CISA, Known Exploited Vulnerabilities Catalog, 13.07.2026.

5 Kleine und mittlere Betriebe stehen im Zentrum, nicht am Rand

Bei Ransomware-Fällen mit bekannter Unternehmensgröße waren **rund 96 Prozent der Opfer kleine und mittlere Unternehmen**. In Österreich wurden 2024 **62.328 Anzeigen wegen Internetkriminalität** erstattet, gegenüber 2015 **mehr als versechsfacht**. Zugleich haben nur **14 Prozent der kleinen Unternehmen** eigene IKT-Fachkräfte.

Quellen [8] Verizon, 2026 DBIR, Mai 2026. [10] Bundeskriminalamt, Cybercrime Report 2024. [11] Statistik Austria, IKT-Einsatz in Unternehmen 2024.

Wie schnell ein offener Zugang gefunden wird

Sicherheitsforscher von Palo Alto Networks stellten 320 Testsysteme bewusst ungeschützt ins Netz. **80 Prozent davon waren binnen 24 Stunden kompromittiert.** Ein einzelner Angreifer übernahm 96 Prozent von 80 Datenbank-Testsystemen **innerhalb von 30 Sekunden**. Ein offener Zugang bleibt nicht unentdeckt, weil Ihr Betrieb klein oder unbekannt ist.

Quelle [12]: Unit 42, Palo Alto Networks, Observing Attacks Against Hundreds of Exposed Services in Public Clouds, 22.11.2021.

Was ein erfolgreicher Angriff konkret bedeutet

Stillstand: Verschlüsselte Systeme heißen: keine Aufträge, keine Rechnungen, keine Kommunikation, so lange die Wiederherstellung dauert.

Datenverlust: Ohne getestete, getrennt aufbewahrte Sicherung sind Ihre Daten im schlimmsten Fall unwiederbringlich weg.

Erpressung: Sie sind den Angreifern ausgeliefert: Lösegeld ohne Garantie, dass Daten zurückkommen oder nicht trotzdem veröffentlicht werden. Wer zahlt, gilt als lohnendes Ziel.

Datenabfluss und Haftung: Gelangen personenbezogene Daten in fremde Hände, greift die Meldepflicht an die Datenschutzbehörde binnen 72 Stunden, Betroffene sind zu informieren und können **Schadenersatz** geltend machen (DSGVO Art. 33, 34 und 82).

Vertrauen und Ruf: Kunden, Partner und Banken erfahren davon. Verlorenes Vertrauen kostet länger als die Wiederherstellung der Systeme.

Was der IT Check daraus macht

Wir prüfen anhand von über 100 Prüfpunkten in acht Bereichen, **was von außen erreichbar ist**, welche Systeme **ungepatcht** sind und ob Sicherungen im Ernstfall tragen. Sie erhalten einen dokumentierten Befund und einen **priorisierten Maßnahmenplan**: die Handvoll Punkte, die bei Ihnen zählt, in der richtigen Reihenfolge.

Quellenverzeichnis

[1] NIST, National Vulnerability Database, services.nvd.nist.gov (Abfrage 13.07.2026)
[2] DARPA, AI Cyber Challenge Results, darpa.mil/news/2025/aixcc-results (08.08.2025)
[3] Google Project Zero, From Naptime to Big Sleep, projectzero.google (01.11.2024)
[4] Google Threat Intelligence Group, Threat Actor Usage of AI Tools, cloud.google.com (05.11.2025)
[5] CISA, Internet Exposure Reduction Guidance, cisa.gov/resources-tools/resources/exposure-reduction (04.06.2025)
[6] CISA, FBI und DC3, Joint Advisory AA24-241A, cisa.gov (28.08.2024)
[7] The Shadowserver Foundation, Statistics und Dashboard, shadowserver.org (Datenstand 12.07.2026)
[8] Verizon Business, 2026 Data Breach Investigations Report, verizon.com (Mai 2026)
[9] CISA, Known Exploited Vulnerabilities Catalog, cisa.gov (Katalogstand 13.07.2026)
[10] Bundeskriminalamt, Cybercrime Report 2024, bundeskriminalamt.at (Wien 2025)
[11] Statistik Austria, IKT-Einsatz in Unternehmen 2024, statistik.at (Wien 2025)
[12] Unit 42, Palo Alto Networks, Exposed Services in Public Clouds, unit42.paloaltonetworks.com (22.11.2021)
[13] Verordnung (EU) 2016/679 (DSGVO), Art. 33, 34 und 82, eur-lex.europa.eu

Die Zahlen geben den Stand zum jeweils genannten Datum wieder und verändern sich laufend. Die Angaben zu offen erreichbaren Diensten zählen eindeutige IP-Adressen pro Tag und lassen keinen Rückschluss auf einzelne Betriebe zu. Wir bewerten ausschließlich technische und organisatorische Maßnahmen Ihrer IT; für rechtliche Fragen empfehlen wir einen passenden juristischen Partner. Alle Preise verstehen sich netto zuzüglich gesetzlicher Umsatzsteuer.