HISOLUTIONS

Schwachstellenreport 2026

hisolutions.com

Schwachstellenreport 2026

HISOLUTIONS

HiSolutions führt seit über 25 Jahren eine große Anzahl unterschiedlicher Penetrationstest und technische Audits durch. Auch 2026 haben wir die Tests des Vorjahres ausgewertet und die identifizierten Schwachstellen nach Schweregrad und Kategorien analysiert. Unser Schwachstellenreport trifft Aussagen über typische Testergebnisse, Problembereiche und häufige Sicherheitslücken und leitet interessante Trends und wichtige Entwicklungen in der Sicherheitslage von Unternehmen und Organisationen ab.

Pentesttypen

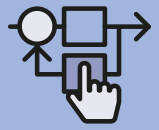
31 %
Konfigurationsaudit/ Architekturreviews

25 %
Infrastruktur (Netze, Systeme)

24 %
Web-Seiten und Web-Anwendungen

7 %
Red und Purple Teaming

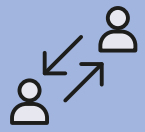
5 %
Anwendungen (Mobile, Desktop)



3 %
Prüfung industrieller Steuerungsanlagen

6 %
Sonstige (u. a. Hardware, Social-Engineering)

Tests nach Branchen



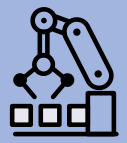
22 %
Beratung/ Dienstleistung

19 %
Öffentliche Verwaltung

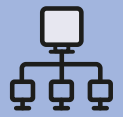
13 %
Transport/ Logistik

12 %
Gesundheitswesen

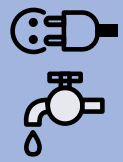
10 %
Finanzen/ Versicherungen



7 %
Industrie

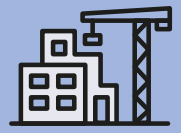


7 %
IT-Dienstleister



3 %
Energie- und Wasserversorgung

2 %
Handel

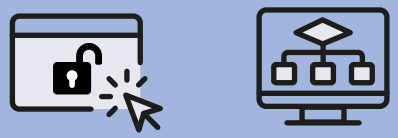


2 %
Baugewerbe und Immobilien

5 %
Sonstige Branchen

Aufgrund der sensiblen Materie listen wir unsere Projektreferenzen im Bereich Penetrationstests und technische Audits nur in anonymer Form. Bei Bedarf werden wir auf Rückfrage gerne versuchen, einen persönlichen Ansprechpartner zu einem von uns durchgeführten Test zu vermitteln.

Hohe oder kritische Schwachstellen-Befunde:
in **60 %** der internen Pentests, in **58 %** der Konfigurations- und Architekturreviews, in **45 %** der Dokumentations- oder Organisationsaudits.



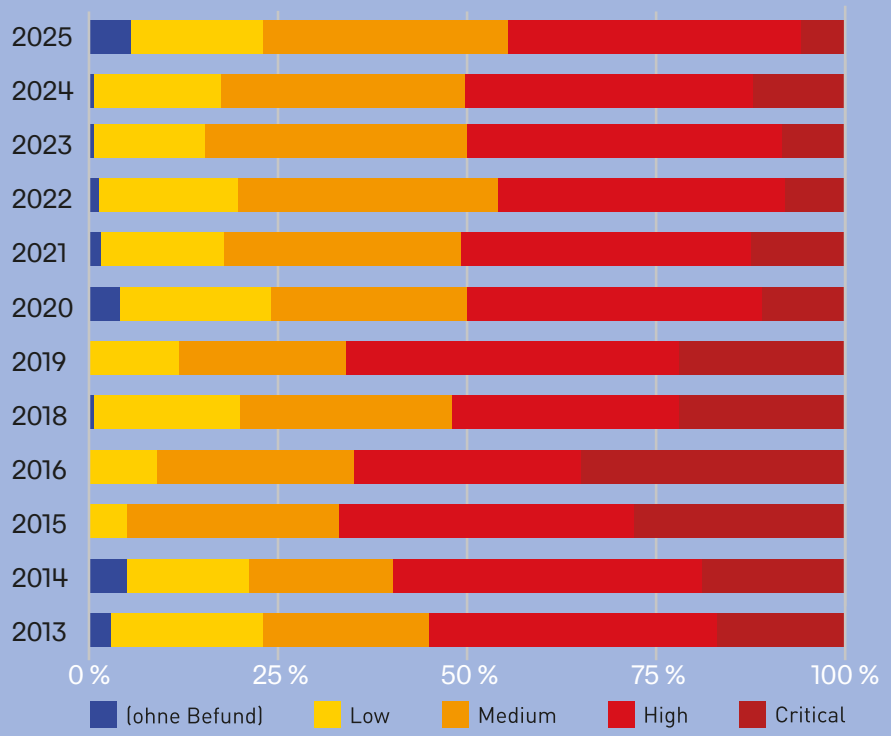
Häufigste Ursachen für Befunde mit der Einstufung hoch oder kritisch:

- Mangelhafte Konfiguration
- Ungeeignete Sicherheitsarchitektur
- Mangelhaftes Benutzer- und Rechtemanagement
- Mangelnde Systempflege
- Falsche Sicherheitskonfiguration

Häufigste Schwachstellenkategorien basierend auf den OWASP Top 10 in Web-Anwendungen (absteigend):

- Security Misconfiguration (OWASP A05:2021)
- Broken Access Control (OWASP A01:2021)
- Vulnerable and Outdated Components (OWASP A06:2021)
- Injection (OWASP A03:2021)
- Insecure Design (OWASP A04:2021)
- Cryptographic Failures (OWASP A02:2021)
- Identification and Authentication Failures (OWASP A07:2021)

Statistik Kritikalität 2013–2025:



Kritikalitätsvektor (0–4) nach Pentesttyp

(Kritikalität des schwerwiegendsten Befundes der Test-Art im ø)

	2019	2020	2021	2022	2023	2024	2025
Externer Penetrationstest	2,12	1,81	1,60	1,69	1,62	1,75	1,68
Interner Penetrationstest	3,00	3,27	2,85	2,52	2,73	2,78	2,38
Web-Penetrationstest	2,12	1,93	2,24	2,04	1,91	1,86	1,84
Applikations- oder API-Test	2,00	2,00	1,70	2,25	2,00	1,50	2,07
Konfigurationsaudit oder Architektur-Review	2,48	2,40	2,48	2,40	2,34	2,43	2,51

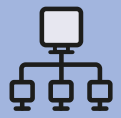
Low Medium High Critical

Im Jahr 2025 durchgeführte Forensik- und Incident-Response-Einsätze:
In anonymisierter Form haben wir die Vorfallskategorien aus ungefähr 260 Fällen aufgeschlüsselt, die wir im vergangenen Jahr in der IT-Forensik untersucht haben.

HISOLUTIONS

Art des Vorfalls

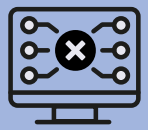
22 %
Ransomware



18 %
Kompromittierung von Servern/Clients

15 %
False Positive

12 %
Phishing/ gefälschte E-Mails



6 %
Ausfall von Systemen/ Anwendungen

4 %
CEO-Fraud/ Rechnungsbetrug

4 %
Erpressung

2 %
Schaden durch Innentäter

1 %
Advanced Persistent Threat

16 %
Sonstige

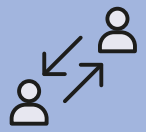
Top-3-Angriffsvektoren

Nutzerinteraktion

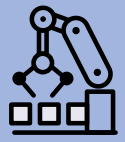
Bekannte CVE

offene Schnittstelle

Branche



30 %
Beratung/IT/ Dienstleistung



13 %
Industrie

10 %
Gesundheits-wesen

9 %
Öffentliche Verwaltung

Bei nur 10 % der betroffenen Organisationen handelte es sich um KRITIS- oder KRITIS-nahe Einrichtungen.

Verdacht auf meldepflichtigen Datenschutzvorfall

47 %
Kein Verdacht

53 %
Meldepflichtiger Vorfall

Die häufigsten Angriffsfolgen:

21 % Datenabfluss
20 % Ausfall einzelner Anwendungen oder Dienste
16 % Verschlüsselung von Daten
14 % Betriebsausfall
5 % Datenmanipulation