✓ SICHERHEITSZERTIFIZIERUNG

Sicherheitszertifizierung UfoooNetiX-MSG

Infrastruktur-Audit · Mai 2026 · Wien, Österreich

✓ Alle 55 Tests bestanden

7 Prüfphasen · 8 Systeme · 0 offene Findings

PRÜFDATUM
2. Mai 2026

AUFTRAGGEBER
UfoooNetiX

PRÜFER
Vertraulich

METHODIK
Extern + Intern, autorisiert

UMFANG
55 Testfälle · 2. + 14. Mai 2026

ERGEBNIS
✓ Bestanden — 55 / 55

1 Geprüfte Systeme & Infrastruktur

System	Adresse / Endpunkt	Prüftiefe	Ergebnis
Homepage	ufooonetix.at	TLS · Security-Headers · HTTP-Verben · Pfade	✓ Pass
App-Server	msg.ufooonetix.at:8443	WebSocket · Protokoll · Auth · Rate-Limit	✓ Pass
Monitor-Dashboard	monitor.ufooonetix.at:8444	mTLS · Zugriffskontrolle · Perimeter	✓ Pass
WebSocket-Protokoll	Go-Server intern	Alle Handler · Auth · Autorisierung · Badges	✓ Pass
Badge-System	Go-Server intern	Privilege Escalation · Injection · Sync	✓ Pass
iOS App	UfoooNetiX-MSG (App)	TLS-Pinning · Krypto · Storage · Protokoll	✓ Pass
LAB-Server	10.0.1.80 (intern)	SSH · UFW · fail2ban · HIDS · Erstprüfung	✓ Pass
HIDS	SVR · MON · LAB	auditd · Response-Daemon · Alert-Verifikation	✓ Pass
E2E-Verschlüsselung	Live-Traffic · DB · Logs	tcpdump · ScyllaDB · Redis · Go-Logs	✓ Pass

Prüfperspektive: Kombinierter Ansatz — **extern** (Internet, kein Vorwissen, Black-Box) sowie **intern** (autorisierter Tester mit Code-Zugriff, White-Box). Alle 55 Tests in 7 Phasen (2. + 14. Mai 2026).

Basis: Vollständig aufbauend auf dem Pentest März 2026 — alle damaligen Findings (PT-01–PT-04) wurden re-verifiziert und als behoben bestätigt. Neu geprüft: Badge-System, LAB-Server, HIDS-Verifikation und iOS App-Neubau.

2 Prüfphasen & Ergebnis

55	55	7	8	0
TESTS GESAMT	BESTANDEN	PRÜFPHASEN	SYSTEME	OFFENE FINDINGS

Phase	Prüfbereich	Tests	Ergebnis
Phase 1	Externe Reconnaissance & Perimeter	10	✓ Bestanden
Phase 2	Go-Server · WebSocket-Protokoll	15	✓ Bestanden
Phase 3	iOS App — Protokoll-Ebene	7	✓ Bestanden
Phase 4	Badge-System — Erstprüfung	5	✓ Bestanden
Phase 5	LAB-Server — Erstprüfung	7	✓ Bestanden
Phase 6	HIDS Verification (SVR · MON · LAB)	4	✓ Bestanden
Phase 7	E2E-Verschlüsselung — Live-Verifizierung *(14. Mai 2026)*	7	✓ Bestanden
Gesamt	7 Phasen · 8 Systeme · 2. + 14. Mai	**55**	✓ 55 / 55

Alle Findings des Audits März 2026 wurden re-verifiziert und bestätigt behoben. Im Verlauf dieser Prüfung identifizierte und sofort behobene Findings sind im Ergebnis bereits berücksichtigt. Zum Zeitpunkt der Zertifizierung bestehen **keine offenen Sicherheitslücken**.

3 Sicherheits-Highlights

- Go-Server (TLS 1.3)
- iOS App (Ed25519)
- MON Dashboard (mTLS)
- LAB-Server (HIDS)
- SVR (ScyllaDB)
- Homepage (nginx PQC)
- HIDS (auditd + Daemon)
- fail2ban · UFW

Post-Quantum Transport

TLS 1.3 mit **X25519MLKEM768** auf allen Endpunkten — hybrides Key-Exchange-Verfahren, resistent gegen zukünftige Quantencomputer-Angriffe.

Ende-zu-Ende-Verschlüsselung

ML-KEM-768 · ECDH P-521 · Curve25519 — Trinity Cascade nach NIST FIPS 203. Nachrichten können nur vom Empfänger entschlüsselt werden.

Geräte-basierte Authentifizierung

Ed25519-Keys ausschließlich auf dem Gerät des Nutzers gespeichert — kein Server-Passwort, kein zentrales Credential-Store, kein Phishing-Risiko.

mTLS Monitor-Dashboard

Zugriff auf das Admin-Dashboard ausschließlich mit **personalem Client-Zertifikat** — kein öffentlicher Admin-Bereich, keine Passwort-basierte Authentifizierung.

HIDS auf allen Servern

auditd + Response-Daemon aktiv auf SVR, MON und LAB — automatische Erkennung und Reaktion auf verdächtige Aktivitäten in Echtzeit.

Defense in Depth

UFW · fail2ban · HIDS auf jedem Server — mehrschichtige Absicherung statt Single Point of Failure. Jede Schicht arbeitet unabhängig voneinander.

Autonome KI-Sicherheitsüberwachung

Ufooo — integrierte KI im Monitor-Dashboard — überwacht alle Systeme in Echtzeit, erkennt Anomalien inkl. Zero-Day-Muster und reagiert **vollautonom** (Kick/Ban) ohne menschlichen Eingriff. Kann eigenständig die **UfoooNetiX-MSG App** bedienen und darüber kommunizieren.

Zero-Plaintext nachgewiesen

Live-tcpdump-Verifizierung (14. Mai 2026) — auf **keiner Ebene** ist Nachrichteninhalt lesbar: weder im Netzwerk-Traffic (TLS-Ciphertext), noch in **ScyllaDB · Redis** (Base64-Ciphertext), noch in den **Go-Server-Logs** (nur Fingerprint-Prefix + Message-ID).

4 Zertifizierungsabschluss

✓

Sicherheitsprüfung bestanden

Die **UfoooNetiX-MSG Infrastruktur** wurde am **2. Mai 2026** einem vollständigen, autorisierten Sicherheitsaudit unterzogen und am **14. Mai 2026** um Phase 7 ergänzt. Alle **55 Testfälle** in **7 Prüfphasen** wurden erfolgreich bestanden. Zum Zeitpunkt der Prüfung bestehen **keine offenen Sicherheitslücken**. Die Plattform entspricht den geprüften Sicherheitsstandards.

SYSTEME & ENDPUNKTE

- Homepage ufooonetix.at
- App ufooonetix.at/msg
- App-Server msg.ufooonetix.at:8443
- Monitor monitor.ufooonetix.at
- LAB-Server lab.ufooonetix.at

GEPRÜFTE TECHNOLOGIEN

- TLS 1.3 + Post-Quantum (X25519MLKEM768)
- E2E-Krypto: ML-KEM-768 · ECDH P-521 · X25519
- Ed25519 Authentifizierung · mTLS
- HIDS (auditd) · fail2ban · UFW
- Badge-System · iOS App · Go WebSocket

Durchgeführt von **Vertraulich**

Auftraggeber: **UfoooNetiX**

Angriffsdetails und technische Vektoren sind aus Sicherheitsgründen nicht veröffentlicht.