MUSTERMANN
IT-SERVICES

IT-Security Konzept Rechtsanwaltskanzlei

KONZEPT · KO-2025-003

Projekt:	IT-Security Audit & Härtung
Kunde:	Richter & Partner Rechtsanwälte
Version:	1.0
Status:	DRAFT
Erstellt:	2025-01-08

Security · DSGVO · Kanzlei · Compliance

Inhaltsverzeichnis

1 Executive Summary

Die IT-Infrastruktur der Kanzlei Richter & Partner weist kritische Sicherheitslücken auf, die ein erhebliches Risiko für Mandantendaten darstellen. Dieses Konzept beschreibt die identifizierten Schwachstellen und empfohlene Maßnahmen zur Härtung der Systeme.

Kritische Findings: 3 kritische, 7 hohe, 12 mittlere Schwachstellen identifiziert. Sofortiges Handeln erforderlich.

2 Ausgangssituation

2.1 Kanzleiprofil

- **Mitarbeiter:** 15 Anwälte, 8 Sekretariat/Verwaltung
- **Standorte:** Berlin (Hauptsitz), München (Zweigstelle)
- **IT-Infrastruktur:** Lokaler Windows-Server, Microsoft 365, Kanzleisoftware RA-MICRO
- **Mandantendaten:** Ca. 3.500 aktive Mandate, sensible Daten (Strafrecht, Familienrecht)

2.2 Regulatorische Anforderungen

Als Rechtsanwaltskanzlei unterliegen Sie besonderen Anforderungen:

- **BRAO §43a:** Verschwiegenheitspflicht
- **DSGVO Art. 32:** Technische und organisatorische Maßnahmen
- **BDSG §64:** Anforderungen an Auftragsverarbeiter
- **Berufsrechtliche Vorgaben:** Hinweise der Rechtsanwaltskammern zur IT-Sicherheit

3 Kritische Findings

3.1 Finding 1: Keine Multi-Faktor-Authentifizierung

Risiko: KRITISCH

Microsoft 365 und RA-MICRO sind nur mit Benutzername/Passwort geschützt. Bei Kompromittierung eines Passworts (Phishing, Leak) hat der Angreifer vollen Zugriff auf Mandantendaten.

Empfehlung: MFA für alle Benutzer aktivieren (Microsoft Authenticator oder Hardware-Token)

3.2 Finding 2: Veraltete Server-Software

Risiko: KRITISCH

Der lokale Windows Server 2012 R2 erhält seit Oktober 2023 keine Sicherheitsupdates mehr. Bekannte Schwachstellen werden aktiv ausgenutzt.

Empfehlung: Migration auf Windows Server 2022 oder Cloud-Migration

3.3 Finding 3: Unverschlüsselte Backup-Festplatten

Risiko: KRITISCH

Die USB-Festplatten für Backups sind nicht verschlüsselt. Bei Diebstahl oder Verlust sind alle Mandantendaten kompromittiert.

Empfehlung: BitLocker-Verschlüsselung aktivieren, besser: Cloud-Backup mit Verschlüsselung

4 Maßnahmenplan

4.1 Phase 1: Sofortmaßnahmen (Woche 1-2)

Nr.	Maßnahme	Priorität
1.1	MFA für alle Microsoft 365 Konten aktivieren	Kritisch
1.2	Passwort-Reset für alle Benutzer erzwingen	Kritisch
1.3	Backup-Festplatten verschlüsseln	Kritisch
1.4	Firewall-Regeln überprüfen und härten	Hoch
1.5	Admin-Passwörter ändern	Hoch

4.2 Phase 2: Kurzfristige Maßnahmen (Woche 3-6)

Nr.	Maßnahme	Priorität
2.1	Server-Migration planen (2012 R2 → 2022)	Kritisch
2.2	E-Mail-Security konfigurieren (SPF, DKIM, DMARC)	Hoch
2.3	Endpoint Protection auf allen Clients	Hoch
2.4	VPN für Remote-Zugriff einrichten	Hoch
2.5	Berechtigungskonzept überarbeiten	Mittel

4.3 Phase 3: Mittelfristige Maßnahmen (Monat 2-3)

Nr.	Maßnahme	Priorität
3.1	Server-Migration durchführen	Kritisch
3.2	Cloud-Backup-Lösung implementieren	Hoch
3.3	Security-Awareness-Schulung	Hoch
3.4	Incident-Response-Plan erstellen	Mittel

3.5	Regelmäßige Schwachstellenscans einrichten	Mittel

5 DSGVO-Compliance

5.1 Technische Maßnahmen (Art. 32 DSGVO)

Maßnahme	Status	Ziel
Verschlüsselung ruhender Daten	❌ Fehlt	✓
Verschlüsselung bei Übertragung (TLS)	⚠ Teilweise	✓
Zugriffskontrolle / MFA	❌ Fehlt	✓
Regelmäßige Backups	✓ Vorhanden	✓
Disaster Recovery Plan	❌ Fehlt	✓
Logging und Monitoring	❌ Fehlt	✓

5.2 Organisatorische Maßnahmen

- **Mitarbeiterschulung:** Jährliche Security-Awareness-Schulung
- **Richtlinien:** IT-Sicherheitsrichtlinie, Passwort-Policy, Clean-Desk-Policy
- **Verträge:** AVV mit allen IT-Dienstleistern prüfen

6 Investitionsübersicht

6.1 Einmalige Kosten

Position	Betrag
Security Assessment & Pentest	10.600 EUR
Server-Migration (Hardware + Lizenzen)	8.500 EUR
Firewall (Sophos XGS 2100)	2.800 EUR
Implementierung Härtungsmaßnahmen	7.000 EUR
Security-Awareness-Schulung	890 EUR
Dokumentation	1.200 EUR
Summe netto	**30.990 EUR**

6.2 Laufende Kosten (monatlich)

Position	Betrag

Managed Detection & Response (MDR)	450 EUR
Cloud-Backup (1 TB)	79 EUR
Microsoft 365 E5 Security (23 User)	299 EUR
Summe monatlich	**828 EUR**

7 Return on Investment

7.1 Risikobewertung ohne Maßnahmen

- **Wahrscheinlichkeit eines Incidents:** 60% innerhalb von 12 Monaten
- **Durchschnittlicher Schaden:** 150.000 - 500.000 EUR
  - Forensik und Wiederherstellung: 30.000 EUR
  - Meldung an Aufsichtsbehörde, Mandanten: 20.000 EUR
  - Reputationsschaden: schwer quantifizierbar
  - Mögliche DSGVO-Bußgelder: bis 4% Jahresumsatz

7.2 ROI-Berechnung

Erwarteter Schaden ohne Maßnahmen: 60% × 250.000 EUR = **150.000 EUR**

Investition in Security: 31.000 EUR + 12 × 828 EUR = **40.936 EUR** (Jahr 1)

Netto-Ersparnis: ca. 109.000 EUR (konservativ geschätzt)

8 Nächste Schritte

1. **Freigabe** dieses Konzepts durch die Kanzleileitung
2. **Beauftragung** der Sofortmaßnahmen
3. **Kickoff-Termin** zur Detailplanung
4. **Start Phase 1** innerhalb von 5 Werktagen

Vertraulichkeit: Dieses Dokument enthält sensible Informationen über Sicherheitslücken und ist ausschließlich für die Geschäftsleitung bestimmt.