Von Schadsoftware bis zu Datendiebstählen: Arztpraxen sollten in Cybersicherheit investieren, denn sie können zum Ziel von Betrügern werden.

Neuer Newsletter Cybersicherheit der FMH

Reinhold Sojer[a], Max Klaus[b], Dominik Kreuter[c]

[a] Dr. rer. biol. hum., Leiter Abteilung Digitalisierung, FMH; [b] Stv. Leiter Operative Cybersicherheit OCS, Nationales Zentrum für Cybersicherheit NCSC; [c] Leiter Abteilung ICT, FMH

Die FMH informiert neu mit einem Newsletter über aktuelle Cyberbedrohungen. Ärztinnen und Ärzte mit eigener Praxistätigkeit können sich über die E-Mail-Adresse cybersecurity[at]fmh.ch für den Newsletter anmelden.

Cyberbedrohungen sind mittlerweile auch in Arztpraxen ein ernstzunehmendes Thema. Dies umso mehr, als die in einer Arztpraxis betriebenen Informationssysteme vernetzt sind und die Daten mit anderen Einrichtungen im Gesundheitswesen ausgetauscht oder sogar vollständig in der sogenannten Cloud durch externe Anbieter betrieben werden, die allenfalls nicht über einen ausreichenden Schutz verfügen. Auch die Möglichkeit eines externen Zugriffs auf die Daten einer Arztpraxis durch Mitarbeitende dürfte im Zusammenhang mit der Covid-19-Pandemie zugenommen haben. Dadurch entstehen zusätzliche Angriffsmöglichkeiten für Betrüger.

Waren früher vereinzelt Arztpraxen von Schadsoftware wie Erpressungs-Trojanern betroffen, die sich über E-Mail-Anhänge verbreiten, Daten verschlüsseln und diese nur gegen ein Lösegeld entschlüsseln [1], wird in den Medien zunehmend über Datendiebstähle berichtet, bei denen Dutzende Arztpraxen betroffen sind, die über die gleichen vulnerablen Systeme verfügen [2, 3]. Die erbeuteten Daten werden oftmals im

Früher waren vereinzelt Arztpraxen von Erpressungs-Trojanern betroffen, heute wird vermehrt über Datendiebstähle berichtet.

«Darknet» publiziert und können von dort für weitere Angriffe genutzt werden.

Empfehlungen IT-Grundschutz

Im Gegensatz zu grossen Gesundheitseinrichtungen, die Sicherheitsexperten zum Schutz der sensiblen Daten beauftragen, verfügen Arztpraxen möglicherweise nicht über die notwendige Expertise. Die FMH hat bereits im Jahr 2019 Empfehlungen zum IT-Grundschutz in Arztpraxen publiziert [4]. Die darin enthaltenen Minimalanforderungen sollen ein Mindestniveau an Sicherheit für Daten, Informationen und die ICT-Infrastruktur in Arztpraxen sicherstellen. Obwohl es keinen hundertprozentigen Schutz gegen Angriffe auf die Informations- und Kommunikationsinfrastruktur einer Arztpraxis gibt, ist es wichtig, die Minimalanforderungen vollständig umzusetzen.

Die FMH möchte Arztpraxen künftig rechtzeitig über aktuelle Bedrohungen in Form eines Newsletters aufmerksam machen.

Die FMH empfiehlt Arztpraxen festzulegen, wie Mitarbeitende mit möglichen Sicherheitsvorfällen umgehen sollen. Wurden schützenswerte Personendaten entwendet oder gelöscht, sind die vorgängig festgelegten Sofortmassnahen umzusetzen. Neben der Isolierung oder Ausserbetriebnahme von einzelnen Diensten oder Geräten muss eine Verletzung der Datensicherheit dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) gemeldet werden. Beim Verdacht auf eine Straftat sollte die Polizei schnellstmöglich kontaktiert werden, wenn mögliche Spuren noch nicht verwischt sind. Die Polizei berät und unterstützt die Praxisinhabenden, insbesondere auch in der Frage, ob allfälliges Lösegeld bezahlt werden soll.

Nationales Zentrum für Cybersicherheit

Weitere Informationen und Hilfestellungen bietet das Nationale Zentrum für Cybersicherheit NCSC [5]. Das NCSC hat u.a. die Aufgabe, die kritischen Infrastrukturen in der Schweiz zu schützen, deren Betrieb von den Informations- und Kommunikationsinfrastrukturen abhängen. Das NCSC publiziert Lageberichte, welche die wichtigsten Tendenzen und Entwicklungen im Bereich der Cybersicherheit umfassen. Es berichtet ausserdem über aktuelle Vorfälle in der Schweiz und weitergehende Empfehlungen bspw. im Zusammenhang mit möglichen Betrugsarten. Auf der Website des NCSC (www.ncsc.admin.ch) finden sich zahlreiche Anleitungen, Checklisten usw. für den sicheren Betrieb Ihrer IT-Infrastruktur. Dort können Sie auch einen Cybervorfall via dem Meldeformular melden und erhalten erste Hilfestellungen»

Newsletter Cybersecurity

Cyberkriminelle nutzen aktuelle Ereignisse wie die Covid-19-Pandemie oder den Krieg in der Ukraine für betrügerische Aktivitäten aus. Die gestiegene Nutzung von Telearbeit oder ein gesteigertes Informationsbedürfnis in einem Umfeld, welches durch Angst und Unsicherheit gekennzeichnet ist, sind Faktoren, die während der Covid-19-Pandemie zu vermehrten Cyberangriffen geführt haben [6].

Die FMH möchte Arztpraxen künftig rechtzeitig auf aktuelle Bedrohungen in Form eines Newsletters aufmerksam machen, wie sie beispielsweise durch das NCSC publiziert werden. Arztpraxen, die sich dafür interessieren, können sich über die E-Mail-Adresse cybersecurity[at]fmh.ch anmelden. Das Angebot richtet sich an Einzelpraxen sowie an Arztpraxen, die aufgrund ihrer Grösse oder Organisationsform nicht über das erforderliche Personal für die technische Sicherheitsinfrastruktur verfügen.

Bildnachweis
Alexandersikov | Dreamstime.com

Literatur
Vollständige Literaturliste unter www.saez.ch oder via QR-Code

FMH
Abteilung Digitalisierung / eHealth
Elfenstrasse 18
CH-3000 Bern 15
Tel. 031 359 11 11
eHealth[at]fmh.ch