DATENSCHUTZ

Hackerangriff auf die Praxis

Das Unabhängige Landeszentrum für Datenschutz (ULD) Schleswig-Holstein informiert.

Eilmeldung: Die Computer einer Arztpraxis in Schleswig-Holstein wurden gehackt. Sämtliche Patientendaten sind unter www.patientenpeep.de frei zugänglich. Wäre dieses Szenario möglich?

Ärzte unterliegen vielfältigen Dokumentationspflichten. Die Patientenverwaltung und die Abrechnung mit Krankenkassen und Privatversicherten erfordern viel „Schreibkram". Gut, dass es Computer gibt. Moderne Informationstechnik (IT) erleichtert die Arbeit. Auch in der Diagnostik ist die IT kaum noch zu ersetzen. Mit einer automatisierten Datenverarbeitung steigen jedoch nicht nur die Möglichkeiten, sondern auch die Risiken für die Datenverarbeitung. Der Gesetzgeber schützt das Patientengeheimnis: Eine unbefugte Offenbarung von Patientendaten steht unter Strafe. Werden Arzt- bzw. Zahnarztpraxen dieser Verantwortung gerecht? Was ist zu beachten? Der neue „Selbst-Check für Arztpraxen" stellt Fragen und gibt Antworten.

Computer werden gehackt und Daten ausspioniert. Kaum ein Tag vergeht, an dem nicht vor neuen Verschlüsselungstrojanern, Computerviren und anderen Sicherheitslücken gewarnt wird. Betrifft dieses Risiko auch Arzt- und Zahnarztpraxen, die ihre Patientendaten automatisiert verarbeiten? Ja! Gerade Arzt- und Zahnarztpraxen sind lohnende Angriffsziele.

Kontakt

Bei Fragen zu diesem Themenkomplex wenden Sie sich bitte an: Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Torsten Koop, Telefon 0431 988 1200

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat wiederholt von schweren Sicherheitsvorfällen berichtet. So von einem ambulanten Pflegedienst, dessen Computer gehackt wurde. Der Angreifer verschlüsselte die Patientendaten und drohte damit, diese im Internet zu veröffentlichen, wenn nicht umgehend Lösegeld gezahlt wird. Oft sind es Unwissen und unbedachte Handlungen der Ärzte bzw. des Praxis-Teams, insbesondere bei der Nutzung neuer oder nicht verständlicher Informationstechnik und die hieraus resultierende Unsicherheit, die zu den Risiken für die Rechte der Patienten führt. Anders dürfte es kaum zu erklären sein, dass in einer psychiatrischen Arztpraxis in Schleswig-Holstein ein unverschlüsselter Datenträger mit einer Sicherheitskopie von über 40.000 Patientendaten gestohlen werden konnte. Nicht auszudenken, welchen Schaden der Dieb mit den Patientendaten anrichten könnte.

Ärzte und Zahnärzte müssen sicherstellen, dass die Anforderungen der „ärztlichen Schweigepflicht" auch bei der Nutzung von IT eingehalten werden. Auch die Mitarbeiterinnen und Mitarbeiter tragen als berufsmäßig tätige Gehilfen Verantwortung. Ärzte- und Zahnärztekammer Schleswig-Holstein entwickeln gemeinsam mit dem ULD einen „Selbst-Check für Arztpraxen". Mit diesem „Selbst-Check für Arztpraxen" kann das Praxisteam feststellen, ob Handlungsbedarf besteht.

Im Teil 3 dieses „Selbst-Checks für Arztpraxen" werden die wichtigsten Fragen zur „Informationstechnik" gestellt. Aufgrund der Vielzahl der Fragen, werden diese in zwei Teilbeiträgen dargestellt. Den zweiten Teil „Informationstechnik" erhalten Sie mit der nächsten Ausgabe.

- Wird sichergestellt, dass für die Verarbeitung von Patientendaten ausschließlich autorisierte Hardware, also keine privaten Notebooks oder Smartphones, verwendet wird?
- Werden in der Praxis ausschließlich autorisierte Verfahren und Programme für die Verarbeitung von Patientendaten eingesetzt, die in einem Verfahrensverfahrensverzeichnis (§ 4e BDSG) erfasst sind?
- Sind Computer mit Patientendaten, die mit dem Internet verbunden sind, tatsächlich ausreichend geschützt (gewartete „Firewall")?
- Sind auf den Computern Virenschutzprogramme installiert, und werden diese täglich aktualisiert?
- Existiert ein Notfall-Handlungskonzept für den Fall eines Sicherheitsvorfalls (z. B. Virenbefall)?
- Sind ausreichende Sicherheitsvorkehrungen getroffen worden, wenn WLAN verwendet wird (Verschlüsselung, starkes Passwort für den WLANRouter, Deaktivierung der Übertragung des Funknetznamens (SSID) im Router, ...)?
- Wird eine Praxis-Software verwendet, die Patientendaten verschlüsselt speichert, soweit dies möglich ist?
- Werden für die Speicherung von Patientendaten Verfahren genutzt, die die Möglichkeit einer Löschung dieser Daten vorsehen?
- Wird regelmäßig eine verschlüsselte Sicherungskopie der Daten gefertigt (möglichst jeden Tag, mindestens einmal die Woche)?
- Werden diese Sicherungskopien ausreichend gegen Diebstahl, Brand etc. geschützt?

Noch Fragen? Die Ärzte- und Zahnärztekammer Schleswig-Holstein und auch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) stehen Ihnen gern zur Verfügung.

Sie finden alle Beiträge dieser Serie unter www.datenschutzzentrum.de, www.aeksh.de oder www.zaek-sh.de.

TORSTEN KOOP, ULD