Was eine Cyberattacke kosten kann – und eine Cyberversicherung deckt (✓)

Musterszenario Datenklau:

Hacker attackieren die IT-Systeme einer Arztpraxis. Sie kopieren die Patientendaten und versprechen, gegen die Zahlung von Lösegeld auf eine Veröffentlichung der Daten zu verzichten.

Angriff

Die Arztpraxis erhält per Mail einen Erpresserbrief. Die Kriminellen behaupten, im Besitz aller Patientendaten zu sein. Als Beleg senden sie kompromittierende Daten über fünf Patienten, die tatsächlich in der betroffenen Praxis in Behandlung waren. Sie drohen damit, die Daten zu veröffentlichen, wenn der Arzt nicht bereit ist, ein hohes Lösegeld zu zahlen.

Informationen an Patienten und Behörden

Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt der Arzt kein Lösegeld. Er muss aber die Datenschutzbehörden und seine Patienten über den Verlust der sensiblen Daten informieren. Um sicher zu gehen, dass er seinen Pflichten in vollem Umfang nachkommt, holt er sich Hilfe bei einem Rechtsanwalt. Die Patienten sind nach der Information verunsichert und haben intensiven Gesprächsbedarf.

- *Informationskosten: 4.000 Euro*
- *Anwaltskosten: 2.000 Euro*

Security-Initiative

IT-Spezialisten suchen und schließen die Schwachstelle, die den Tätern Zugriff zu den Daten erlaubte. Die Systeme werden desinfiziert und gehärtet.

- *Kosten für IT-Forensik: 5.000 Euro*

Betriebsunterbrechung

Bis die Schwachstellen geschlossen und weitere Datendiebstähle verhindert sind, bleibt die Arztpraxis geschlossen. Auch die Abrechnung mit den Krankenkassen ist unmöglich.

- *Kosten für 2 Tage Betriebsunterbrechung: 5.000 Euro*

Datenmissbrauch

Die Hacker veröffentlichen die Gesundheitsdaten einiger Patienten. Die Betroffenen beauftragen Spezialisten mit der Löschung der unrechtmäßig veröffentlichten Daten und verlangen vom Arzt Schadenersatz.

- *Schadensersatz: 20.000 Euro nach Art. 82 DSGVO*

Vertrauenskrise

Nachdem die lokale Presse über den Datendiebstahl berichtet, wenden sich zahlreiche Patienten von der Praxis ab, der Patientenstamm schrumpft deutlich.

- *Krisenkommunikation: 1.000 Euro*

Der Umsatzrückgang ist nicht gedeckt

Aufarbeitung

Die Datenschutzbehörden verhängen aufgrund des Datenverlustes ein hohes Bußgeld.

Das Bußgeld ist nicht gedeckt

Musterszenario Ransonware:

Hacker attackieren die IT-Systeme einer Apotheke und sperren die Systeme. Sie wollen die Systeme erst wieder freigeben, wenn sie vom Apotheker Lösegeld bekommen.

Angriff

Die IT-Systeme der Apotheke sind ohne Funktion, auf den Bildschirmen erscheint lediglich die Nachricht der Erpresser.

Austausch der IT-Systeme

Nach Rücksprache mit Polizei und Staatsanwaltschaft zahlt der Apotheker kein Lösegeld. IT-Spezialisten suchen und schließen die Schwachstelle, die den Tätern Zugriff zum System erlaubte. Sie setzen neue, sichere Systeme auf und stellen alle Daten der Apotheke aus den Sicherungskopien wieder her.

- *Kosten für IT-Forensik: 5.000 Euro*

Betriebsunterbrechung

Bis die Systeme wieder laufen, bleibt die Apotheke geschlossen. Auch die Abrechnung mit den Krankenkassen ist unmöglich.

- *Kosten für 5 Tage Betriebsunterbrechung: 12.500 Euro*

Vertrauenskrise

Nachdem die lokale Presse vom Cyberangriff erfährt und darüber berichtet, wenden sich zahlreiche Kunden von der Apotheke ab, der Kundenstamm schrumpft deutlich.

- *Krisenkommunikation: 1.000 Euro*

Der Umsatzrückgang ist nicht gedeckt