NETZ
INFORMATIONS
SYSTEME

NIS AG
Buchenstrasse 8
CH-6210 Sursee
Tel. +41 41 267 05 05
info@nis.ch
www.nis.ch

Whitepaper

Externer Penetration Test 2025

Professionelles Hosting des Netzinformationssystems – sicher, performant und umfassend betreut.

Ziel und Einordnung

Als Anbieterin von Fullservice Angeboten für Kunden mit erhöhten Anforderungen an Informationssicherheit, Verfügbarkeit und Resilienz lässt die NIS AG ihre Sicherheitsorganisation und Angebote regelmässig durch unabhängige externe Stellen überprüfen.

Für die NIS AG sind Penetration Tests ein integraler Bestandteil dieses mehrschichtigen Sicherheitsansatzes. Sie ergänzen kontinuierliche Security-Tests innerhalb des CI/CD-Prozesses, automatisierte Schwachstellenanalysen sowie die operative Sicherheitsüberwachung im Cloud-Betrieb.

Untersucht werden jeweils die NIS 3 Applikationen sowie die Full-Service Angebote nisHosting und nis365. Ziel dieser Prüfungen ist es, potenzielle Schwachstellen frühzeitig zu identifizieren, Risiken realistisch zu bewerten und die Wirksamkeit der implementierten Sicherheitsmassnahmen aus externer Sicht zu validieren.

Dieses Whitepaper bezieht sich exemplarisch auf den im Jahr 2025 durchgeführten Penetration Test und dient als transparenter, unabhängiger Nachweis der technischen Sicherheit der genannten Produkte und Plattformen.

Was ist ein Penetration Test?

Ein Penetration Test (kurz *PenTest*) ist eine gezielte, kontrollierte Sicherheitsüberprüfung, bei der qualifizierte Sicherheitsexperten versuchen, Schwachstellen in Systemen, Anwendungen oder Schnittstellen wie ein realer Angreifer auszunutzen. Ziel ist es nicht, theoretische Schwächen aufzulisten, sondern reale Risiken unter praxisnahen Bedingungen zu identifizieren.

Im Unterschied zu rein automatisierten Scans kombiniert ein Penetration Test manuelle Angriffstechniken, Erfahrung und Kontextwissen. Dadurch können auch komplexe Schwachstellen erkannt werden, die durch automatisierte Werkzeuge allein nicht zuverlässig identifiziert werden können.

Umfang und Methodik

Der in diesem Whitepaper referenzierte Penetration Test wurde durch ein spezialisiertes, unabhängiges Sicherheitsunternehmen durchgeführt. Der Fokus lag auf realistischen Angriffsszenarien gegen produktionsnahe Systemkomponenten der NIS-Plattform. Ziel war eine praxisnahe Bewertung realer Sicherheitsrisiken unter möglichst realistischen Bedingungen.

Geprüft wurden unter anderem öffentlich erreichbare Schnittstellen und Dienste, Authentifizierungs- und Autorisierungsmechanismen, der Schutz vor typischen Web- und API-Angriffen sowie relevante Konfigurations- und Architekturentscheidungen.

Vorgehen

Der Test wurde als Whitebox-Penetration Test durchgeführt. Im Gegensatz zu einem Blackbox Test werden den Prüfern gezielt technische Informationen zur Architektur, zu eingesetzten Technologien sowie zu sicherheitsrelevanten Designentscheidungen zur Verfügung gestellt. Dieser Ansatz ermöglicht eine deutlich tiefere und präzisere Analyse als rein Blackbox-basierte Tests, da auch komplexe Logikfehler, Fehlkonfigurationen oder Schwachstellen in nicht öffentlich exponierten Komponenten identifiziert werden können. Gleichzeitig reduziert der Whitebox-Ansatz die Gefahr von Fehlinterpretationen und erlaubt eine realistische Einordnung der tatsächlichen Risiken.

Methodik

Die Methodik orientierte sich am **Open Worldwide Application Security Project (OWASP)**[1] **Application Security Verification Standard (ASVS)**[2]. ASVS definiert strukturierte, überprüfbare Sicherheitsanforderungen für Web-Anwendungen und APIs, unter anderem in den Bereichen Authentifizierung, Autorisierung, Session-Management, Datenverarbeitung und Schutz vor bekannten Angriffsmustern. Durch die Orientierung an OWASP ASVS wurde sichergestellt, dass der Penetration Test systematisch, nachvollziehbar und entlang etablierter Sicherheitsanforderungen durchgeführt wurde.

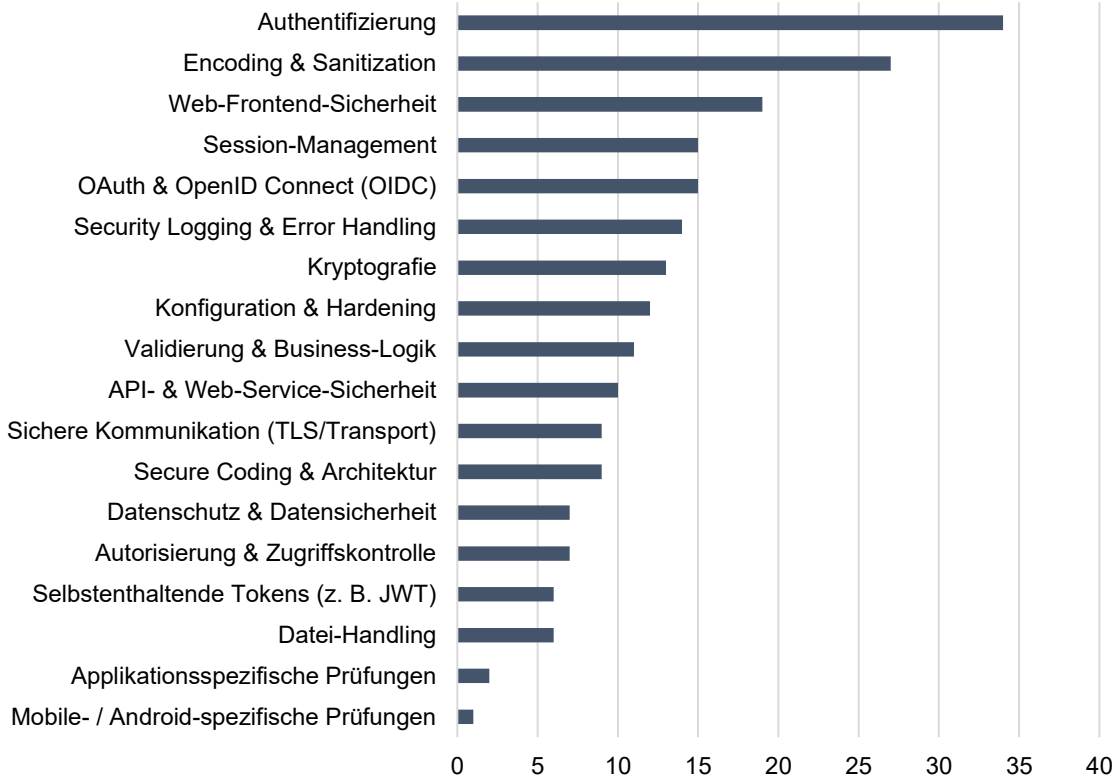

Abbildung 1: Die insgesamt 217 geprüften Anforderungen aufgelistet nach Kategorie.

Umgang mit Findings und Verbesserungsmassnahmen

Alle im Rahmen des Penetration Tests identifizierten Findings wurden nach Abschluss der Prüfung systematisch analysiert, priorisiert und in die bestehenden internen Prozesse der NIS AG überführt. Die Planung und Umsetzung von Massnahmen erfolgt risikobasiert unter Berücksichtigung der potenziellen Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Nach Umsetzung der Massnahmen wird die Wirksamkeit der Behebung überprüft, beispielsweise durch gezielte Verifikation oder Retests. Darüber hinaus fliessen die gewonnenen Erkenntnisse in bestehende Secure SDLC-, Architektur- und Betriebsprozesse ein. Dieser strukturierte Ansatz

[1] OWASP, Open Worldwide Application Security Project, *„Explore the world of cyber security“* [Online]. Available: https://owasp.org/. [Zugriff am 09 02 2026].

[2] OWASP, Open Worldwide Application Security Project, *„OWASP Application Security Verification Standard (ASVS)“* [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/. [Zugriff am 09 02 2026].

stellt sicher, dass auch nicht-kritische Schwachstellen nachhaltig adressiert werden und langfristig zur Reduktion zukünftiger Sicherheitsrisiken beitragen.

Zusammenfassung der Ergebnisse

Die Ergebnisse des Penetration Tests lassen sich wie folgt zusammenfassen:

- Es wurden **keine kritischen Schwachstellen** identifiziert
- Es wurden **keine Hinweise auf eine Kompromittierung** von Systemen oder Daten festgestellt
- Die getesteten Sicherheitsmechanismen erwiesen sich als **wirksam und angemessen implementiert**

Aus externer Sicht wurde die NIS 3 Plattform als sicherheitskonform und **für den produktiven Einsatz geeignet** bewertet.

Diese Ergebnisse bestätigen die Wirksamkeit der bestehenden Sicherheitsarchitektur sowie der eingesetzten Schutzmechanismen.

Transparenz und weitere Informationen

Dieses Whitepaper stellt eine bewusst verdichtete Darstellung dar. Detaillierte technische Informationen und Nachweise können auf Anfrage und unter NDA zur Verfügung gestellt werden.

Kontakt

NIS AG

Buchenstrasse 8

CH-6210 Sursee

Tel. 041 267 05 05

info@nis.ch · www.nis.ch

Literaturverzeichnis

[1] OWASP, Open Worldwide Application Security Project, *„Explore the world of cyber security“* [Online]. Available: https://owasp.org/. [Zugriff am 09 02 2026].

[2] OWASP, Open Worldwide Application Security Project, *„OWASP Application Security Verification Standard (ASVS)“* [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/. [Zugriff am 09 02 2026].