



Checkliste

IT-SCHWACHSTELLEN

Jedes IT-System hat Schwachstellen und es kommen auch oft neue hinzu. Es sind **sehr zielgerichtete Prozesse und Verfahren** notwendig, um diese Schwachstellen zu finden und auch zukünftig zu vermeiden, denn entscheidende und immer wieder ausgenutzte Schwachstellen lassen sich weder durch interne Sicherheitslösungen noch durch PenTests entdecken. Die vorliegende Checkliste konzentriert sich auf die **am häufigsten ausgenutzten Schwachstellen** und ist eine essenzielle und kostenlose Hilfe, um Ihre Systeme **sofort sicherer zu machen**.

BENUTZER

Oft wird seitens der Nutzer und der IT argumentiert: „Ich habe doch MFA/SSO, alles sicher im EntraID ausgesteuert, wir haben On-/Offboarding Prozess im Griff“, aber die Wahrheit ist:

Einige kritische Applikationen haben kein MFA oder SSO und der Prozess des Benutzer-Management sollte verbessert werden – das gilt sogar bis zur Firewall selbst, auf der z.B. VPN-Benutzer angelegt werden (unklare Benutzersituationen an dieser Stelle sind ein wesentlicher Schwachpunkt). Oder die neue Entra-ID Schwachstelle CVE-2025-55241 (inzw. geschlossen) erlaubte einen möglichen Einbruch im zentralen Benutzermanagement ohne jegliche Spuren im Audit Log zu hinterlassen.

Schwachstelle	Ursache
Login ohne MFA oder ohne SSO	Alte Software
„Least Privilege Regel“ nicht eingehalten, zu wenige Benutzer oder zu viele Benutzer für ein System oder mit zu hohen Rechten	Fehlende Prozesse, ISMS
Schwache Kennworte, Unsicheres Kennwort-Management	Fehlende Prozesse, ISMS
Geteilte User-Accounts	Fehlende Prozesse, ISMS
VPN-Benutzer auf der Firewall nicht gemanagt	Fehlende Prozesse, ISMS
Phishing	Fehlendes Security Awareness Training oder ohne Lernkontrolle
Active-Directory, GPOs und Berechtigungen	Falsche oder nicht ständig angepasste Rechte
Keine Secure Printing-PIN auf Druckern	Fehlendes Default-Setting
Fehlbedienung von Teams oder anderer Meeting-Software, Aufzeichnungen, uvm.	Fehlendes Training

Maßnahme: Sofortige **Systemdurchsichten**; **Prozesse & Verfahren** für kritische Systeme etablieren, **professioneller Kennwort-Manager** einführen, **Training**





Checkliste

SOFTWARE

Die **TOP 12 ausgenutzten** Software-Schwachstellen (inkl. OS/ iOS) – erzeugt durch die Hersteller – in den letzten Jahren waren und sind:

Schwachstelle	CVSS-Score	EPSS-Score
ZeroLogon: NetLogon Remote Protocol (CVE-2020-1472)	5	94%
Log4Shell: Apache Log4J (CVE-2021-44228)	10	94%
ICMAD: SAP Internet Communication Manager (CVE-2022-22536)	10	93%
Proxy Logon, Microsoft Exchange (CVE-2021-26855)	9,1	94%
Spring4Shell (CVE-2022-22965)	9,8	94%
Atlassian Confluence (CVE-2022-26134)	9,8	94%
VMware vSphere (CVE-2021-21972)	9,8	93%
Google Chrome Zero-Day (CVE-2022-0609)	8,8	61%
Follina: Microsoft Diagnostic Tool MSDT , (CVE-2022-30190)	7,8	93%
PetitPotam, Windows LSA Spoofing (CVE-2021-36942)	7,5	93%
Cisco WebUI/iOS (CVE 2023-20198)	10	94%
Microsoft SharePoint (CVE-2025-53770)	10	

CVSS-Score: Schweregrad der Lücke, EPSS-Score: Wahrscheinlichkeit der Ausnutzung

Die öffentlichen **CVE-Datenbanken** sind hier:

- US-Version: <https://app.openCVE.io/>
- Europäische Version: [Vulnerability Database](#)
- Deutsche Version: [Warn- und Informationsdienst - Aktuelle Sicherheitshinweise](#)
- Deutsche Version: <https://cve.engineering.com/>

Maßnahme: Sofortige Release/Patch Kontrolle; Automatische, schnelle **Patch-Verteilung** auf Client Geräten und Server

