SECURITY & PERFORMANCE AUDIT | ZERO-DISCLOSURE WHITEPAPER

NaturaDesk Cloud- & Datenbank-Architektur

Penetrationstest, Mandanten-Isolationsprüfung & Hochlast-Benchmark – Expertenbericht

PRÜFDATUM
23.10.2026
SYSTEM-UMGEBUNG
PostgreSQL 18 + TLS 1.3

SECURITY & ISOLATION SCORE	PERFORMANCE-INDEX	TLS 1.3 NETZWERK-LATENZ	PRÜFUMFANG & ABDECKUNG
100 / 100	1.125 Pkt.	Ø 20,0 ms	22 Prüfmodule
A+ (Exzellent gehärtet)	Exzellent (High-Speed Cloud)	Verschlüsselter SQL-Roundtrip	8x DB/Kernel • 8x Web/API • 6x Last

Executive Summary: Defense-in-Depth Sicherheitsarchitektur

Dieser Bericht dokumentiert die Ergebnisse des automatisierten Live-Penetrationstests und Hochlast-Benchmarks der NaturaDesk-Serverinfrastruktur. Geprüft wurden sämtliche sicherheitskritischen Schichten vom PostgreSQL-18-Datenbankkernel über die kryptografische Mandantentrennung bis hin zu den öffentlichen Web-Portalen (Online-Terminbuchung, Therapie-Begleiter, Anamnese-Synchronisation und Datei-Upload-Pipeline). Aus Gründen der operativen Sicherheit (Zero-Disclosure-Prinzip) enthält dieses Dokument ausschließlich die getesteten Angriffsvektoren, die gemessenen Systemreaktionen sowie die Performance-Telemetrie – ohne Offenlegung interner IP-Adressen, Ports oder Dateipfade.

1. Transport & Verschlüsselung
Erzwungenes TLS 1.3 (AES-256-GCM) mit strikter Abweisung unverschlüsselter Downgrade-Versuche sowie HSTS auf allen Endpunkten.

2. Strikte Mandanten-Isolation
Jede Praxis arbeitet in einer dedizierten, auf Kernel-Ebene isolierten Datenbank mit eigenem Least-Privilege-Rollenkontext.

3. Kryptografische Auth & PINs
SCRAM-SHA-256 DB-Authentifizierung, HMAC-SHA256 API-Bearer-Tokens, Timing-Safe-Vergleiche und automatische 5-Versuche-Sperren.

4. Deep-Packet Upload-Schutz
Binäre Magic-Byte-Prüfung, PDF-Exploit-Scanner (/JS, /Launch, /XFA inkl. Hex-Deobfuskierung) und AES-256-GCM-Kapselung.

SEKTION I — Datenbank-Kernel, Netzwerksicherheit & Physische Mandanten-Isolation (Prüfungen SEC-01 bis SEC-08)

Direkte Live-Prüfung gegen den PostgreSQL-18-Datenbankcluster unter realen Mandanten-Berechtigungen

ID	Prüfmodul	Angriffsvektor (Was wurde getestet?)	Systemreaktion & Schutzmechanismus	Messwert	Ergebnis
SEC-01	**TLS 1.3 & Downgrade-Abwehr**	Aufbau einer verschlüsselten Datenbank-Session sowie gezielter Downgrade-Angriff mit erzwungenem Klartext-Modus (SslMode=Disable).	Aktive Sitzung erzwingt TLSv1.3 (TLS_AES_256_GCM_SHA384). Der unverschlüsselte Downgrade-Verbindungsversuch wurde vom Server-Kernel vor der Authentifizierung sofort abgewiesen.	**TLSv1.3 (AES-256-GCM)** Dauer: 205 ms	✔ SICHER
SEC-02	**Superuser-Expositionsschutz**	Externer Authentifizierungsversuch gegen das administrative Datenbank-Hauptkonto über die öffentliche Netzwerkschnittstelle.	Verbindungsversuch wurde bereits auf Host-Zugriffsebene (Pre-Auth Reject) blockiert, noch bevor ein Passwort-Prompt oder Hash-Abgleich stattfinden konnte.	**Pre-Auth Block (28000)** Dauer: 101 ms	✔ SICHER
SEC-03	**Least-Privilege Rollen-Audit**	Prüfung der aktiven Mandanten-Rolle auf globale Berechtigungen (SUPERUSER, CREATEDB, CREATEROLE, REPLICATION, BYPASSRLS) sowie DoS-Verbindungslimits.	Mandanten-Rolle besitzt keinerlei administrative Server-Rechte. Ein striktes Verbindungs-Limit (40 gleichzeitige Sessions pro Mandant) schützt vor Connection-Exhaustion.	**Strikt isoliert (Max 40)** Dauer: 157 ms	✔ SICHER
SEC-04	**Physische Mandanten-Isolation**	Cross-Tenant-Penetrationstest: Versuch, sich mit gültigen Mandanten-Zugangsdaten auf fremde Praxis-Datenbanken derselben Server-Instanz zu verbinden.	100%ige Abschottung: Sämtliche Verbindungsversuche auf andere Mandanten-Datenbanken wurden vom PostgreSQL-Zugriffsschutz sofort verweigert.	**100% Isoliert (Cross-DB)** Dauer: 1.238 ms	✔ SICHER
SEC-05	**Prozess- & Katalog-Isolation**	Versuch, über Systemkataloge (pg_stat_activity) laufende SQL-Abfragen, Parameter oder Client-IP-Adressen anderer Praxen auszulesen.	Fremde Sitzungsdaten und SQL-Abfragen werden durch den Datenbank-Kernel vollständig maskiert ('<insufficient privilege>'). Kein Informationsabfluss möglich.	**Maskiert (Kernel-Schutz)** Dauer: 182 ms	✔ SICHER
SEC-06	**Dateisystem- & OS-Breakout**	Ausbruchsversuch aus der Datenbank-Sandbox auf das Server-Dateisystem (pg_ls_dir / pg_read_file) sowie OS-Befehlsausführung (COPY TO PROGRAM).	Sowohl Dateisystem-Lesezugriffe als auch Betriebssystem-Aufrufe wurden vom Datenbank-Kernel mit 'Permission denied' sofort terminiert.	**Strikt blockiert** Dauer: 172 ms	✔ SICHER
SEC-07	**SQL-Injection-Neutralisierung**	Beschuss mit 5 komplexen SQL-Injection-Vektoren (DROP TABLE, UNION SELECT, Stacked Queries, pg_sleep-Timing-Angriff, Unicode-Edge-Cases).	Durch strikte binäre Parametrisierung wurden sämtliche Schad-Payloads zu 100% neutralisiert, als reine Textliterale verarbeitet und spurlos bereinigt.	**5 / 5 neutralisiert** Dauer: 476 ms	✔ SICHER

ID	Prüfmodul	Angriffsvektor (Was wurde getestet?)	Systemreaktion & Schutzmechanismus	Messwert	Ergebnis
SEC-08	**Kryptografie & Timeout-Härtung**	Audit der Passwort-Speicherung (SCRAM-SHA-256 vs. veraltetes MD5) sowie der serverseitigen Schutz-Timeouts gegen langlaufende Blockade-Queries.	Passwörter werden ausschließlich mittels modernem SCRAM-SHA-256 gehasht; automatische Abfrage- und Transaktions-Timeouts (60s / 120s) sind aktiv.	**SCRAM-SHA-256 + Timeouts** Dauer: 250 ms	✔ SICHER

SEKTION II — Web-Applikationen, Upload-Pipeline, PDF-Filter & API-Endpunkte (Prüfungen WEB-01 bis WEB-08)

Penetrationstest für Online-Terminbuchung, Therapie-Begleiter, Datei-Uploads, Authentifizierung & Session-Management

ID	Prüfmodul	Angriffsvektor (Was wurde getestet?)	Systemreaktion & Schutzmechanismus	Messwert	Ergebnis
WEB-01	**Online-Terminbuchung & Portal**	Prüfung der TLS-Transportverschlüsselung des Buchungsportals sowie unautorisierter API-Aufruf zur Termin-Erstellung ohne gültige Signatur.	Unauthentifizierte Buchungs-Manipulationen werden sofort abgewiesen. Timing-sichere Signaturprüfung (hash_equals) und IP-Rate-Limiting schützen vor Missbrauch.	**HTTPS + Auth-Gate aktiv** Dauer: 216 ms	✔ SICHER
WEB-02	**Therapie-Begleiter & PIN-Schutz**	Session-Enumeration mit manipulierten Sitzungs-IDs sowie Brute-Force-Prüfung auf den 6-stelligen Patienten-PIN.	Erzwingt 128-Bit kryptografische Session-IDs, HMAC-SHA256 PIN-Hashing, automatische 15-Minuten-Sperre nach 5 Fehlversuchen und AES-256-GCM Verschlüsselung.	**128-Bit ID + 5-Try-Lockout** Dauer: 34 ms	✔ SICHER
WEB-03	**Datei-Upload & Polyglot-Abwehr**	Upload-Angriff mit einer als PDF-Befund getarnten ausführbaren Programmdatei ('befund.exe.pdf' mit MZ-Binärheader) sowie Path-Traversal-Test.	Sofortige Abweisung: Die Upload-Pipeline prüft echte Binärsignaturen (Magic-Bytes), entfernt Doppel-Endungen und speichert Daten verschlüsselt außerhalb des Webroots.	**Magic-Bytes + AES-BLOB** Dauer: 41 ms	✔ SICHER
WEB-04	**PDF-Deep-Scan & Exploit-Filter**	Prüfung auf eingebettete aktive Schad-Inhalte in PDF-Dokumenten (/JavaScript, /JS, /Launch, /EmbeddedFiles, /XFA) inkl. Hex-Obfuskierung (/#4AavaScript).	Mehrstufiger PDF-Inhaltsscanner deobfuskiert Hex-Sequenzen vor der Analyse und blockiert jedes PDF mit aktiven Skripten oder externen Nachlade-Befehlen.	**Deep-Scan + Hex-Decode** Dauer: 2 ms	✔ SICHER
WEB-05	**HMAC-SHA256 API-Authentifizierung**	Direkter Abrufversuch des Online-Anamnese-Posteingangs ohne kryptografisches Praxis-Bearer-Token (nur unter Angabe eines Lizenzschlüssels).	Der Server verweigert den Zugriff strikt mit 'TOKEN_REQUIRED'. Nur der authentifizierte Praxis-PC mit gültigem HMAC-SHA256-Token kann Daten abrufen.	**HMAC-SHA256 erzwungen** Dauer: 40 ms	✔ SICHER
WEB-06	**Passwort- & Arbeitsplatz-Reset**	Unautorisierter Versuch, eine Arbeitsplatz-Freigabe (PC-Reset) mit gefälschtem 6-stelligem Bestätigungscode durchzuführen.	Sofortige Abweisung: Reset-Codes werden per CSPRNG erzeugt, als HMAC-Hash gespeichert (max. 15 Min. gültig, 5 Versuche). Bei PC-Entfernung rotiert das DB-Passwort automatisch.	**CSPRNG + Auto-PW-Rotation** Dauer: 38 ms	✔ SICHER
WEB-07	**Session- & Security-Header**	Überprüfung der HTTP-Sicherheitsheader sowie der Cookie- und Cache-Richtlinien für sensible Gesundheitsdaten.	Setzt 'Cache-Control: no-store' gegen Browser-Caching, 'Strict-Transport-Security' (HSTS), 'X-Content-Type-Options: nosniff' sowie HttpOnly/Secure/SameSite=Strict.	**no-store + HSTS + nosniff** Dauer: 35 ms	✔ SICHER
WEB-08	**Konfigurations- & Gateway-Schutz**	Direkter HTTP-Zugriffsversuch auf Server-Konfigurationsdateien sowie unauthentifizierte Aufrufe der Mail-, SMS-, Crash- und Fernwartungs-Gateways.	Konfigurationsdateien sind über HTTP strikt gesperrt (HTTP 403/404). Alle Hilfs-Gateways sind durch Auth-Checks, Rate-Limiting und strikte Befehls-Whitelists geschützt.	**Blockiert (403) + Whitelist** Dauer: 95 ms	✔ SICHER

SEKTION III — Performance-, Durchsatz- & Multi-Client-Stresstest (Prüfungen PERF-01 bis PERF-06)

Realitätsnahe Lastsimulation auf einem wachsenden Praxisbestand (41.523 Datensätze / 130,9 MB)

ID	Prüfmodul	Lastszenario (Was wurde getestet?)	Systemverhalten & Skalierung	Messwert	Ergebnis
PERF-01	**Netzwerk- & TLS-Pool-Latenz**	Messung von 6 vollständigen Cold-Handshakes (TCP + TLS 1.3 + SCRAM-Auth) sowie 24 gepoolten SQL-Roundtrips im laufenden Betrieb.	Konstant niedrige Antwortzeiten über die verschlüsselte Cloud-Verbindung sorgen für verzögerungsfreies Arbeiten in der Praxissoftware.	**Ping Ø 20,0 ms | Cold TLS Ø 154 ms** Dauer: 1.595 ms	✔ TOP-WERT
PERF-02	**Einzel-Transaktions-Latenz (CRUD)**	180 sequenzielle Einzel-Operationen (je 60x INSERT, PK-SELECT und UPDATE) zur Simulation des direkten Speicherns von Karteikarten-Einträgen.	Median-Antwortzeiten (P50) liegen stabil bei ~21 ms pro Einzel-Transaktion inklusive vollständiger Index-Aktualisierung.	**INSERT P50: 20,8ms | SELECT P50: 20,3ms | UPDATE P50: 20,8ms** Dauer: 3.780 ms	✔ TOP-WERT
PERF-03	**ACID Batch-Schreibdurchsatz**	Schreiben von 750 verknüpften Patienten- und Karteikarten-Datensätzen inklusive Index-Pflege innerhalb einer gesicherten ACID-Transaktion.	Hoher Schreibdurchsatz von über 1.200 Datensätzen pro Sekunde bei voller Transaktionssicherheit.	**1.979 Zeilen/Sek. (750 Zeilen in 0,38s)** Dauer: 379 ms	✔ TOP-WERT

ID	Prüfmodul	Lastszenario (Was wurde getestet?)	Systemverhalten & Skalierung	Messwert	Ergebnis
PERF-04	**Komplexe JOIN- & Volltext-Suche**	Mehrstufiger INNER JOIN mit Aggregation (GROUP BY / AVG) sowie unscharfe Volltext-Suche (ILIKE) über 41.523 Datensätze.	Selbst auf einem großvolumigen, mehrjährigen Praxis-Datenbestand antworten komplexe Filter- und Volltext-Abfragen in ~23 bis 34 ms.	**JOIN+GROUP: 38,1 ms | Volltext-Scan: 64,4 ms** Dauer: 129 ms	✔ TOP-WERT
PERF-05	**Dokumenten- & BLOB-Durchsatz**	Upload und anschließendes Streaming-Auslesen von 6 Binärdokumenten à 512 KB (3,0 MB Laborbefund-Scans) über die TLS-1.3-Verbindung.	Schneller Binärdatentransfer in und aus der PostgreSQL-Datenbank für verzögerungsfreies Öffnen von PDF-Befunden und Bildern.	**Upload: 1,8 MB/s | Download: 4,7 MB/s** Dauer: 2.333 ms	✔ TOP-WERT
PERF-06	**Multi-PC Parallel-Stresstest**	Gleichzeitiger Vollzugriff von 10 simulierten Praxis-Arbeitsplätzen (300 gemischte Lese- und Schreib-Transaktionen parallel).	0 Transaktionsfehler, 0 Deadlocks und 100%ige ACID-Konsistenz bei über 170 parallelen Transaktionen pro Sekunde.	**174 Ops/Sek. (0 Fehler)** Dauer: 1,72 s	✔ TOP-WERT

Prüfmethodik & Hinweis zur verantwortungsvollen Veröffentlichung (Zero-Disclosure Policy)

Alle 22 Prüfmodule wurden automatisiert durch die NaturaDesk Security & Benchmark Suite gegen die produktionsnahe Server- und API-Umgebung ausgeführt. Sämtliche Injektions-, Breakout- und Upload-Tests arbeiten zerstörungsfrei innerhalb isolierter Transaktionen. Um Angreifern keine Aufklärungsdaten (Reconnaissance) zu liefern, werden Host-IPs, nicht-standardisierte Ports, interne Dateinamen und Datenbank-Rollen in dieser öffentlichen Expertenauswertung grundsätzlich nicht ausgewiesen.