Work smarter, not harder!

cloudANWALT

LEITFADEN

IT-Sicherheit für Rechtsanwaltskanzleien im digitalen Zeitalter

Warum Sie jetzt auf die Cloud setzen sollten

cloudANWALT

Inhaltsverzeichnis

cloudANWALT

Warum Rechtsanwaltskanzleien jetzt auf die Cloud setzen sollten

Rechtsanwaltskanzleien stehen vor der Herausforderung, ihre **sensiblen Daten umfassend zu schützen**. Lokale Server bieten längst nicht mehr den nötigen Schutz gegen Cyberangriffe, Datenverluste oder technische Ausfälle.

Doch es gibt eine **sichere Alternative**: **moderne Cloud-Technologie**.

Mit Cloud-Lösungen können Sie Ihre Kanzlei nicht nur **besser gegen externe Bedrohungen absichern**, sondern auch Ihre **IT-Infrastruktur zukunftssicher gestalten**.

In diesem Leitfaden erfahren Sie, wie Sie **Ihre Daten und die Ihrer Mandanten optimal schützen**. Zudem erhalten Sie eine **praktische IT-Checkliste**, mit der Sie überprüfen können, ob Ihr aktuelles IT-System den steigenden Anforderungen an die IT-Sicherheit gerecht wird.

cloudANWALT

Die 5 größten Sicherheitsrisiken für Rechtsanwaltskanzleien

1. Serverstandort

Lokale Server stehen häufig in **unzureichend geschützten Räumen**. Sie sind anfällig für **unberechtigte Zugriffe** und **physische Gefahren** wie Feuer, Hochwasser oder Einbrüche, da diese Serverräume selten rund um die Uhr überwacht oder klimatisch abgesichert sind. Ein umfassender Schutz vor diesen Risiken ist für viele Kanzleien schwer zu gewährleisten.

2. Nutzerverhalten

Das **Verhalten der Mitarbeiter** kann eine erhebliche Sicherheitslücke darstellen. Fehlverhalten, wie das **Öffnen von Phishing-E-Mails** oder das **Herunterladen schadhafter Software**, kann das gesamte Netzwerk gefährden. Schulungen zum sicheren Umgang mit IT-Systemen sind hier unerlässlich.

3. Fehlende Updates

Sicherheitsupdates spielen eine zentrale Rolle, um Schwachstellen im System zu beheben. Wenn diese **nicht regelmäßig installiert** werden, entstehen Lücken, die von Cyberkriminellen ausgenutzt werden können. Ein **veraltetes System** ist ein offenes Ziel.

4. Unzureichender Schutz durch die Firewall

Auch **Firewalls und Spamfilter** müssen regelmäßig aktualisiert werden. Eine **veraltete Sicherheitsinfrastruktur** kann nicht mit den ständig wachsenden Bedrohungen im Cyberraum Schritt halten und bietet keinen ausreichenden Schutz vor Angriffen.

5. Mangelhafte Datensicherung

Datensicherungen sind der Schlüssel zur Wiederherstellung nach einem Vorfall. Doch viele Kanzleien **sichern ihre Daten entweder gar nicht oder nur auf einem einzigen Medium**. Dies erhöht das Risiko eines **vollständigen Datenverlusts**, sollte dieses Medium beschädigt oder gestohlen werden.

cloudANWALT

Cloud vs. lokaler Server - ein Sicherheitsvergleich

	Cloudlösung	Herkömmliche Serverlösung
Physische Gebäude-sicherheit	· Hochsicherheitsrechenzentrum mit Videoüberwachung · Protokolliertes, biometrisches Zutrittssystem · Brandschutz	· Büroräume · Häufig keine gesicherte IT-Infrastruktur · Keine permanente Überwachung
Überwachung	Permanente 24/7-Überwachung durch automatisierte Systeme und Personal	Überwachung nur während der Bürozeiten, oft abhängig vom Personal
Datensicherheit	Regelmäßige und automatisierte Updates ohne Arbeitsunterbrechung	Updates manuell, können den Betrieb stören, werden oft verzögert oder nicht durchgeführt
Speicherung der Daten	· Regelmäßige Backups · Georedundanz: Daten weden in mehreren, geografisch getrennten Rechenzentren gespeichert	· Oft keine Redundanz · Risiko eines Ausfalls der Backup Funktion
Ausfallsicherheit	· Vollständige Redundanz aller Systemkomponenten · Schnelle Wiederherstellung im Notfall	· Risiko eines längeren Ausfalls bei Hardware-Schäden · keine automatische Redundanz
Firewall	· Mehrstufiges Firewallkonzept · Kontinuierliches Monitoring	· Oft einfache, nicht redundante Firewalls · Seltene Wartung
Endgeräte der Nutzer	· Wartungsvertrag: Regelmäßige Updates für Betriebssysteme und Anti–Virus Software · Minimierte Sicherheitslücken	· Unsichere, nicht regelmäßig gewartete Geräte · Anfälligkeit für Sicherheitslücken
Arbeitsaufwand und Verantwortung	IT-Spezialisten des Cloud-Anbieters übernehmen Wartung, Überwachung und Updates	Eigenverantwortung der Kanzlei für Wartung, Updates und Sicherheit

cloudANWALT

So schützt die Cloud Ihre sensiblen Daten: IT-Sicherheitsstandards für Rechtsanwaltskanzleien

Mit dieser Checkliste können Sie überprüfen, ob Ihre aktuelle IT-Lösung alle relevanten Sicherheitsstandards erfüllt oder ob Handlungsbedarf besteht.

Ihre Checkliste für IT-Sicherheit

Sicherheitskriterien	meine derzeitige Lösung	Cloudlösung
Die ISO 27001 Norm für physische Sicherheit wird erfüllt (zB Löschanlage)		✓
Mehrstufige Sicherheitsvorkehrungen sind vorhanden		✓
24/7 Überwachung der Serverräume		✓
Schutz der Endgeräte		✓
Georedundante Datensicherung an verschiedenen Standorten in Österreich		✓
Regelmäßige Hardware-Upgrades ohne Zusatzaufwand		✓
Automatisierte Software-Wartung und Updates		✓
Backups ermöglichen die schnelle Wiederherstellung eines kompromittierten Sytems		✓

Hinweis zur Checkliste IT-Sicherheit:
Ein zentraler Aspekt der IT-Sicherheit ist die Schulung des Personals. Die besten Technologien können nur dann effektiv sein, wenn die Mitarbeiter über ein ausreichendes Sicherheitsbewusstsein verfügen. Regelmäßige Schulungen und Sensibilisierungsmaßnahmen sind daher unerlässlich, um das Risiko menschlicher Fehler zu minimieren und ein sicheres Arbeitsumfeld zu schaffen. Investieren Sie in die Weiterbildung Ihres Teams, um die Sicherheitskultur in Ihrer Kanzlei nachhaltig zu stärken.

Ihr sicherer Weg in die Cloud

1. Beratung und Angebotseinholung

Der erste Schritt in Richtung Cloud-Transformation ist die **individuelle Beratung**. Hierbei wird ermittelt, welche **Anforderungen** Ihre Kanzlei hat und welche Lösungen am besten zu Ihren Bedürfnissen passen. Auf dieser Basis erhalten Sie ein **maßgeschneidertes Angebot**.

2. Planung der Umstellung

In dieser Phase erfolgt die **detaillierte Planung der Migration**. Es werden alle relevanten Daten und Prozesse analysiert, um einen **reibungslosen Übergang** sicherzustellen. Ein gut durchdachter Plan ist entscheidend, um mögliche Störungen im Betrieb zu minimieren.

3. Datenübernahme und Konfiguration

Im Rahmen der Datenübernahme werden Ihre **vorhandenen Informationen in die Cloud transferiert** und entsprechend konfiguriert. Dies beinhaltet die **Anpassung der Systeme** an die **spezifischen Anforderungen** Ihrer Kanzlei, um eine **optimale Funktionalität** zu gewährleisten.

4. Echtbetrieb und Support

Nach **erfolgreicher Migration** in die Cloud beginnt der **Echtbetrieb**. Hier stehen Ihnen Experten zur Seite, um sicherzustellen, dass alles reibungslos läuft. Bei Fragen oder Problemen erhalten Sie **umfassenden Support**, um Ihre Rechtsanwaltskanzlei **optimal zu unterstützen**.

cloudANWALT

Komplettlösung für Rechtsanwaltskanzleien

Wenn Sie über den Wechsel in die Cloud nachdenken, ist es entscheidend, einen **erfahrenen Partner** an Ihrer Seite zu haben.

Mit cloudANWALT profitieren Sie von:

- Einfacher und schneller Einrichtung
- Startklar innerhalb von 10 Werktagen
- Maximaler Sicherheit
- Inklusive Microsoft Office und Antivirus
- Mehrstufiger Datensicherung

cloudANWALT ist ein Produkt der Business Data Solutions GmbH, die als IT-Systemhaus **seit über 25 Jahren** als Advokat-Partner Rechtsanwaltskanzleien betreut.

Möchten Sie mehr erfahren?

Wir beraten Sie gerne telefonisch oder persönlich.
sales@bds.info +43 2622 82 570

Mag. Gerald Wondra
Key Account Manager
M +43 664 358 20 75
g.wondra@bds.info

bds

Business Data Solutions GmbH
Fischauergasse 150, 2700 Wr. Neustadt
Büro Wien: Hauffgasse 20/4, 1110 Wien

cloudanwalt.info