Dr. René Sasse
RECHTSANWALT

RA Dr. René Sasse ● Chemnitzer Straße 126 ● 44139 Dortmund

Dr. René Sasse
Rechtsanwalt

Chemnitzer Str. 126
44139 Dortmund

Telefon 02 31.130 90 33
Mobil 01 76.21 05 22 46
Telefax 02 31.799 23 15

E-Mail info@rechtsanwalt-sasse.de
info@sasse-heilpraktikerrecht.de

Internet www.rechtsanwalt-sasse.de
www.sasse-heilpraktikerrecht.de

pgt technology scouting GmbH
Ruschgraben 51
76139 Karlsruhe

26.08.2022

Das Problem

Die DSGVO fordert bei der Verarbeitung von Gesundheitsdaten effektive Maßnahmen zur IT-Sicherheit. Nach Art. 32 DSGVO muss der Verantwortliche geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Bei der Verarbeitung von sensiblen Gesundheitsdaten der Patienten ist zu beachten, dass diese besonders schutzwürdig sind. Verstöße können nach Art 82 DSGVO einen Schadensersatzanspruch des Patienten zur Folge haben.

Doch um welche Maßnahmen handelt es sich konkret? Hier besteht bei Therapeuten oft erhebliche Unsicherheit. Diese Orientierungsliste zur IT-Sicherheit in der Heilpraktikerpraxis soll Sie unterstützen, diese Unsicherheit zu verringern. Sie beinhaltet Maßnahmen, die Sie in Ihrer Praxis umsetzen können, um Ihre IT-Sicherheit zu steigern. Besonderen Wert legen wir darauf, dass die Maßnahmen realitätsnah sind und sich – mit grundlegendem IT-Wissen - ohne große Kosten in den Praxisalltag integrieren lassen. Wir möchten Sie hierdurch für sicherheitsrelevante IT-Themen sensibilisieren und einen datenschutzkonformen Betrieb Ihrer Praxis ermöglichen.

Auch wenn das Ziel die DSGVO-konforme Heilpraktikerpraxis ist, soll und kann diese Liste nicht vollständig oder abschließend sein; sie erfordert jeweils der Anpassung im Einzelfall. Es kann nur vor Ort beurteilt werden, welche der Maßnahmen umgesetzt werden müssen und ob weitere Maßnahmen erforderlich sind. Die hier genannten Maßnahmen dienen der Veranschaulichung und stellen Beispiele dar. Es handelt sich um die unverzichtbaren „Basics“. Die Ausführungen richten sich an Personen, die durchschnittliche IT-Kenntnisse haben. Wir verzichten an dieser Stelle

deshalb auf technische Feinheiten und legen den Schwerpunkt auf die Verständlichkeit und Umsetzbarkeit. Eine individuelle IT-Beratung kann diese Aufzählung nicht ersetzen.

- Updates / Aktuelle Software

Halten Sie Ihre Software aktuell, um mögliche Schwachstellen zu reduzieren. Führen Sie regelmäßig (Sicherheits-)Updates auf allen technischen Geräten (wie PC, Laptop, Smartphone, Tablet) durch. Dies gilt sowohl für die Betriebssysteme (Windows, Android, OS, MacOS und Linux), als auch für die von Ihnen genutzten Programme (Praxissoftware, Browser, Office, PDF-Reader etc.)

Nutzen Sie keine veralteten Geräte, für die keine (Sicherheits-)Updates (mehr) verfügbar sind. (z.B. ältere Smartphones oder Tablets). Achten Sie bei der Anschaffung darauf, dass Sie möglichst über einen langen Zeitraum Updates erhalten.

- Information

Informieren Sie sich über aktuelle Sicherheitswarnungen, zum Beispiel auf der Website des Bundesamts für Sicherheit in der Informationstechnik – BSI (https://www.bsi.bund.de/DE/Home/home_node.html)

- Virenschutz & Firewall

Verwenden Sie einen wirksamen Anti-Malware-Schutz (Antivirenprogramm) und eine Firewall. Die Antivirensignaturen müssen stets aktuell sein. (Tägliche Aktualisierung). Die Stiftung Warentest hat einen aktuellen Test veröffentlicht, der Ihnen einen guten Überblick über die möglichen Anbieter verschafft. Abrufbar gegen eine Gebühr von 5 € unter https://www.test.de/thema/computersicherheit/.

Mit einem Trojaner können Kriminelle Ihre Daten verschlüsseln, um Lösegeld zu erpressen. Dies gefährdet Ihre Patientendokumentation und den gesamten Datenbestand. Eine Verschlüsselung der Patientendaten hat gravierende Konsequenzen. Deshalb sind vorbeugende Maßnahmen zum Schutz gegen Verschlüsselungstrojaner zwingend erforderlich. Stellen Sie sicher, dass Ransomsoftware Ihre Backups/Datensicherungen nicht verschlüsseln kann. Öffnen Sie keine Dateien (insbesondere E-Mail-Dateianhänge) unbekannter Herkunft ohne vorherige Sicherheitsprüfung. Stellen Sie Ihr System so ein, dass Programme oder Dateien nicht automatisch ausgeführt werden.

- Passwortschutz & Zwei-Faktor-Authentifizierung

Schützen Sie Ihre Benutzerkonten durch geeignete (starke) Passwörter. Dies ist insbesondere wichtig, um den Login (Anmeldung) in ein Programm oder eine Datenverarbeitung in der Cloud wirksam abzusichern. Die Passwörter sind vertraulich zu halten und dürfen nicht weitergegeben werden. Aufgrund der Vielzahl von Passwörtern kann die Nutzung eines geeigneten Passwortmanagers sinnvoll sein. Ein Speichern von Passwörtern im Browser ist hingegen nicht ratsam. Weitere Infos zu Passwörtern finden Sie unter anderem auf der Internetpräsenz des BSI, https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Sichere-Passwoerter-erstellen/sichere-passwoerter-erstellen_node.html
Unter https://www.test.de/Passwort-Manager-im-Test-5231532-0/ finden Sie einen gebührenpflichtigen Testbericht der Stiftung Warentest zu Passwortmanagern.

Der unbefugte Zugriff auf sensible (Gesundheits-/Patienten-)Daten ist durch weitere Maßnahmen zu verhindern. Hierzu bietet sich die Zwei-Faktor-Authentifizierung an. Neben dem Passwort ist hier für den Zugriff auf Patientendaten ein weiterer Zugangsfaktor erforderlich. Der Anbieter sendet Ihnen beim Anmeldeprozess nach Eingabe des Passwortes einen Bestätigungscode an ein weiteres von Ihnen hinterlegtes Gerät zu (z.B. an Ihr Smartphone). Der zweite Faktor kann zudem die Verwendung eines USB-Sticks (Fido-Sticks) oder einer Chipkarte sein. Bei einem Login in eine cloudbasierte Patientenverwaltungssoftware sollte z.B. eine solche Zwei-Faktor-Authentifizierung genutzt werden.

- Vorsicht bei E-Mails

Wenn Sie sich E-Mails im „Nur-Text-Format“ anzeigen lassen, sind manipulierte Links besser zu erkennen. Verwenden Sie ein Anti-Virenprogramm, um E-Mail-Anhänge vor dem Öffnen zu prüfen. Blockieren Sie gefährliche Anhänge (wie z. B. .exe, .doc, .cmd). Folgen Sie keinen unbekannten Links in nicht vertrauenswürdigen E-Mails. Sofern Ihr Provider dies anbietet, können Sie dort eine serverseitige Anti-Viren-Prüfung veranlassen.

- Backups / Datensicherung

Trotz aller Bemühungen ist ein Datenverlust niemals komplett auszuschließen. Deshalb ist eine Datensicherung ein unverzichtbarer Bestandteil der IT-Sicherheit. Mit regemäßigen und vollständigen Sicherungen können Sie einen Datenverlust kompensieren. Wichtig ist hierbei:

Verfassen Sie ein schriftliches Backup-Konzept. Führen Sie tägliche Backups nach der 3-2-1 Regel durch. Das bedeutet: Drei Datenspeicherungen auf zwei verschiedenen Backupmedien, wobei eine an einem externen Standort gelagert wird. Sofern Sie einen mobilen Datenträger nutzen, achten Sie darauf, dass dieser per starker Kryptographie (z. B. AES 256 Bit) verschlüsselt ist und an einem geeigneten Ort aufbewahrt wird. (Brandschutz, Schutz vor Wasserschäden, unbefugter Zugriff).

Schützen Sie Ihre Datensicherungen davor, dass Trojaner auf diese übergreifen können.

Regelmäßige Überprüfung, ob sämtliche wichtigen Daten im Backup vorhanden sind und die Wiederherstellung möglich wäre.

- Verschlüsselung

Sofern Sie Daten übermitteln, nutzen Sie eine Transportverschlüsselung (z. B. TLS) nach Stand der Technik bzw. eine Ende-zu-Ende-Verschlüsselung, sofern Gesundheitsdaten übertragen werden.

Bei mobilen Rechnern und beruflich genutzten Smartphones sollte eine Verschlüsselung der Daten gewährleistet sein. Der Zugriff muss z.B. durch Pineingabe geschützt sein.

Nutzung vom WLAN nur mit starken Passwörtern. Das WLAN sollte nach aktuellem Standard verschlüsselt sein (WPA3). Nutzen Sie kein öffentliches / fremdes WLAN, sofern Sie Patientendaten bearbeiten.

- Fernwartung

Beaufsichtigen Sie Fernwartungsarbeiten. Beauftragen Sie nur sorgfältig ausgewählte Firmen nach Abschluss eines Vertrages, der auch eine Vertraulichkeitsregelung umfasst. Suchen Sie sich präventiv (in Ruhe) ein Unternehmen, welches Sie im Falle eines IT-Notfalls rasch unterstützen kann und notieren Sie sich dessen Telefonnummer auf einem Blatt Papier.

- Trennung von Arbeit und Privat

Nutzen Sie Ihren „Arbeitsrechner“ und Ihr berufliches Smartphone möglichst ausschließlich zu beruflichen Zwecken. So verhindern Sie, dass durch private Nutzung (Daten, Surfen etc.) ein Schaden entstehen kann. Problematisch wäre auch ein Zugriff von private genutzten Apps (wie z.B. Whatsapp) auf die Telefonnummern Ihrer Patienten.

- Sonstige Maßnahmen

Nicht mehr erforderliche Dateien müssen wirksam gelöscht werden. Hierauf ist auch bei der Entsorgung von Altgeräten zu achten.

Sperren Sie den Bildschirm Ihres Rechners, wenn dieser unbeaufsichtigt ist.

Schulen Sie Mitarbeiter, die auf Ihre EDV zugreifen regelmäßig über aktuelle und häufige Cyberangriffe sowie Sicherheitsrisiken.

Weitere Maßnahmen finden Sie unter den folgenden Links.
Orientierungshilfe zum Gesundheitsdatenschutz,
https://www.bmwk.de/Redaktion/DE/Publikationen/Wirtschaft/orientierungshilfe-gesundheitsdatenschutz.html
https://www.lda.bayern.de/de/thema_schadcode.html
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf