Schwachstellenreport 2023

HISOLUTIONS

HiSolutions führt seit über 20 Jahren eine große Anzahl unterschiedlicher Penetrations- und Schwachstellentests durch. Auch 2023 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

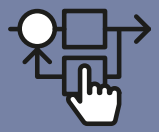
28 %
Infrastruktur (Netze, Systeme)

27 %
Web-Seiten und Web-Anwendungen

23 %
Konfigurations-audits

13 %
Sonstige (u. a. Hardware, Social-Engineering)

6 %
Anwendungs-software

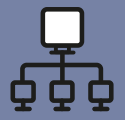


3 %
Prüfung industrieller Steuerungsanlagen

Tests nach Branchen

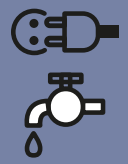
16 %
Gesundheitswesen

14 %
Beratung/ Dienstleistung



12 %
IT-Dienstleister

11 %
Öffentliche Verwaltung

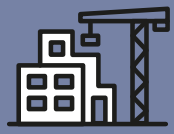


11 %
Energie- und Wasserversorgung

10 %
Industrie

9 %
Transport/ Logistik

7 %
Finanzen/ Versicherungen

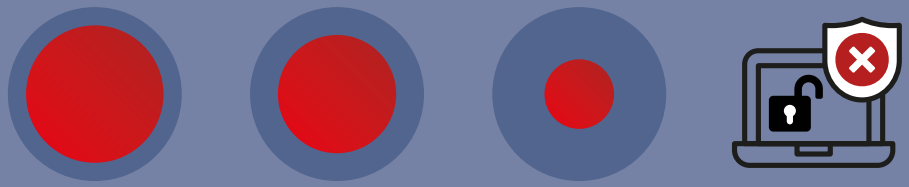


2 %
Baugewerbe und Immobilien

7 %
Sonstige Branchen

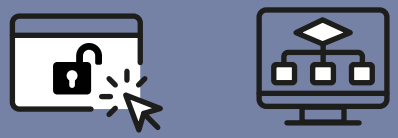
Im Jahr 2022 getestete Komponenten und Branchen

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 **79 %** der internen Pentests, in **68 %** der Konfigurations- und Architektur-Reviews, in **40 %** der Web-Pentests

www.hisolutions.com



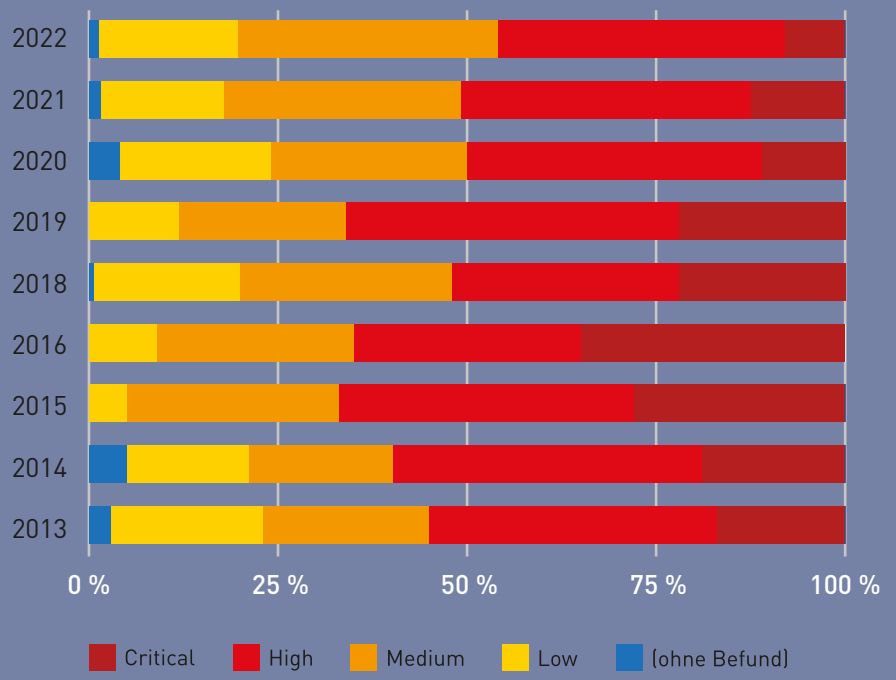
Häufigste Ursachen für Befunde mit Einstufung hoch oder kritisch:

- Falsche Sicherheitskonfiguration
- Ungeeignete Sicherheits-architektur
- Anfällige und veraltete Komponenten
- Mangelhaftes Benutzer- und Rechtemanagement
- Fehlerhafte Zugriffsbeschränkungen

Häufigste Befunde, die die Kompromittierung von AD-Umgebungen erlaubten oder begünstigten:

- Schwachstellen in veralteten Systemen
- Mängel in der Passwortstärke, -Speicherung und -Verwendung
- Angriffe auf Netzwerkprotokolle (z. B. ARP, LLMNR)
- Schützenswerte Daten in unbeschränkten Dateifreigaben
- Schwachstellen in AD-Zertifikatsdiensten

Statistik Kritikalität 2013–2022:



Kritikalitätsvektor (0–4) nach Pentesttyp

	2019	2020	2021	2022
Externer Penetrationstest	2,12	1,81	1,6	1,69
Interner Penetrationstest	3	3,27	2,85	2,52
Web-Penetrationstest	2,12	1,93	2,24	2,04
Applikations- oder API-Test	2	2	1,7	2,25
Konfigurationsaudit oder Architekturreview	2,48	2,4	2,48	2,4

www.hisolutions.com

Im Jahr 2022 durchgeführte Forensik- und Incident-Response-Einsätze:

In anonymisierter Form haben wir die Vorfallskategorien aus ungefähr 400 Fällen aufgeschlüsselt, die wir im vergangenen Jahr in der IT-Forensik untersucht haben.

39 %
Ransomware, davon 12 % mit Erpressung

27 %
Phishing/ gefälschte E-Mails

6 %
CEO-Fraud/ Rechnungsbetrug

6 %
Spam-Problem

5 %
Crypto-Mining

5 %
Sonstige Schadsoftware

4 %
Erpressung

2 %
Ausfall von Systemen/ Anwendungen

2 %
Schaden durch Innentäter

2 %
TK-Einbruch

1 %
IT-DL RZ offline

Top 5
Empfehlungen zur Vorfallsprävention:

Mehrfaktorenauthentifizierung bei Zugriffen über öffentliche Netze

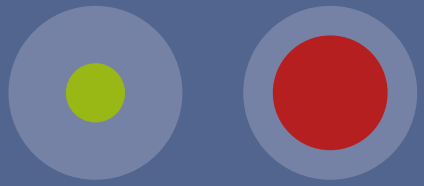
Zugriffskontrolle auf administrative Konsolen

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

Zeitnahes Patchen exponierter Dienste und Systeme

Detektionsverfahren für bekannte Angriffswerkzeuge oder Angreifersysteme

Verdacht auf meldepflichtigen Datenschutzvorfall



34 %
Kein Verdacht

66 %
Meldepflichtiger Vorfall

Im Jahr 2022 haben zwei Unternehmen einen geschäftsvernichtenden Sicherheitsvorfall nicht überlebt.

www.hisolutions.com