www.hisolutions.com

HISOLUTIONS

Schwachstellenreport 2025

Schwachstellenreport 2025

HISOLUTIONS

HiSolutions führt seit über 25 Jahren eine große Anzahl unterschiedlicher Penetrationstest und technische Audits durch. Auch 2025 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.

Getestete Komponenten

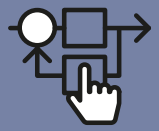
32 %
Infrastruktur (Netze, Systeme)

26 %
Web-Seiten und Web-Anwendungen

22 %
Konfigurations-audits

16 %
Sonstige (u. a. Hardware, Social-Engineering)

2 %
Anwendungs-software



2 %
Prüfung industrieller Steuerungsanlagen

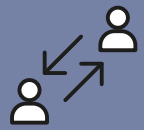
Tests nach Branchen

22 %
Öffentliche Verwaltung

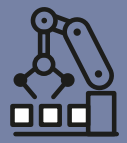
11 %
Gesundheitswesen

11 %
IT-Dienstleister

11 %
Finanzen/ Versicherungen



10 %
Beratung/ Dienstleistung



9 %
Industrie

9 %
Transport/ Logistik

6 %
Energie- und Wasserversorgung

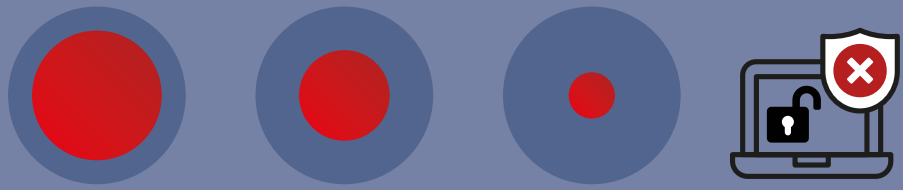
5 %
Handel

2 %
Chemie/Pharma

5 %
Sonstige Branchen

Im Jahr 2024 getestete Komponenten und 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 **66 %** der internen Pentests, in **54 %** der Konfigurations- und Architektur-Reviews, in **23 %** der Web-Pentests

www.hisolutions.com

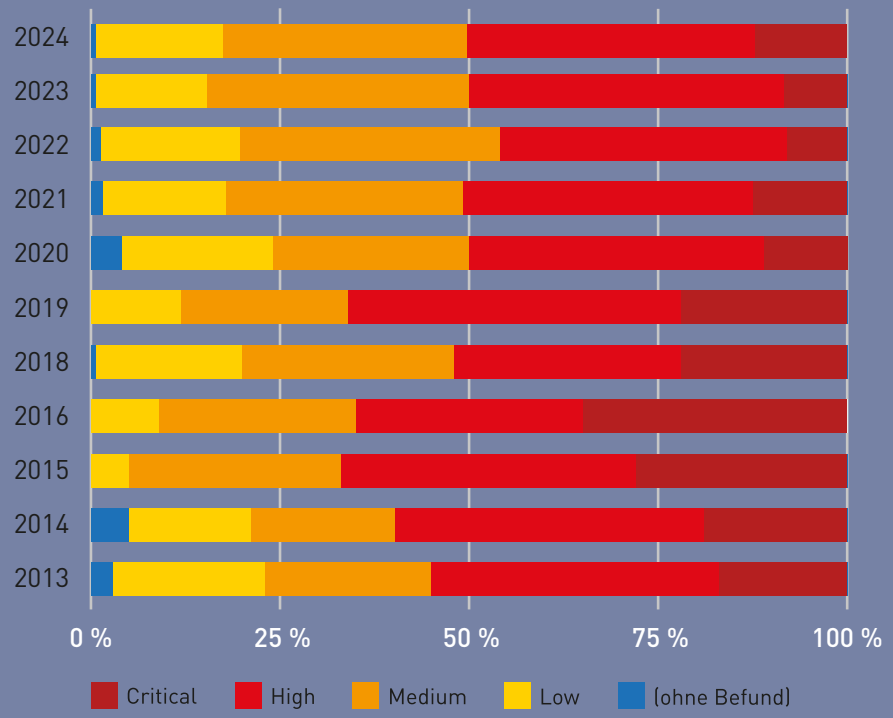
Häufigste Ursachen für Befunde mit der Einstufung hoch oder kritisch:

- Ungeeignete Sicherheits-architektur
- Mangelhafte Konfiguration
- 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)
- **Cryptographic Failures** (OWASP A02:2021)
- **Vulnerable and Outdated Components** (OWASP A06:2021)
- **Identification and Authentication Failures** (OWASP A07:2021)
- **Injection** (OWASP A03:2021)
- **Insecure Design** (OWASP A04:2021)
- **Broken Access Control** (OWASP A01:2021)

Statistik Kritikalität 2013–2024:



Häufigste Befunde im internen Pentest:

- **Angriffe auf Netzwerkprotokolle** (z. B. ARP, LLMNR, NetBios)
- **Mängel in der Passwortstärke, -speicherung, -verwendung**
- **Ausnutzbare Mängel in der Härtung**
- **Ungeeignete Netzwerkarchitektur**
- **Unsichere Konfiguration von Diensten und Anwendungen**
- **Schwachstellen in veralteten Systemen**

Kritikalitätsvektor (0–4) nach Pentesttyp