Gastbeitrag von Mark Peters

# Cyberschutz – die Notfallübung

Hackerangriffe, Phishingmails, Cybererpressung – die Digitalisierung, die Einzug in den Praxisalltag hält, bringt auch Gefahren mit sich. Was im Notfall zu tun ist, sollte in einem Notfallplan schriftlich festgehalten und regelmäßig trainiert werden.


Alle Arztpraxen sollten Maßnahmen ergreifen, um für den Notfall gerüstet zu sein. Dabei sollten auch Gefahren durch einen Stromausfall oder einen Wasserrohrbruch berücksichtigt werden. Der Ausfall des EDV-Systems stellt ein hohes Risiko für die Datensicherheit dar und kann zu massiven finanziellen Einbußen führen. Gerade für kleine und mittelgroße Praxen stellt das Thema „IT-Sicherheit" eine große Herausforderung dar, da diese üblicherweise nicht über eigene IT-Fachkräfte verfügen. Doch gerade mit Einführung der IT-Sicherheitsrichtlinie der KBV und einer zunehmenden Anzahl von Cyberangriffen gerät das Thema immer mehr in den Fokus. Aufgrund der Komplexität steht man als Praxisinhaber dann oft vor der Frage, wo man anfangen soll und wie man sich im Falle eines IT-Notfalls richtig verhält.

So sollten Sie vorgehen, wenn Sie ein Sicherheitskonzept für Ihre Praxis erarbeiten möchten:

- Das bestehende EDV-System in einem Netzwerkplan abbilden (gegebenenfalls den IT-Dienstleister hinzuziehen)
- Mögliche Schwachstellen ermitteln (hierbei auch andere Risiken wie Stromausfälle oder Wasserschäden berücksichtigen)
- Einen Notfallplan bzw. ein Notfallhandbuch erstellen
- Regelmäßige Notfallübungen durchführen (mindestens einmal pro Jahr)
- Ergebnisse der Notfallübungen auswerten und Anpassungen vornehmen

Wichtig ist, dass Sie neben dem Praxisteam oder, wenn Sie allein als Psychotherapeut*in tätig sind, die externe IT-Firma in den Prozess einbinden. Dies sorgt einerseits für die notwendige Akzeptanz der zu ergreifenden Maßnahmen, andererseits können Ihnen die MFAs auch wichtige Hinweise auf mögliche Schwächen liefern.

Eine hilfreiche und nützliche Quelle ist die Seite des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Mit dem „IT-Grundschutz“ und dem „Maßnahmenkatalog zum Notfallmanagement fokussiert auf IT-Notfälle“ des BSI erhalten Sie einen profunden Prozessbegleiter (Download: **https://bit.ly/3nUpX4H**).

Der beste Notfallplan hilft Ihnen nicht, wenn Sie ihn nicht regelmäßig auf seine Praxistauglichkeit testen. So sollten Sie einmal pro Jahr Ihr Backup überprüfen, indem Sie die Datenwiederherstellung testen. Auch sollten Sie kontinuierlich überwachen, dass die „Unterbrechungsfreie Stromversorgung (USV)“ Ihres Servers (wenn vorhanden) auch tatsächlich bei einem Stromausfall einspringt. Damit Ihr EDV-Netzwerk vor Wasserschäden geschützt ist, sollten die Geräte nicht direkt auf dem Boden stehen.

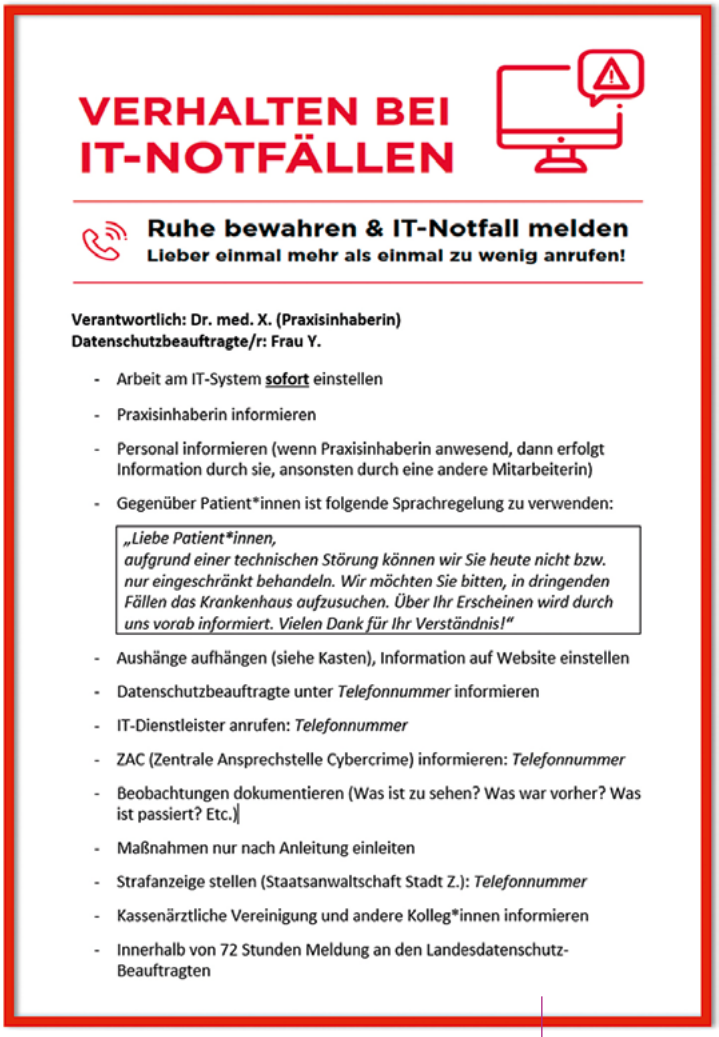
Um die Mitarbeitenden für mehr Aufmerksamkeit zu sensibilisieren, könnten Sie beispielsweise einen Bekannten, den die MFAs nicht kennen, bitten, während der Sprechzeiten in die Praxis zu kommen, sich einen der vorhandenen Laptops oder Tablets zu nehmen und mit diesem die Praxis wieder zu verlassen.

Auch das Erkennen von Phishingmails sollte eingeübt werden. Hierfür finden Sie im Internet kostenlose Anbieter, die in einem Training schadlose E-Mails an die Praxis schicken, um den Blick der Mitarbeitenden zu schärfen.

Das Einüben anderer Cyberangriff-Szenarien ist hingegen komplexer und mitunter auch mit Kosten verbunden. Die neue IT-Sicherheitsrichtlinie beziehungsweise das Heidelberger Cyberschutz-Rating bietet einfache Alternativen.

Mitunter benötigen Sie für diese Notfallübungen jedoch externe Unterstützung. Gemeinsam mit den Experten können Sie auf die Praxis zugeschnittene Szenarien entwickeln und mit Ihrem Team durchspielen. Die Testszenarien, die Ergebnisse und die daraus abgeleiteten Maßnahmen sollten Sie in einem Übungsbuch oder im QM-Handbuch der Praxis festhalten.

Konnten trotz aller ergriffenen Maßnahmen Cyberkriminelle Ihr Praxisnetzwerk angreifen, sollten Sie über einen Notfallplan verfügen, der auch ein entsprechendes Wording gegenüber den Patientinnen und Patienten enthält. Dieser könnte so aussehen:



**VERHALTEN BEI IT-NOTFÄLLEN**

**Ruhe bewahren & IT-Notfall melden**
**Lieber einmal mehr als einmal zu wenig anrufen!**

**Verantwortlich: Dr. med. X. (Praxisinhaberin)**
**Datenschutzbeauftragte/r: Frau Y.**

- Arbeit am IT-System **sofort** einstellen
- Praxisinhaberin informieren
- Personal informieren (wenn Praxisinhaberin anwesend, dann erfolgt Information durch sie, ansonsten durch eine andere Mitarbeiterin)
- Gegenüber Patient*innen ist folgende Sprachregelung zu verwenden:

  *„Liebe Patient*innen,*
  *aufgrund einer technischen Störung können wir Sie heute nicht bzw. nur eingeschränkt behandeln. Wir möchten Sie bitten, in dringenden Fällen das Krankenhaus aufzusuchen. Über Ihr Erscheinen wird durch uns vorab informiert. Vielen Dank für Ihr Verständnis!“*
- Aushänge aufhängen (siehe Kasten), Information auf Website einstellen
- Datenschutzbeauftragte unter *Telefonnummer* informieren
- IT-Dienstleister anrufen: *Telefonnummer*
- ZAC (Zentrale Ansprechstelle Cybercrime) informieren: *Telefonnummer*
- Beobachtungen dokumentieren (Was ist zu sehen? Was war vorher? Was ist passiert? Etc.)
- Maßnahmen nur nach Anleitung einleiten
- Strafanzeige stellen (Staatsanwaltschaft Stadt Z.): *Telefonnummer*
- Kassenärztliche Vereinigung und andere Kolleg*innen informieren
- Innerhalb von 72 Stunden Meldung an den Landesdatenschutz-Beauftragten

Mit diesen Tipps erhalten Sie erste Anregungen für ein umfassendes IT-Sicherheitskonzept. Die Firma Praxismanagement Bublitz-Peters ist eine von vielen Firmen, die solche Dienstleistungen anbieten.

Am besten benennen Sie gleich einen „Held*in der Praxis“ als Cyberschutzbeauftragte*n oder, wenn Sie allein als Psychotherapeut*in tätig sind, kümmern sich im Notfall um den reibungslosen Praxisablauf. Anschließend setzen Sie einen Termin für die erste Cybernotfallübung. Beziehen Sie Ihren ITler und, wenn vorhanden, den externen Datenschutzbeauftragen in die Übung ein. Schnell werden Sie feststellen, dass nach der ersten Übung ein siebter Sinn für Cyberrisiken entsteht und somit ein nachhaltiges Sicherheitsgefühl hervorgerufen wird. ■

Mark Peters