CYBERVERSICHERUNG

Cyberrisiken: ...

...Datenleck kann alle Freiberufler betreffen!

Ende November 2019 berichtete der NDR von einem niedergelassenen Arzt aus Celle, dessen Patientendaten für einen längeren Zeitraum frei im Internet zugänglich waren. Sämtliche Arztbe-richte, Röntgenbilder und alle weiteren Daten der Arztpraxis konnten durch Dritte eingesehen werden. Aber was war passiert?

War der Arzt Opfer eines Cyberangriffs geworden?

Die Antwort lautet: **Nein.**

Die Daten waren durch einen frei zugänglichen Windowsserver ohne zusätzlichen Schutz ins Internet gelangt. Ein IT-Experte ist eher zufällig über die Daten im Netz gestolpert und informierte den Arzt über seinen Fund. Bis zu einer endgültigen Schließung der Datenlücke dauerte es jedoch noch mehrere Tage.

Der Arzt hat daraufhin umgehend Kontakt mit seinem IT-Dienstleister aufgenommen, die Fehleranalyse und Beseitigung der Lücke konnten jedoch nicht sofort festgestellt oder abgestellt werden; die sensiblen Daten der Patienten und auch die der Mitarbeiter waren somit weiterhin frei zugänglich im Internet. Einmal ins Netz gelangt, waren diese nicht mehr zu löschen.

Schwachstelle war ein Telekom-Router.
Laut dem Bericht des NDR war eine Schwachstelle in dem in der Praxis verwendeten Telekom-Router Ursache für das Datenleck. Der Router hatte eine falsche Grundeinstellung und hierdurch konnten die Daten des Arztes unbemerkt ins Internet gelangen. Die Schwachstelle selbst ließ sich nur durch ein Update der Telekom beseitigen.

Unklar wie viele weitere Unternehmen betroffen sind. Laut Aussage des NDR wird der Router von der Telekom häufig an Geschäftskunden abgegeben. Es sei nicht klar, wie viele andere Unternehmen durch die Sicherheitslücke des Geräts betroffen sind.

https://www.ndr.de/nachrichten/niedersachsen/hannover_weser-leinegebiet/Datenleck-in-Praxis-30000-Patienten-betroffen,patientendaten116.html

Jeder Nutzer eines der betroffenen Telekomrouter muss sich bewusst sein, dass eventuell neben Geschäftsgeheimnissen auch personenbezogene Daten, Gesundheitsdaten von Kunden oder Mitarbeitern frei zugänglich im Internet sein könnten. Spätestens jetzt sollte sich jedes Unternehmen und nicht nur der Arzt aus Celle die Frage stellen: „Liegt bei mir eine Datenschutzpanne vor und wenn ja was muss ich beachten, was sind meine nächsten Schritte?“

Ähnlich wie bei einem Cyberangriff sind aber viele Unternehmen auch bei dem Thema IT-Sicherheit und Datenschutz noch nicht optimal aufgestellt und im Ernstfall hilflos.

Dabei ist bei einer möglichen Datenpanne nach der Europäischen Datenschutz-Grundverordnung (DSGVO) bereits im Vorfeld einer Risikobewertung der Datensicherheit notwendig und bei Bekanntwerden einer sog. Datenpanne ein zügiges Handeln geboten. Nach Art. 33 Abs. 1 DSGVO muss eine Datenpanne binnen 72 Stunden nach der Kenntnis der Datenschutzverletzung an die zuständige Datenschutzbehörde gemeldet werden.

Vorsicht vor DSGVO-Fallsticken!

Die Vorschrift enthält dabei einige für den Laien unbekannte Fallstricke. So wird eine dokumentierte Risikobewertung gefordert, die als Grundlage für die Entscheidung dient, ob die Datenpanne der Datenschutzbehörde zu melden ist. Auch kann es notwendig werden, dass z. B. Patienten, Kunden oder Mitarbeiter über die Datenpanne informiert werden müssen. Für die meisten Menschen auch unbekannt sind dann die Meldewege, die Meldeinhalte usw. Des Weiteren hat die Datenschutzbehörde, egal ob der Vorfall gesetzlich gemeldet werden muss oder nicht, Erwartungen bezüglich sofort zu treffender Maßnahmen. In jedem Fall wird im Meldefall der Datenpanne geprüft, ob vorgelagerte Pflichten erfüllt worden sind. Eine dieser vorgelagerten Pflichten ist beispielsweise eine dokumentierte Angemessenheitsbewertung der sogenannten technischen und organisatorischen Maßnahmen (Art. 32 DSGVO). Prekär ist, dass man bei schuldhaften Verzöge-rungen der Meldepflichten oder fehlerhaften Meldungen die DSGVO-Bußgelder befürchten muss. Auch gegenüber einem Kunden oder der eigenen Mitarbeiter kann man unter Umständen schadensersatzpflichtig werden, wenn dessen personenbezogene Daten von einer Datenpanne betroffen sind.

Netzwerk an Experten benötigt.

Der Unternehmer benötigt daher unverzüglich nach der Kenntnis ein Netzwerk an Experten, die ihn zeitnah beraten und bei der richtigen Entscheidungsfindung helfen. Neben einem externen Datenschutzbeauftragten oder einem Rechtsanwalt mit Schwerpunkt Datenschutz wird in der Regel auch ein Kommunikationsexperte zum Umgang mit der Presse, den Betroffenen (z. B. Patienten, Mitarbeiter) und der Datenschutzbehörde benötigt.

Wo findet der Unternehmer die Experten im Ernstfall? Reicht hier der Blick in die Gelben Seiten?

Steuerung und Vermittlung von Experten durch die HDI.

Wir als HDI Versicherung AG können auch in dieser schwierigen Lage den dringend benötigten Support mit der Cyberversicherung liefern. Bei dieser Versicherung sind nicht nur Eigen- und Drittschäden als Folge eines Cyberangriffs, z. B. in Form einer Betriebsunterbrechung versichert, son-dern auch die Folgen einer Datenschutzverletzung oder Datenvertraulichkeitsverletzung.

Auch ein Cyberangriff kann zu einer Datenschutzverletzung führen, wenn z. B. ein Hacker Gesundheitsdaten ausspäht oder sogar entwendet und im Darknet verkauft. Wie das Beispiel des Celler Arztes zeigt, kann auch eine technische Sicherheitslücke zu einem Datenschutzproblem werden.

Welche Vorteile bietet die Cyberversicherung?

Support:
Über unsere Cyberversicherung mit integrierter Schadenhotline können wir sofort einen der folgenden Dienstleister vermitteln:

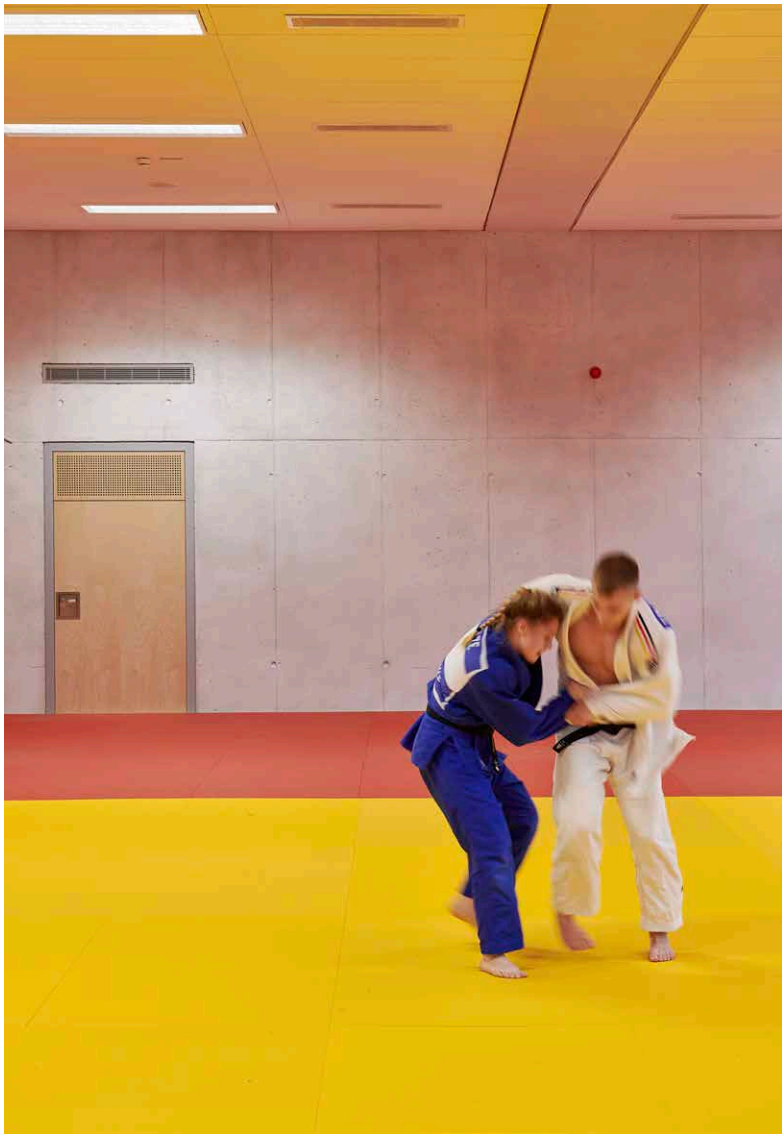
- einen Forensiker (zur Unterstützung des IT-Dienstleisters);
- einen Rechtsanwalt mit Schwerpunkt Datenschutz (zur Prüfung, ob eine Datenschutzpanne vorliegt, gesetzliche Meldepflichten zu beachten sind, wie und mit welchen Inhalten zu melden ist),
- und eine PR-Agentur (als Kommunikationsmanager)

Schadenersatzansprüche:
Wir übernehmen darüber hinaus auch die berechtigten Schadenersatzansprüche von Dritten, die aus einem Hackerangriff, einem Datenverlust oder einer Datenschutzverletzung resultieren können.

Wir übernehmen:

- Ansprüche wegen Urheber- und Namensrechtsverletzungen bei unberechtigter Veröffentlichung elektronischer Medieninhalte;
- Forderungen zur Zahlung von Vertragsstrafen durch E-Payment-Service-Provider;
- die Kosten der Verteidigung in Datenschutzverfahren;
- Vertragsstrafen wegen Datenvertraulichkeitsverletzungen;
- immaterielle Schäden und Personenschäden aufgrund von Persönlichkeitsverletzungen;
- vertragliche Freistellungsverpflichtungen gegenüber Auftragsdatenverarbeitern;
- und vertragliche Schadenersatzansprüche.

Durch die zeitnahe und vollumfängliche Unterstützung mit allen Experten können wir unsere Kunden nicht nur monetär unterstützen, sondern insbesondere den zeitnahen, dringend benötigten Support bieten.



EXPERTENTIPPS:

Zum Schluss haben wir noch ein paar wertvolle Tipps von unseren Experten aus dem HDI Group Data Protection Team:

- **Checklisten einführen!**

Führen Sie eine sog. Angemessenheitsprüfung mittels einer Checkliste durch und dokumentieren Sie diese. Checklisten bieten den Vorteil, dass sie i. d. R. die praxisbezogenen Stolpersteine bei Datensicherheitslücken gut verständlich enthalten. Gleichzeitig unterstützt eine ausgefüllte Checkliste den Nachweis der Durchführung.

Denken Sie daran, dass Sie bei Veränderung der Datensicherheitsinfrastruktur den geänderten Aspekt in der Checkliste neu bewerten. Am besten legen Sie sich das auf Wiedervorlage, so dass Sie sich beispielsweise einmal im Jahr etwaige Änderungen nochmals vor Augen führen.

Mittlerweile gibt es branchenspezifische Checklisten über die gängigen Suchmaschinen im Internet zum Herunterladen, auch die Industrie- und Handelskammern (IHK) bieten häufig entsprechende Muster zum Download an (siehe z. B. https://www.ihk-muenchen.de/de/Service/Recht-und-Steuern/Datenschutz/Die-EU-Datenschutz-Grundverordnung/). Holen Sie sich unter Umständen auch Unterstützung durch Ihren IT-Dienstleister.

- **Datenpanne:**

Zusätzlich sollten Sie sich Gedanken machen, was als Datenpanne nach Art. 33 DSGVO bei Ihnen vorkommen kann. So wissen Sie ganz genau, wann Sie nach DSGVO reagieren müssen. Die IHK bietet auch grobe Leitfäden für den Umgang mit einer Datenpanne an, die eine ge-naue Bewertung des Risikos für den Betroffenen leider nicht zulässt (siehe z.B. Merkblatt https://www.ihk-berlin. de/service-und-beratung/recht-und-steuern/vertragsrecht-online-recht/datenschutzgrundverordnung/meldepflichten-linkliste-4005684), weshalb Sie dafür sorgen müssen ist, dass Sie zumindest einen Experten fragen können.

Machen Sie sich Gedanken, wo und in welcher Weise bei Ihnen welche Art von Datenpannen passieren können. Genau dazu sollten Sie sich einen kontrollierenden Blick angewöhnen.

- **Richtiges Schreddern:**

Wenn z. B. ein Schredder eingesetzt wird, dann schauen Sie sich an, ob das für alle Papierkörbe sichergestellt ist und ob die geschredderten Streifen tatsächlich schmal genug sind. Wenn bessere Schredder erhältlich sind (z. B. kleine Schnipsel statt Streifen), kann sich das für die zusätzliche Sicherheit lohnen.

- **Achtung beim Versand von Informationen!**

Beim Versand von z. B. Berichten per E-Mail sollten Sie unbedingt sichere Verfahren wählen, wenn in diesen Dokumenten personenbezogene Daten und vor allem Gesundheitsdaten vorhanden sind. Diese Verfahren sollten Sie detailliert in Ihren Arbeitsanweisungen niederschreiben. Noch immer passiert es häufig, dass hochsensible Daten offen verschickt werden oder die Dokumente in einem verschlüsselten Archiv versandt werden, das dazugehörige Passwort aber in der gleichen Mail mitgeteilt wird. Nutzen Sie, wenn verfügbar, auch die sicheren Austausch-Plattformen Ihrer Kammern.

- **Immer den Rechner sperren.**

Auch sollten Sie darauf achten, dass eventuell vorhandene Rechner an jedem einzelnen Arbeitsplatz immer gesperrt sind, wenn sich Kunden allein dort aufhalten – ein unbefugter Zugriff auf die Unternehmenssoftware ist unter allen Umständen zu vermeiden.

Gewöhnen Sie sich zudem ruhig an, regelmäßig sich selbst über Suchmaschinen zu suchen. Damit können Sie sogar Datenpannen Anderer zu Ihrer Person ausmachen und zeitnah reagieren.

- **Dokumentation der Datenpanne nicht vergessen!**

Versuchen Sie im Falle einer Datenpanne sofort alle notwendigen Informationen über Ursache, Umfang, betroffene Daten, zeitliche Dauer und denkbare Einsichtnahme zusammenzutragen. Wenn Dienstleister dabei eine Rolle spielen, lassen Sie sich nicht vertrösten. In der Regel sind auch diese Dienstleister zur Mitwirkung des Geschehens gesetzlich oder vertraglich verpflichtet.

- **Das Wichtigste zum Schluss:**

Suchen Sie sich sofort Rat von Experten. Guter Rat ist hier mal nicht teuer!

Autoren

Britta Kruse, Fachreferentin Firmenschaden
Dr. Manuel Piaszek, HDI-Datenschutzexperte
Tobias Rudkowski, HDI-Datenschutzexperte