DKSchV Dini · Cyber-Security

OFFENSIVE SECURITY & REVISIONSSICHERE AUDITS

Dokument: RoE-PENTEST-CH-2026
Rechtsstand: revDSG / Art. 143/143bis StGB
Gültigkeit: Schweizerische Eidgenossenschaft

RECHTSVERBINDLICHE VEREINBARUNG

Vereinbarung über die Durchführung eines Penetrationstests

Rules of Engagement (RoE) & Rechtliche Ermächtigungserklärung

AUFTRAGGEBER (KUNDE / SYSTEMINHABER)

Firma: .....
Strasse / Nr.: .....
PLZ / Ort: .....
Vertretungsberechtigt: .....
Funktion: .....
(nachfolgend «Auftraggeber» genannt)

AUFTRAGNEHMER (PRÜFER)

Firma: DKSchV Dini (DKSchV Schweiz)
Inhaber: Andreas Dini
Adresse: Bammattenweg 19, CH-3904 Naters (Wallis)
E-Mail: info@dkschv.ch
Telefon (24/7): +41 79 844 66 69
(nachfolgend «DKSchV» genannt)

Präambel: Der Auftraggeber beabsichtigt, die Widerstandsfähigkeit seiner IT-Infrastruktur durch eine simulierte, kontrollierte Cyber-Sicherheitsanalyse (Penetrationstest) überprüfen zu lassen. Ziel ist das rechtzeitige Aufdecken von Verwundbarkeiten und Konfigurationsfehlern vor böswilligen Angreifern.

1. AUSDRÜCKLICHE ERMÄCHTIGUNG & STRAFFREIHEIT (ART. 143 & 143BIS STGB)

1.1. Der Auftraggeber bestätigt an Eides statt, uneingeschränkter Eigentümer, Betreiber oder hierzu vollumfänglich und schriftlich bevollmächtigter Verfügungsberechtigter der in Abschnitt 2 definierten Zielsysteme (Scope) zu sein.

1.2. Der Auftraggeber ermächtigt DKSchV hiermit ausdrücklich und unwiderruflich für die Dauer des Testzeitraums, die freigegebenen Systeme mit Methoden des ethischen Hackings zu analysieren, Schutzmechanismen zu überprüfen und Schwachstellen kontrolliert nachzuweisen.

1.3. Diese schriftliche Vereinbarung gilt als **ausdrückliche Einwilligung des Berechtigten**. Die Prüfhandlungen von DKSchV erfolgen somit befugt und unterliegen **nicht** den Schweizer Straftatbeständen von Art. 143 StGB (Unbefugte Datenbeschaffung) oder Art. 143bis StGB (Unbefugtes Eindringen in ein Datenverarbeitungssystem).

2. ZIELDEFINITION & FREIGEGEBENER PRÜFUMFANG (SCOPE)

Folgende Systeme sind **ausdrücklich für die Sicherheitsanalyse freigegeben (In-Scope)**:

Pos.	Externe IP-Adresse / IP-Range	Domain / Subdomain / FQDN	Systembeschreibung
01	.....	.....	Haupt-Firewall / Gateway
02	.....	.....	Firmen-Website / Webshop
03	.....	.....	VPN-Gateway / Remote Access
04	.....	.....	Mailserver / MX-Record

Pos.	Externe IP-Adresse / IP-Range	Domain / Subdomain / FQDN	Systembeschreibung
05	.....	.....	Cloud-Instanz / API-Endpoint

Strengstens ausgeschlossen (Out-of-Scope):

- Volumetrische Denial-of-Service-Angriffe (DoS/DDoS), die auf eine dauerhafte Lahmlegung der Bandbreite abzielen.
- Infrastrukturen und Netze Dritter (z. B. Shared-Hosting-Nachbarn, ISP-Uplinks, Dritt-SaaS), für die keine Vollmacht vorliegt.
- Physische Einbruchstests (Social Engineering / Lockpicking vor Ort), sofern nicht explizit gesondert beauftragt.
- Destruktive Aktionen: Es werden keine Daten gelöscht, manipuliert oder verschlüsselt (Ransomware-Simulationen erfolgen rein non-destruktiv via Proof-of-Concept).

DKSchV Dini · Cyber-Security

RULES OF ENGAGEMENT (ROE) · SEITE 2 VON 2

Auftraggeber: .....
Referenz: RoE-PENTEST-CH-2026

3. TESTMETHODIK & ART DER PRÜFUNG

- ☐ **Externer Perimeter-Scan (Blackbox):** Ermittlung aller offenen Ports, Dienste, Banner und veralteten Softwareversionen ohne Vorwissen.
- ☐ **Web-Applikations-Audit (OWASP Top 10):** Prüfung auf Injektionslücken, defekte Authentifizierung, fehlerhafte Autorisierung und Fehlkonfigurationen.
- ☐ **Cloud & Microsoft 365 Baseline Check:** Prüfung auf offene Speicherbereiche (Blobs/Buckets), fehlerhafte Mandanteneinstellungen und Legacy-Auth.
- ☐ **Credential-Leak-Abgleich:** Passive Analyse auf exponierte Firmenpasswörter und kompromittierte Zugangsdaten im Darknet/Breach-Daten.

4. ZEITFENSTER & NOTFALL-ESKALATION (EMERGENCY STOP)

Vereinbarter Testzeitraum:
Von: ..... bis: 2026

Erlaubte Testzeiten:
[ ] 24/7 rund um die Uhr [ ] Nur 19:00 - 06:00 Uhr

🚨 **SOFORTIGER TESTABBRUCH (EMERGENCY STOP PROCEDURE)**

Sollte während der Prüfung eine unvorhergesehene Beeinträchtigung kritischer Betriebsprozesse auftreten, kann der Auftraggeber den Test durch Nennung des vereinbarten Codeworts **augenblicklich stoppen**:

Notfall-Codewort:
_____

DKSchV Notfall-Direktlinie: +41 79 844 66 69

5. VERTRAULICHKEIT (NDA) & DATENSCHUTZ (NDSG / REVDSG)

5.1. DKSchV verpflichtet sich zu uneingeschränkter, zeitlich unbefristeter Vertraulichkeit über alle im Rahmen der Prüfung erlangten Geschäftsgeheimnisse, Netzwerktopologien und identifizierten Sicherheitslücken.

5.2. Erfasste Protokolle, Belege und Berichte werden ausschliesslich auf isolierten, verschlüsselten Schweizer Systemen gehalten und nach Projektabschluss sowie Freigabe durch den Auftraggeber revisionssicher vernichtet.

6. HAFTUNGSBEGRENZUNG & DATENSICHERUNGSPFLICHT DES KUNDEN

6.1. DKSchV wendet bei sämtlichen Analysen höchste handwerkliche und methodische Sorgfalt an. Dennoch können instabile Zielsysteme in seltenen Einzelfällen auf Scans mit Dienstneustarts oder Fehlern reagieren.

6.2. **Backup-Garantie des Auftraggebers:** Der Auftraggeber verpflichtet sich ausdrücklich, unmittelbar vor Beginn der Testaktivitäten eine **vollständige, geprüfte und wiederherstellbare Datensicherung** aller im Scope befindlichen Systeme durchzuführen.

6.3. Die Haftung von DKSchV für leichte Fahrlässigkeit, indirekte Schäden, Betriebsunterbrüche oder entgangenen Gewinn wird im gesetzlich zulässigen Rahmen (Art. 100 OR) ausgeschlossen.

7. ANWENDBARES RECHT & GERICHTSSTAND

Auf diese Vereinbarung ist ausschliesslich **Schweizer Recht** anwendbar. Ausschliesslicher Gerichtsstand für alle Streitigkeiten ist der Sitz von DKSchV Dini in **Brig / Naters (Kanton Wallis)**.

Ort, Datum: .....

Für den Auftraggeber (Kunde):

Rechtsgültige Unterschrift & Firmenstempel

NAME & FUNKTION IN BLOCKSCHRIFT

Für den Auftragnehmer (DKSchV Dini):

Prüfungsleitung & Vertraulichkeitszusicherung

ANDREAS DINI, INHABER DKSCHV DINI