PRAXIS-IT // Ransomware, Cyberkriminalität, Phishing-Mails: Die Digitalisierung, die zunehmend Einzug in den Praxisalltag hält, bringt auch Gefahren mit sich. Was im Notfall zu tun ist, sollte schriftlich in einem Notfallplan festgehalten und die Abläufe regelmäßig trainiert werden.

CYBERSCHUTZ – DIE NOTFALLÜBUNG

Mark Peters, Bettina Ritter / Heidelberg

Als niedergelassener Zahnarzt sollten Sie Maßnahmen ergreifen, um für den Notfall gerüstet zu sein. Da der Ausfall des EDV-Systems ein hohes Risiko für die Datensicherheit darstellt und massive finanzielle Einbußen zur Folge haben kann, sollten auch Gefahren durch einen Stromausfall oder einen Wasserrohrbruch bei den Überlegungen berücksichtigt werden.

Gerade für kleine und mittelgroße Zahnarztpraxen 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 nach § 75b SGB V und einer zunehmenden Anzahl von Cyberangriffen gerät das Thema immer mehr in den Fokus. Aufgrund der Komplexität der Gefahrenlage steht man dann oft vor der Frage, wo man anfangen soll und wie man sich im Falle eines Falles richtig verhält.

Bei der Erarbeitung eines Sicherheitskonzeptes für Ihre Praxis sollten folgende Aspekte berücksichtigt werden:

- Das bestehende EDV-System ist in einem Netzwerkplan abzubilden (gegebenenfalls den IT-Dienstleister hinzuziehen).
- Mögliche Schwachstellen sind zu ermitteln (hierbei sind auch andere Risiken wie Stromausfälle oder Wasserschäden zu berücksichtigen).
- Die zu ergreifenden Maßnahmen sind in einem Notfallplan bzw. einem Notfallhandbuch schriftlich dargelegt.
- Mindestens jährlich sollte eine Notfallübung durchgeführt werden.
- Die Ergebnisse der Notfallübung sind im Nachgang auszuwerten.
- Die gewonnenen Erkenntnisse und die damit verbundenen Anpassungen werden in den Notfallplan eingearbeitet. Das Thema „IT-Sicherheit" sollte fester Bestandteil der Team-Besprechungen sein.

Schlüsselrolle IT-Berater

Wichtig ist, dass Sie Ihr Praxisteam und Ihren externen IT-Betreuer in den Prozess einbinden. Dies sorgt einerseits für die notwendige Akzeptanz der zu ergreifenden Maßnahmen, andererseits können Ihnen Ihre Mitarbeitenden auch wichtige Hinweise auf mögliche Schwachstellen 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" erhalten Sie einen profunden Prozessbegleiter (Download-Adresse: https://bit.ly/3nUpX4H).

Der beste Notfallplan hilft Ihnen jedoch nicht, wenn Sie ihn nicht regelmäßig auf seine Praxistauglichkeit testen. So sollten Sie mindestens einmal pro Jahr Ihr Back-up überprüfen, indem Sie die Datenwiederherstellung testen. Auch soll-

ten Sie kontinuierlich überwachen, dass die „Unterbrechungsfreie Stromversorgung (USV)" Ihres Servers (wenn vorhanden) auch tatsächlich bei einem Stromausfall einspringen würde. Damit Ihr EDV-Netzwerk vor Wasserschäden geschützt ist, sollten die Geräte nicht direkt auf dem Boden stehen.

Übungen für die Praxis – Selbsttest

Kleine Übungen zur Schärfung der Aufmerksamkeit könnten folgendermaßen aussehen:

Sie könnten beispielsweise einen Bekannten, den Ihre Mitarbeiter 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 Phishing-Mails sollte eingeübt werden. Hierfür finden Sie im Internet kostenlose Anbieter, die zu Trainingszwecken schadlose E-Mails an die Praxis schicken, um den Blick der Mitarbeiter 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 jedoch einfache Alternativen.

Mitunter benötigen Sie für diese Notfallübungen jedoch externe Unterstützung. Gemeinsam mit Fachleuten 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 Zahnarztpraxis festhalten.

Notfallplan im Vorfeld bereitlegen

Konnten trotz aller ergriffenen Maßnahmen Cyberkriminelle Ihr Praxisnetzwerk angreifen, sollten Sie über einen Notfallplan verfügen, der auch ein entsprechendes „Wording" gegenüber den Patienten enthält. Schließlich möchten Sie sie ja nicht in Panik versetzen, bevor feststeht, ob Daten gestohlen wurden oder nicht.

Außerdem sollten Sie eine Cyberschutzbeauftragte benennen. Anschließend setzen Sie einen Termin für die erste Cybernotfallübung. Beziehen Sie Ihre IT-Betreuer und – wenn vorhanden – den (externen) Datenschutzbeauftragten in die Übung ein. Schnell werden Sie feststellen, dass nach der ersten Übung ein siebter Sinn für Cyberrisiken entsteht und somit ein nachhaltiges Sicherheitsverständnis hervorgerufen wird.

PRAXISMANAGEMENT
BUBLITZ-PETERS
GMBH & CO. KG
Rohrbacher Straße 28
69115 Heidelberg
Tel.: +49 6221 438500
info@bublitz-peters.de
www.bublitzpeters.de