Cyber-Sicherheit ist Chefsache!

Die voranschreitende Digitalisierung birgt trotz aller Automatisierung und Vereinfachung auch ihre Schattenseiten. Nicht erst durch WannaCry* im Mai 2017 birgt die Digitalisierung stets neue und nicht unerhebliche Risiken. Dies gilt im Privaten als auch im Beruflichen. Beinahe täglich erfährt man von neuen Sicherheitslücken oder Hackerangriffen. Unternehmen wie auch Arztpraxen sehen sich einer immer ernster zu nehmenden Bedrohung ausgesetzt.

Auch ein Arzt muss sensible Daten gegen Datenschutzverletzungen schützen. Gleiches gilt für die Datensicherung der Abrechnungen, des Controllings und des Qualitätsmanagements.

Aktuelle Beispiele:

- Die Erpresser-Schadsoftware „WannaCry“ legte im Mai 2017 mindestens 200.000. Rechner lahm. Krankenhäuser in England, die Deutsche Bahn, die deutsche Autoindustrie uvm. waren davon betroffen.
- Vom Humanmediziner bis hin zum Tier-mediziner haben die Hackerangriffe auf Arztpraxen zugenommen. Hierbei sind laut aktuellen Studien um die 75% der Hackerangriffe selbst verschuldet.
- Gesamtschaden für 2016 liegt in Deutschland bei über 50 Mio. € laut BKA. Leider ist die Dunkelziffer um einiges höher, da viele Betroffene einen Reputationsschaden fürchten, werden die meisten Angriffe nicht gemeldet.[1]

So oder so ähnlich haben viele in den letzten Monaten Ihren Computer vorgefunden. In diesem Fall wurden für die Entschlüsselung in erster Instanz „nur“ 300$ verlangt. Ob oder wann man an seine Daten wieder gelangt ist trotzdem nicht garantiert.

Fragen, die Sie sich als Praxiseigentümer stellen sollten: Reichen die eigenen IT Sicherungen in meiner Praxis bei…

- …Hackerangriffen?
- …Viren oder Trojanern?
- …„Innentätern“?
- …Cyber Erpressung?
- …Ansprüche gegen die Praxis infolge von Datenschutzverletzungen?

Die wachsende Bedrohung macht eine Cyberversicherung unentbehrlich.

Eine gute Cyberversicherung bietet hierbei mehr als nur Schadenersatz sondern auch umfassende Assistance Leistungen:

1. Risiko-Check durch Versicherer
2. Analyse und Herausstellung von Schwachstellen der IT Sicherheit in der Praxis
3. Präventives Cybertraining zur Mitarbeitersensibilisierung
4. Cyber Krisenplan – Unmittelbare Expertenhilfe im Schadenfall - 24/7 Hotline
5. Einschluss von Hackerschäden an medizinischen Geräten
6. Anwaltliche Vertretung gegenüber Aufsichtsbehörden
7. Information aller Betroffenen
8. Entschädigung von Betriebsunterbrechungsschäden infolge von Cyber Angriffen

[1] https://www.n-tv.de/wirtschaft/Cyber-Attacken-treffen-unzaehlige-Firmen-article19812353.html

Unsere Empfehlung:

Berücksichtigung der Empfehlungen beim Einsatz von EDV gemäß Datenschutz-und Datensicherheitsleitfaden von der BZÄK /KZBV!

Ein Beispiel aus der Praxis:

Durch die fortschreitende Digitalisierung und die wachsenden Datenschutzansprüche müssen sensible Daten besonders gesichert werden. Im Falle eines Worst-Case-Szenarios steht man oftmals mit dem Rücken zur Wand und hat ohne die richtigen Vorkehrungen nur bedingt die Möglichkeit schlimmeren Schaden abzuwenden. Was kann man also tun, wenn trotz aller Sicherheitsvorkehrungen das eigene System der Praxis gehackt wurde und welche Absicherungsmechanismen kommen für Arztpraxen in Frage?

Diese und weitere Fragen möchten wir in unserem Seminar „IT-Security & Cyberattacken“ thematisieren. Gemeinsam mit Finanzexperten, Juristen und IT-Consultants möchten wir zu einem offenen Diskurs einladen, in dem für die Arztpraxis bestehende Lösungen erläutert, diskutiert und abgewogen werden.

Jan Siol
www.auxmed.de

M.A. Management
Financial Planner&Consultant
Finanzfachwirt (FH)

Haben Sie noch Fragen?

Wir beraten Sie gerne!