www.hisolutions.com

HISOLUTIONS

Schwachstellenreport 2024

Schwachstellenreport 2024

HISOLUTIONS

HiSolutions führt seit über 20 Jahren eine große Anzahl unterschiedlicher Penetrations- und Schwachstellentests durch. Auch 2024 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

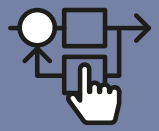
35 %
Infrastruktur (Netze, Systeme)

25 %
Web-Seiten und Web-Anwendungen

22 %
Konfigurations-audits

12 %
Sonstige (u. a. Hardware, Social-Engineering)

4 %
Anwendungs-software

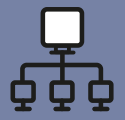


1 %
Prüfung industrieller Steuerungsanlagen

Tests nach Branchen

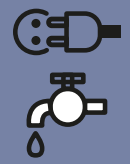
22 %
Öffentliche Verwaltung

16 %
Gesundheitswesen

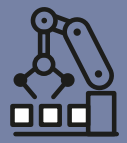


14 %
IT-Dienstleister

12 %
Beratung/ Dienstleistung



9 %
Energie- und Wasserversorgung



7 %
Industrie

7 %
Finanzen/ Versicherungen

5 %
Transport/ Logistik

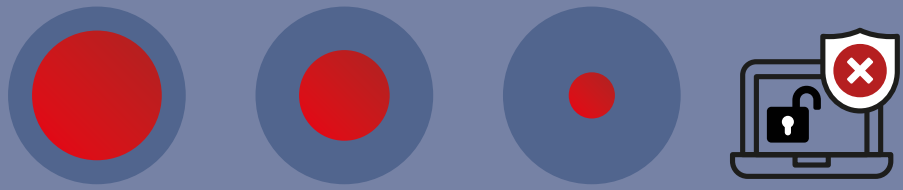
3 %
Chemie/Pharma

3 %
Handel

4 %
Sonstige Branchen

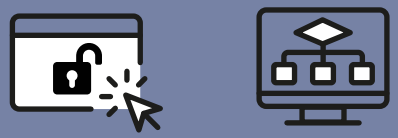
Im Jahr 2023 getestete Komponenten und Branchen

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 **73 %** der internen Pentests, in **51 %** der Konfigurations- und Architektur-Reviews, in **26 %** der Web-Pentests

www.hisolutions.com



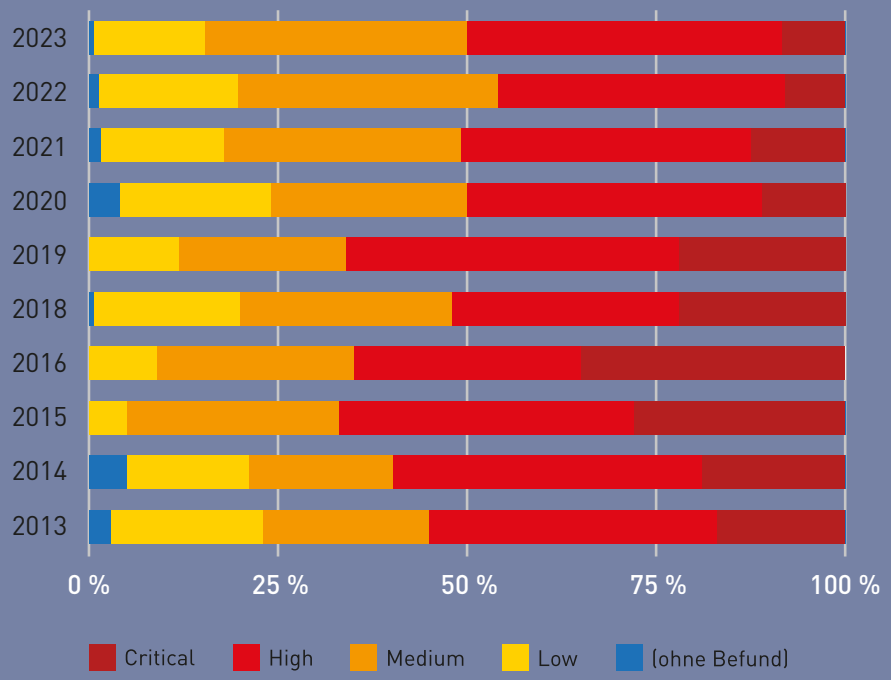
Häufigste Ursachen für Befunde mit Einstufung hoch oder kritisch:

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

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

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

Statistik Kritikalität 2013–2023:



Kritikalitätsvektor (0–4) nach Pentesttyp

	2019	2020	2021	2022	2023
Externer Penetrationstest	2,12	1,81	1,60	1,69	1,62
Interner Penetrationstest	3,00	3,27	2,85	2,52	2,73
Web-Penetrationstest	2,12	1,93	2,24	2,04	1,91
Applikations- oder API-Test	2,00	2,00	1,7	2,25	2,00
Konfigurationsaudit oder Architektur-Review	2,48	2,40	2,48	2,40	2,34

Critical High Medium Low (ohne Befund)

www.hisolutions.com

Im Jahr 2023 durchgeführte Forensik- und Incident-Response-Einsätze:

In anonymisierter Form haben wir die Vorfallskategorien aus ungefähr 250 Fällen aufgeschlüsselt, die wir im vergangenen Jahr in der IT-Forensik untersucht haben.

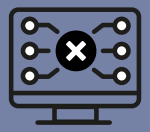
30 %
Ransomware, davon 6 % mit Erpressung

13 %
Phishing/ gefälschte E-Mails

11 %
Hacker-Einbruch

11 %
IT-DL RZ offline

10 %
Sonstige Schadsoftware



7 %
Ausfall von Systemen/ Anwendungen

5 %
TK-Einbruch

3 %
CEO-Fraud/ Rechnungsbetrug

2 %
Erpressung

2 %
Schaden durch Innentäter

1 %
Spam-Problem

Top 5
Empfehlungen zur Vorfallsprävention:

Mehrfaktorenauthentifizierung bei Zugriffen über öffentliche Netze

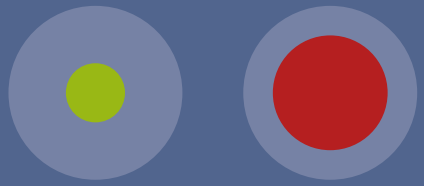
Zugriffskontrolle auf administrative Konsolen

Manipulationsgesicherte Datensicherungsverfahren (z.B. Offline-Back-up oder isoliert von den gesicherten Systemen)

Zeitnahes Patchen exponierter Dienste und Systeme

Detektionsverfahren für Angriffswerkzeuge oder Angreifersysteme und Protokollierung von Systemaktivitäten

Verdacht auf meldepflichtigen Datenschutzvorfall



40 %
Kein Verdacht

60 %
Meldepflichtiger Vorfall

Im Jahr 2023 hat ein Unternehmen einen geschäftsvernichtenden Sicherheitsvorfall nicht überlebt.

www.hisolutions.com