Leitfaden: IT-Sicherheit & Ausfallsicherheit in der Arztpraxis

Ein Praxis-Guide für den niedergelassenen Gesundheitsbereich in Österreich

1. Einleitung: Sicherheit bedeutet Betriebsfähigkeit

In der modernen Ordination ist IT-Sicherheit gleichbedeutend mit Versorgungssicherheit. Auch wenn Gesundheitsdaten sehr wertvoll sind, sind nicht immer internationale Hacker das größte Risiko. In der Realität führen oft technische Defekte (z. B. Festplattencrash), physischer Diebstahl von Geräten oder unbeabsichtigte Fehlbedienungen zu Datenverlusten und Praxisstillstand.

Dieser Leitfaden unterstützt Sie dabei, Ihre Ordination sowohl gegen Cyber-Kriminalität als auch gegen alltägliche technische Risiken abzusichern. Er beschreibt ein Mindestmaß an Maßnahmen, die bereits einen Großteil der Gefahren abwehren. Ziel ist der Schutz Ihrer Patienten, die Einhaltung der DSGVO und die wirtschaftliche Stabilität Ihrer Praxis.

⚠ **WICHTIG:** Die in dieser Richtlinie (Guideline) aufgeführten Maßnahmen definieren lediglich einen Mindeststandard für die IT-Sicherheit in Ordinationen. Sie stellen weder eine Garantie für Vollständigkeit dar noch begründen sie einen Anspruch auf eine vollumfänglich ausreichende IT-Sicherheit. Da jede Praxis sowohl organisatorisch als auch technisch individuelle Rahmenbedingungen aufweist, erfordert die Gewährleistung angemessener Sicherheit eine separate Betrachtung und die Implementierung maßgeschneiderter Sicherheitsmaßnahmen.

Handlungsempfehlung: Wir empfehlen Ihnen, sich die notwendige Zeit zu nehmen, um alle Punkte dieser Richtlinie (Guideline) für Ihre Ordination sorgfältig zu prüfen. Diskutieren Sie offene Fragestellungen gegebenenfalls mit Ihrem IT-Dienstleister oder konsultieren Sie einen externen Fachexperten für eine fundierte Klärung. Lassen Sie sich die Umsetzung aller relevanten Punkte schriftlich bestätigen und protokollieren Sie diesen Vorgang nachweisbar.

2. Die Basis: Verfügbarkeit sichern (Hardware & Infrastruktur)

Bevor wir über Hacker sprechen: Was passiert, wenn die Technik einfach versagt? Jede Hardware hat ein Ablaufdatum und kann jederzeit funktionsfähig sein.

- **Schutz vor Festplatten-Ausfall (Redundanz):** Ihr Server bzw. der Hauptcomputer mit der Patientendatenbank sollte über gespiegelte Festplatten verfügen (ein sogenanntes RAID-System). Fällt eine Festplatte fehlerbedingt aus, übernimmt die

andere nahtlos. Der Praxisbetrieb läuft ohne Unterbrechung weiter. Festplatten sind durch die hohe Beanspruchung über die Zeit häufiger als andere Hardware von Ausfällen betroffen. *Hinweis:* Ein RAID ist kein Backup! Wer versehentlich eine Datei löscht, löscht sie auf redundanten Festplatten gleichzeitig.

- **Schutz vor Stromproblemen (USV):** Ein abrupter Stromausfall kann Festplatten oder darauf befindliche Datenbanken beschädigen. Eine unterbrechungsfreie Stromversorgung (USV/Batteriepuffer) schützt Ihre Systeme vor Datenverlust bei Stromausfall oder Spannungsschwankungen (z. B. durch Blitzschlag) und ermöglicht ein sauberes Herunterfahren.
- **Verschlüsselung mobiler Geräte:** Laptops, Tablets und externe Festplatten können verloren gehen oder gestohlen werden. Sind die Geräte verschlüsselt (z. B. mit BitLocker unter Windows), ist der Diebstahl zwar ein finanzieller Schaden, aber **keine meldepflichtige Datenschutzkatastrophe**, da die Daten für Dritte unlesbar sind.
- **Veraltete Hardware (End-of-Life):** Hardware, die älter als 5 Jahre ist, hat ein exponentiell höheres Ausfallrisiko und manche Systeme erhalten oft keine Treiber-Updates mehr. Planen Sie eine rechtzeitige Erneuerung der Komponenten.
- **Netzwerk-Trennung:** Es ist zwingend nötig, das Netzwerk in der Arztpraxis nur für die Verbindung der nötigen Geräte zu verwenden! - Stellen Sie sicher, dass das Gäste-WLAN für Ihre Patient:innen strikt getrennt ist und niemals Zugriff auf die Praxis Infrastruktur erhält. Vergewissern Sie sich auch, dass keine Netzwerkanschlüsse unbeaufsichtigt verwendet werden können (z.B. über Außenanschlüsse am Haus). Verwendete Sicherheitskameras oder andere Systeme, z.B. Warteraum-TV, sollten auch ein getrenntes Netzwerk (LAN) verwenden, wenn nötig. Achten Sie bei Verwendung eines WLAN für das interne Ärztenetzwerk auf ausreichende Absicherung: Neben dem klassischen WLAN Passwort kann man auch Zugriffslisten einrichten, so dass nur „bekannte" Geräte Zugriff zum WLAN bzw. Netzwerk erlangen. Besprechen Sie das bei Bedarf mit Ihrem IT-Dienstleister.

3. Die Lebensversicherung: Das Backup

Datensicherung ist das einzige Netz, das Sie auffängt, wenn alle anderen Stricke reißen – egal ob durch Verschlüsselungs-Trojaner, Brand oder versehentliches Löschen.

- **Die 3-2-1 Regel:** Bewährter Mindest-Standard: **3** Kopien Ihrer Daten, auf **2** verschiedenen Medientypen, mindestens **1** Kopie davon extern gelagert (Schutz vor Brand/Einbruch in der Ordination). *Tipp:* Speichern Sie nicht alle Backups auf derselben externen Festplatte! Verwenden Sie mehrere Festplatten im Wechsel (Rotationsprinzip). Eine Netzwerkfestplatte (NAS) kann auch in einem anderen Raum gelagert werden. Mindestens ein Backup sollte automatisiert regelmäßig (täglich) Backups machen.
- **Das Offline-Backup (Air Gap):** Viele moderne Viren (Ransomware) verschlüsseln auch angeschlossene Backup-Festplatten. Es ist zwingend notwendig, dass es ein Backup-Medium gibt, das nach der Sicherung **physisch vom Netzwerk/Strom getrennt wird.**

- **Cloud-Backup:** Verschlüsselte Cloud-Backups in zertifizierten Rechenzentren (Standort Österreich/EU) sind eine valide Ergänzung zur „Außer-Haus-Lagerung", setzen aber eine schnelle Internetverbindung voraus und ist deshalb nicht überall geeignet.
- **Der Restore-Test:** Ein Backup, dessen Wiederherstellung nie getestet wurde, ist wertlos. Testen Sie oder Ihr IT-Dienstleister mindestens einmal jährlich eine **Test-Rücksicherung** auf einem Testsystem (am besten baugleicher Art wie der Server) und protokollieren Sie diese.

WICHTIG: Sollten Sie in Ihrer Praxis noch keine Datensicherung implementiert haben oder die bestehende Umsetzung unzureichend sein, empfehlen wir Ihnen, diese unverzüglich nachzuholen. Speichermedien (Festplatten, etc.) sind im Vergleich zum potenziellen erwarteten Schaden äußerst kostengünstig. Es existiert keine bessere Investition im Rahmen der IT-Sicherheit als die Implementierung eines funktionsfähigen Backups.

4. Zugriffskontrolle & „Menschliche Firewall"

Technik ist nur so sicher wie ihre Bedienung. Der Mensch ist oft die erste und letzte Verteidigungslinie.

- **Eindeutige Identifizierung:** Jeder Nutzer (auch Vertretungsärzte, Famulanten oder Praktikanten) benötigt einen eigenen Benutzerzugang. Geteilte Accounts (User: „Praxis", Passwort: „123") sollten vermieden werden.
- **Bildschirmsperre:** Ein unversperrter PC im leeren Behandlungszimmer ist ein Sicherheitsrisiko. Gewöhnen Sie sich und Ihrem Team die Tastenkombination Windows-Taste + L an, sobald der Platz verlassen wird, dann wird der Rechner gesperrt.
- **Sichere Passwörter:**
  - Verwenden Sie ausreichend sichere Passwörter! **Länge schlägt Komplexität:** Ein Satz wie Kaffee-Pause-Um-10:00! ist sicherer und leichter zu merken als Tr5$x9!.
  - Verwenden Sie niemals mehrmals das gleiche Passwort für unterschiedliche Anwendungen / Systeme!
  - Schreiben Sie Ihre Passwörter nirgends nieder: weder auf ein Post-It noch in ein Buch! - Verwenden Sie einen Passwortmanager.
  - Ein Passwortmanager ist aktuell State-of-the-art und sehr empfehlenswert für die Verwaltung verschiedener Passwörter. Der Passwortmanager besitzt ein Masterpasswort, welches alle weiteren Passwörter freigibt. So müssen Sie sich nur ein Passwort merken. Der Passwortmanager unterstützt außerdem beim Erstellen von Passwörtern für verschiedene Dienste.

Passwortmanager gibt es von verschiedenen Anbietern, erkundigen Sie sich unbedingt bei Ihrem IT-Dienstleister für die passende und sichere Lösung in Ihrer Arztpraxis.

- Verwenden Sie Zwei-Faktor-Authentifizierung (2FA), wenn möglich für externe Dienste. Sie bekommen dann z.B. noch ein SMS mit einem Code, den Sie zusätzlich zu Ihrem Passwort für den Login benötigen. Wichtig ist 2FA vor allem für externe Dienste oder Dienste, bei denen Sie sich von extern auf ihr internes Netzwerk verbinden (z.B. per VPN), um auf die Ordinationssoftware zuzugreifen. Bei internen Systemen (z.B. der Login in der Praxissoftware) ist eine 2FA meist im Arbeitsfluss hinderlich, da der Login-Vorgang zu aufwändig ist und sehr häufig durchgeführt werden muss (Ausloggen beim Verlassen des Arbeitsplatzes und Login bei Rückkehr). Hier ist es meist effizienter, das interne Ordinations-Netzwerk von außen abzusichern (siehe Punkt „gesicherter Internetzugang“) und auf 2FA intern zu verzichten.
- Besprechen Sie im Team, wie Sie geteilte Passwörter organisieren (z.B. für Onlineplattformen zur Bestellung). Sie können z.B. einen eigenen Passwortmanager für die Ordination verwenden, so müssen sich die Mitabreiter:innen nur ein Passwort merken und können auf jedem Rechner darauf zugreifen.
- Notfall-Regelung: Sollten Sie Passwörter physisch aufbewahren müssen (z. B. das Master-Passwort für den Notfall), gehört dieses Blatt Papier zwingend in einen **versperrten Tresor**, zu dem nur die Praxisleitung Zugriff hat.

- Sichere Fernwartung: Zugriffe von außen (Homeoffice, IT-Dienstleister) müssen besonders geschützt sein. Nutzen Sie sichere VPN-Verbindungen und bei Lösungen und zwingend eine **2FA.**
- Keine Admin-Rechte: Wenn möglich, arbeiten Sie im Alltag nicht mit einem Benutzerkonto, das Administrator-Rechte hat. Schadprogramme können sich so viel schwerer im System festsetzen. Oft ist das mit der verwendeten Arztpraxis-Software leider nicht möglich, klären Sie das mit Ihrem IT-Dienstleister.
- Gesunde Skepsis im Arbeitsalltag:
  - **Vor Ort: Geben Sie Unbekannten** keinen Zugang zur Infrastruktur (Serverraum, Router). Vorsicht vor „falschen Servicetechnikern“, die unangekündigt „nur kurz ein Update installieren“ wollen.
  - **Telefon:** Geben Sie niemals unbekannten Anrufern Fernwartungszugriff (z. B. AnyDesk/TeamViewer). Prüfen Sie bei Anrufern (z. B. angebliche Support-Mitarbeiter Ihrer Softwarefirma) durch Rückruf unter der offiziellen Nummer, ob die Person und der nötige Vorgang echt ist. Vergewissern Sie sich stets über die Notwendigkeit von Updates, die per Fernwartung installiert werden müssen.

- E-Mail: Öffnen Sie keine Anhänge und klicken Sie keine Links von unbekannten Absendern, auch wenn diese „Rechnung“ oder „Mahnung“ heißen.
- USB-Stick: Stecken Sie niemals unbekannte USB-Sticks an Ihren PC, den Sie z.B. im Wartezimmer finden. Es kann sich darauf unter Umständen auch eine Schadsoftware (Virus, etc.) befinden.

- Schulung und Kultur: Sensibilisieren Sie Ihr Team!
  - Sicherheitskritische Angriffe passieren oft (gezielt) dann, wenn die Ordination im vollen Betrieb ist und Stress herrscht („Dringendes Update“, „Letztes Mal war das aber auch kein Problem“). Nehmen Sie sich trotzdem stets die Zeit, die Plausibilität zu prüfen und lassen Sie sich nicht zu unüberlegten Handlungen überreden.
  - Melden Sie Auffälligkeiten sofort: Sollten Sie im Praxisbetrieb ungewöhnliche Vorkommnisse feststellen – beispielsweise eine veränderte Anmeldemaske, unerwartete Systemmeldungen, Info über „falsches Passwort“ obwohl garantiert mehrmals korrekt eingegeben, unbekannte Pop-ups oder verdächtige E-Mails/Anrufe – melden Sie dies umgehend und überprüfen Sie es bzw. klären es mit Ihrem IT-Dienstleister! – Auch Ihr Team sollte stets Auffälligkeiten umgehend melden! - Im Zweifel gilt: Lieber einmal zu viel melden als einmal zu wenig.

5. Sicherer Umgang mit Software & Netzwerk

- Updates (Patch-Management): Veraltete Software ist wie ein offenes Fenster. Installieren Sie zeitnah Sicherheitsupdates für Betriebssysteme, Praxissoftware und Office bzw. vergewissern Sie sich, dass es automatisch ordnungsgemäß aktualisiert wird. *Oft vergessene Geräte:* Auch Drucker, Scanner, Router, Telefonanlagen, Warteraum-TV und alle anderen Geräte mit aktivem Netzwerkzugang (LAN oder WLAN) benötigen Firmware-Updates, die Sie oder Ihr IT-Dienstleister regelmäßig durchführen sollten.
- Gesicherter Internetzugang: Vergewissern Sie sich, dass Ihr Internet in der Ordination ausreichend von außen gesichert ist (korrekt konfigurierte Firewall) und klären Sie das bei Bedarf mit Ihrem IT-Dienstleister. Oft verwenden Ordinationen auch den gesicherten Internetzugang als Mehrwertdienst des GIN (Gesundheits-Informations-Netz) - das ist ein gesichertes Internet für Gesundheitsdienste in Österreich, über welches auch die Befundübertragung und die E-Card Dienste angeboten werden. Dennoch ist es empfehlenswert, das Internet auf Praxis-Rechnern ausschließlich für notwendige Tätigkeiten zu verwenden und für privates „Surfen” auf ein anderes Internet auszuweichen (z.B. auf einem unabhängigen Rechner über das mobile Handynetz).
- Antivirus / Endpoint Protection: Ein aktueller Virenscanner ist auf den Praxis-Rechnern Pflicht. *Wichtig:* Kostenlose „Home-User“-Lösungen (und auch der unüberwachte Windows Defender) reichen oft nicht aus. Empfehlenswert sind „Managed Antivirus“-Lösungen, die von Ihnen oder Ihrem IT-Dienstleister zentral

überwacht werden können. Antiviren-Systeme sollten Sie an die Ordinations-Software, die sie in Ihrer Praxis verwenden, anpassen. Erkundigen Sie sich bei Ihrem Softwareanbieter über geeignete Antiviren-Lösungen. Bei falscher Konfiguration des Virenscanners kann dieser die Ordinationssoftware blockieren, was häufig zu schwer erkennbaren Problemen im Praxisalltag führt (z.B. „Software läuft langsam", „Befunde werden nicht mehr geöffnet", etc.)

6. Prozess für den Ernstfall: Training & Notfallbetrieb

Technik kann ausfallen - auch über einen längeren Zeitraum. Entscheidend ist, dass Ihre Ordination deswegen nicht im Chaos versinkt. Erstellen Sie einen klaren Ablaufplan für den „analogen Betrieb" und schulen Sie Ihr Team darauf.

1. **Die „Rote Mappe" (Das Notfall-Kit)** Bereiten Sie eine physische Mappe oder Box vor, die griffbereit liegt. Inhalt:
   - **Wichtige Telefonnummern:** IT-Support, Software-Anbieter, Internet-Provider, Elektriker.
   - **Blanko-Formulare:** Rezepte, Überweisungen, Verordnungen, Krankschreibungen (in ausreichender Stückzahl).
   - **Papier-Kalender & Stifte:** Um Termine und Patientenströme manuell zu verwalten.
   - **Diktiergeräte oder Protokollbögen:** Für die ärztliche Dokumentation.
   - **Der analoge Arbeitsablauf (Workflow):** Definieren Sie, wie im Ausfallzeitraum gearbeitet wird:
2. **Patienten-Kommunikation:** Informieren Sie wartende Patienten sofort über Verzögerungen. Klären Sie, ob nur noch Akutfälle behandelt werden können.
   - **Dokumentation:** Dokumentieren Sie jede Behandlung handschriftlich auf vorbereiteten Bögen oder verwenden Sie einen anderen verfügbaren Laptop (z.B. mit Word). *Wichtig:* Notieren Sie zwingend **Name, SV-Nummer, Geburtsdatum, Uhrzeit und die gesetzten Maßnahmen**. Schreiben Sie leserlich, um Fehler bei der späteren Digitalisierung zu vermeiden.
   - **Sicherheits-Check:** Ohne PC fehlen automatische Warnhinweise und Informationen (z. B. Cave-Meldungen, Allergien, Wechselwirkungen). Fragen Sie Patienten in diesem Modus aktiv und doppelt nach Allergien und aktuellen Medikamenten!
3. **Die Nachbearbeitung (Re-Digitalisierung):** Sobald die Systeme wieder laufen, müssen die analogen Daten ins System übertragen werden.
   - Planen Sie hierfür **Personal-Ressourcen** ein (z. B. Überstunden am Wochenende oder Einsatz von Schreibkräften).
   - Scannen Sie die handschriftlichen Protokolle als Beleg ein oder übertragen Sie die Daten manuell in die Patientenkartei (gekennzeichnet als „Nacherfassung").
4. **Das Trockentraining** Ein Notfallplan, den niemand kennt, ist nutzlos. Simulieren und besprechen Sie einmal im Jahr im Team den Ausfall: *„Das Internet und der Server sind weg – wo ist die Mappe und wer macht was?"*. Das nimmt im Ernstfall die Panik und

schafft Routine. Schreiben Sie außerdem die Prozesse in einem Dokument nieder und nutzen Sie dies als Schulungsunterlage für Ihre Mitarbeiter:innen.

7. Management des IT-Dienstleisters

Als Praxisinhaber sind Sie für den Datenschutz verantwortlich (Verantwortlicher gem. DSGVO Datenschutz-Grundverordnung), auch wenn Sie die IT ausgelagert haben.

Achten Sie auf:

1. **Auftragsverarbeitungsvertrag (AVV):** Dieser muss laut DSGVO schriftlich vorliegen. *Hinweis*: Erkundigen Sie sich allgemein über Ihre Pflichten nach DSGVO in der Arztpraxis.
2. **Reaktionszeiten (SLA):** Klären Sie *vor* dem Notfall: Wie schnell sind wir nach einem Server-Totalausfall wieder arbeitsfähig? (4 Stunden? 24 Stunden? 3 Tage?).
3. **Protokollierung:** Fordern Sie regelmäßige Nachweise über durchgeführte Updates und Backup-Tests.

Cyber-Versicherung als Sicherheitsnetz:

Da ein technisches Restrisiko nie gänzlich ausgeschlossen werden kann, ist eine spezielle Cyber-Versicherung oft von Vorteil. Sie bietet nicht nur finanziellen Schutz bei Schadensersatzforderungen oder Betriebsunterbrechungen, sondern stellt im Ernstfall (z. B. bei einer Ransomware-Attacke) meist sofortigen Zugriff auf spezialisierte IT-Forensiker und Krisenmanager (Assistance-Leistungen) bereit. Erkundigen Sie sich bei Ihrem Versicherungsberater oder IT-Dienstleister über maßgeschneiderte Lösungen für Ihren Betrieb.

8. Checkliste: IT-Sicherheit in der Ordination

Nutzen Sie diese Liste für eine Bestandsaufnahme der IT-Sicherheit Ihrer Praxis.

A. Technische Sicherheit & Ausfallschutz

Status	Maßnahme	Erklärung
☐	Offline-Backup vorhanden	Gibt es ein Backup, das nach der Sicherung physisch vom Netz getrennt wird (Schutz vor Verschlüsselung)?
☐	Restore-Test durchgeführt	Wurde in den letzten 12 Monaten getestet, ob sich das Backup tatsächlich zurückspielen lässt?

☐	USV (Notstrom) aktiv	Ist der Server gegen Stromausfall abgesichert? Fährt er bei leerem Akku automatisch herunter?
☐	Festplatten gespiegelt	Läuft der Server weiter, wenn eine Festplatte kaputt geht (RAID)?
☐	Mobile Geräte verschlüsselt	Sind Laptops/Tablets/Sticks verschlüsselt (BitLocker etc.)?
☐	Updates automatisiert	Werden Sicherheitsupdates (Windows, Praxissoftware) automatisch installiert und überwacht?
☐	Updates von Hardware	Ist andere verwendete Hardware in der Ordination (Drucker, Router, NAS) mit dem neuestem Update aktualisiert?
☐	Antivirus	Ist der Virenschutz aktuell und wird zentral von Ihnen oder Ihrem IT-Partner überwacht?

B. Organisatorische Sicherheit

Status	Maßnahme	Erklärung
☐	Personalisierte Nutzer	Hat jeder Mitarbeiter einen eigenen Login (kein Account-Sharing)?
☐	Starke Passwörter	Werden lange Passwörter (Sätze) verwendet und nicht auf Post-its notiert? Sind auch Smartphones und andere Geräte mit

		Netzwerkzugang mit einem Code abgesichert?
☐	2-Faktor-Authentifizierung geprüft	Ist ein Fernzugriff (Homeoffice/Wartung) jederzeit möglich und ist dieser doppelt abgesichert?
☐	Clean Desk / Sperren	Werden PCs gesperrt (Win+L), wenn der Platz verlassen wird?
☐	Notfall-Mappe analog	Gibt es bekannte Prozesse, Telefonlisten und Papier-Formulare für den Fall eines Totalausfalls?
☐	Datenträgervernichtung	Werden alte Festplatten und Akten sicher vernichtet (Schredder)?
☐	Mitarbeiter:innen Schulung	Wurden Ihre Mitarbeiter:innen in den letzten 12 Monaten zu IT-Sicherheit geschult?
☐	Neue Mitarbeiter:innen	Gibt es eine allgemeine Schulung zu IT-Sicherheit in der Ordination für neue Mitarbeiter:innen?

C. Rechtliches & Dienstleister

Status	Maßnahme	Erklärung
☐	AVV Vertrag	Liegt ein unterzeichneter Auftragsverarbeitungsvertrag mit allen IT-Dienstleistern vor?

☐	Netzwerktrennung geprüft	Ist das Patienten-WLAN strikt vom Praxis-Netzwerk getrennt?
☐	Versicherung geprüft	Wurde geprüft, ob eine Cyber-Versicherung (für Eigenschaden und Drittschaden) sinnvoll ist?

Bei Fragen stehen wir von der UMIT-Tirol für die Initiative im DIH-West gerne zur Verfügung: marco.schweitzer@umit-tirol.at

Herausgeber:
UMIT Tirol – Division für Gesundheitsvernetzung und Telehalth
DI Dr. Marco Schweitzer, BSc
Kontakt: marco.schweitzer@umit-tirol.at

DIH West (Digital Innovation Hub West)
Web: www.dih-west.at