# PRÄVENTIONSTIPPS

## TIPPS FÜR **SICHERE DATEN**

> **Verschlüsselung der Daten.** Für die Speicherung der Daten sollten verschlüsselte Laufwerke verwendet werden, um es potenziellen Eindringlingen so schwer wie möglich zu machen. Hierzu zählt, dass die Kommunikation zwischen Dienstleister*innen, aber auch zum Beispiel die Kommunikation mit Krankenkassen, immer verschlüsselt abläuft.

> **Ein einheitliches Protokoll für das Verhalten von Mitarbeiter*innen am Arbeitsplatz**. Speziell gilt das für Systeme, auf denen Daten gespeichert sind. Es wäre vernünftig, unterschiedliche Berechtigungsstufen für die Mitarbeitenden zu schaffen. Jede Person soll nur die Zugriffsrechte haben, die sie unbedingt benötigt.

> **Die Datensicherung.** Sollte es zu einem erfolgreichen Ransomware-Angriff kommen, muss der Betrieb in der Lage sein, die Daten wieder zu restaurieren. Hier ist es also zentral, über ein Backup- und Recovery-Konzept zu verfügen, mit dem man das Allerschlimmste – nämlich den längerfristigen Ausfall der Systeme und den Verlust der Daten – verhindern kann.

> **Absicherung der Infrastruktur.** Ein sinnvolles Back-up-System sowie die Verschlüsselung von Daten ist essentiell. Hier ist auch die Industrie gefordert, Lösungen zu erarbeiten, die auch für kleine Ordinationen oder Gesundheitsdienstleister*innen umsetzbar sind.

Quelle: KFV-Studie zur Sicherheit von Patient*innendaten
Titelbild: National Cancer Institute / Unsplash
Bildrechte: Vectorstock


**Medieninhaber und Herausgeber:**
**KFV (Kuratorium für Verkehrssicherheit)**
Schleiergasse 18, A-1100 Wien
Tel: +43-(0)5 77 0 77-0
Fax: +43-(0)5 77 0 77-1186
E-Mail: kfv@kfv.at

# SICHERHEIT VON PATIENT*INNENDATEN

## Cybersicherheit und Cyberkriminalität im österreichischen Gesundheitswesen

**Daten sind ein wertvolles und schützenswertes Gut. Sie tragen Informationen über Individuen, ihre Verhaltensmuster, ihre Vorlieben, aber auch ihre gesundheitlichen Merkmale. Die medizinische Akte eines Menschen ist hochsensibel. Nicht umsonst unterliegt diese besonderen Schutzmaßnahmen durch den Gesetzgeber. Durch die Digitalisierung aller gesellschaftlichen Aspekte ist auch die Krankengeschichte eines Menschen digital vorhanden und abgespeichert. So kann schnell und vernetzt auf einen gesundheitlichen Vorfall reagiert werden, der Austausch von Ärzt*innen und die Behandlung über Fachgebietsgrenzen hinaus wurde vereinfacht.**

### GESUNDHEITSDATEN

Vernetzte medizinische Geräte und elektronische Gesundheitsakten ermöglichen eine Verbesserung und Erleichterung in der Patient*innenversorgung. Daten werden gespeichert, um medizinische Behandlungen nachzuvollziehen oder zu planen. Dabei entstehen große Mengen an Daten, die besonders sensibel und schützenswert sind. Gesundheitsdaten sind einmalig und nicht veränderbar. Dadurch sind sie besonders wertvoll. Je nach Vollständigkeit kann eine Patient*innenakte auf einschlägigen Online-Portalen auf dem Schwarzmarkt zwischen zehn und tausend US-Dollar einbringen. Knapp ein Drittel der weltweit gespeicherten digitalen Daten sind Gesundheitsdaten. Die Entwicklung der digitalen Patient*innenakten hat in den letzten Jahren deutlich schneller zugenommen als die Entwicklung entsprechender Sicherheitsmaßnahmen.

### DIE PROBLEMATIK

Gesundheitsdaten existieren also in großer Zahl, sowohl im privaten digitalen Raum, als auch im digitalen Gesundheitswesen. Deren Schutz ist ein Thema, das in den letzten Jahren immer mehr an Bedeutung gewonnen hat. Gesundheitsdaten sind besonders sensibel, einmalig und nicht veränderbar. Mit der Datenschutz-Grundverordnung, kurz DSGVO, wurden Fragen zur Speicherung von Daten und deren Schutz in unterschiedlichen Bereichen diskutiert und geregelt. Gesundheitsdaten sind für Kriminelle von großem Interesse. Sie sind auf dem Schwarzmarkt sehr viel mehr wert als andere personenbezogene Daten, und sie können für viele unterschiedliche Dinge eingesetzt werden.

### KFV-STUDIE

Wie steht es nun aber um den Schutz dieser Daten in Österreich? Dieser Frage haben sich die Plattform Patientensicherheit und das KFV angenommen. In einem Methodenmix aus qualitativen Expert*inneninterviews, einer quantitativen Befragung von Gesundheitsbetrieben, sowie einem Experiment wurden unterschiedliche Aspekte dieser hochkomplexen Thematik beleuchtet.

Die Ergebnisse zeigen, dass Datenschutz in Österreich in der Praxis bereits gut gelebt wird, es jedoch im Bereich Datensicherheit noch sehr viel Luft nach oben gibt. Hier ist es vor allem eine Frage des Zugangs zu Informationen und Unterstützung, die benötigt wird, um die Sicherheit von Patient*innendaten bestmöglich zu gewährleisten.

Da die Forschung zeigt, dass der Mensch das schwächste Glied in der Cybersicherheit ist, wird in allen Bereichen betont, wie wichtig es ist, das Bewusstsein der Endnutzer*innen zu schärfen. Sicherheitsmaßnahmen können daher ohne die aktive Beteiligung der verschiedenen Akteur*innen nicht erfolgreich sein.

### METHODIK

Im Auftrag des KFV wurde eine Befragung von Gesundheitsdienstleister*innen ergänzt durch Expert*inneninterviews durchgeführt. Zudem wurde als dritte Methode ein „White-Hat-Hack“ Experiment gewählt.

Studienzeitraum: Juni 2021 - Jänner 2022

# Diebstahl von Patient*innendaten

## Datenschutz und Datensicherheit bei Gesundheitsdienstleister*innen

**94 %**

der Befragten verwenden einen Stand-PC fur die Arbeit

**52 %**

der Befragten verwenden die Endgerate am Arbeitsplatz auch für privates Surfen

**90 %**

der Befragten geben an, eine Datenschutzrichtlinie im Unternehmen etabliert zu haben

## Angriffswerkzeuge sind vor allem Phishing und Ransomware

Phishing ist häufig, da die Kosten für ein täuschend echtes E-Mail mittlerweile gering sind. Außerdem sind die Klickraten im Gesundheitsbereich überdurchschnittlich hoch. Ransomware wird in harmlos aussehenden E-Mail-Anhängen versteckt. Die Software verschlüsselt die Daten. Zur Freigabe wird meist Lösegeld in Form von Kryptowährungen gefordert.

## Anfälligkeit im Bereich der Gesundheitsdienstleister*innen

Ausgelöst durch hohe Arbeitslast, ein hohes Grundvertrauen in die Seriosität von eintreffenden E-Mails und unzureichende Schulung von Mitarbeitenden.

## Gründe für Angriffe

Gesundheitsdaten sind am Schwarzmarkt viel mehr wert als andere persönliche Daten. Mit erbeuteten Daten können auf die Gesundheitsgeschichte abgestimmte Scams durchgeführt werden, falsche Versicherungsansprüche erhoben oder verschreibungspflichtige Medikamente erworben werden.

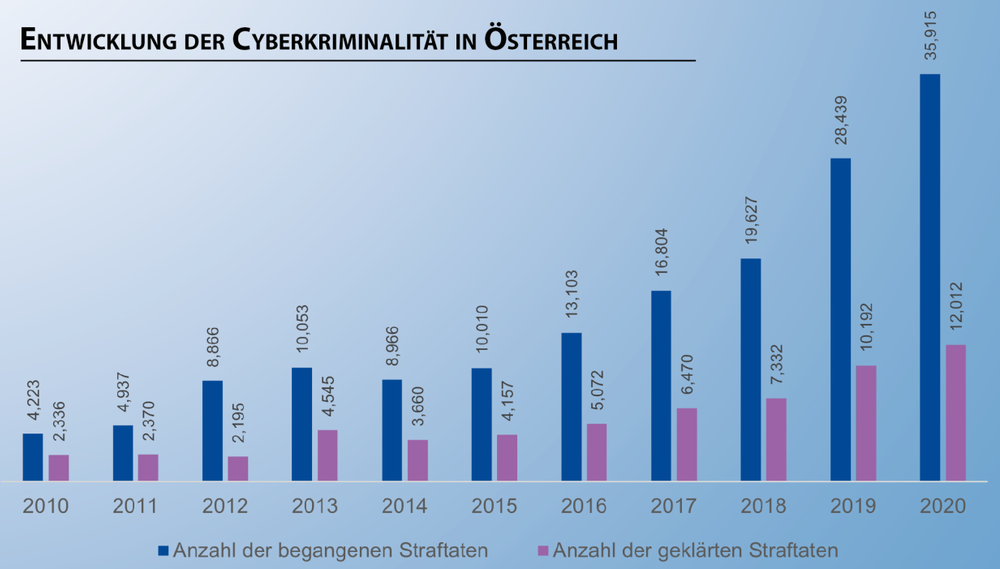
## Drei grosse Risiko-Szenarien für Patient*innendaten

Die Nichtverfügbarkeit der Daten aufgrund eines Ransomware-Angriffs


Die Authentizität der retournierten Daten nach einem Angriff ist nicht gewährleistet

Verkauf der entwendeten Daten oder Erpressungsversuche mit den Daten

## Entwicklung der Cyberkriminalität in Österreich




Quellen: KFV (Kuratorium für Verkehrssicherheit); Bundeskriminalamt

www.kfv.at