Versicherungsmakler. Seit 1927.

Kleist

Cyber-Versicherung für Krankenhäuser

17. International Insurance Day Taylor Wessing

Agenda

- Cyberrisiken für medizinische Einrichtungen
- Möglichkeiten und Grenzen einer Cyber-Versicherung

- Stand der Technik
- Schmerzensgeld
- Bußgelder

- Zusammenfassung

Cyberrisiken für medizinische Einrichtungen

Hacker-Angriff auf das Uniklinikum Düsseldorf

- „Shitrix“-Angriff auf die Server des Uniklinikums Düsseldorf am 10.09.2020.
- Umfassender Ausfall der IT-Systeme des Maximalversorgers führte zur Abmeldung von der Notfallversorgung und zu weitreichenden Störungen des Geschäftsablaufs.
- In der Folge musste eine Patientin umgeleitet werden, welche anschließend verstarb. Die Presse titelt: „Patientin starb nach Hacker-Angriff: Die Spur führt nach Russland“.

Foto: dpa

Pressemitteilung des UKD v. 17.09.2020; Handesblatt v. 18.09.2020; Focus v. 22.09.2020

Cyberrisiken für medizinischer Einrichtungen

Stellung der Cyber-Versicherung im Risikomanagement

Operationelles Risiko

Risikoanalyse

Risikoreduktion / -vermeidung?

Nicht transferierbare Restrisiken

Transferierbare Restrisiken

Möglichkeiten und Grenzen der Cyber-Versicherung

Elemente einer Cyber-Versicherung

1. Einrichtung der Cyber-Versicherung – Risikodialog

2. Eigenschadenversicherung – Betriebsunterbrechung

3. Drittschadenversicherung – Haftpflichtansprüche

4. Assistance – weitere Schadenkosten

Möglichkeiten und Grenzen der Cyber-Versicherung

Einrichtung und Risikodialog

- Der Entscheidung einer medizinischen Einrichtung zum Abschluss einer Cyber-Versicherung folgt ein umfangreicher Beratungs- und Platzierungsprozess. Im Fokus steht dabei der Risikodialog zwischen einem oder mehreren Versicherern und dem Krankenhaus.

- Ziel des Risikodialogs ist eine **umfangreiche Prüfung des Risikos aus Sicht des Versicherers**. Dabei werden das bestehende IT-Sicherheitsmanagement, technische Strukturen und eingesetzte Systeme in einem gemeinsamen Dialog detailreich geprüft und bewertet.

- Dieser Prozess dient nicht nur der Risikoprüfung des Versicherers. Im Krankenhaus wird für eine weitere Professionalisierung und externe Bewertung der Maßnahmen und Ergebnisse aus der ersten und zweiten Ebene des Risikomanagements gesorgt.

Möglichkeiten und Grenzen der Cyber-Versicherung

Eigenschäden

- Nach einer Informationssicherheitsverletzung werden bestimmte genannte **Eigenschäden der Versicherungsnehmerin** durch den Versicherer finanziell kompensiert.

- Im Fokus steht die Kompensation einer **Betriebsunterbrechung** infolge einer Informationssicherheitsverletzung. Außerdem können Kosten für die notwendige Wiederherstellung von Daten versichert werden.

- Problematisch ist die genaue Ermittlung des entstandenen Schadens.

Möglichkeiten und Grenzen der Cyber-Versicherung

Drittschäden

- Nach einer Informationssicherheitsverletzung besteht Versicherungsschutz für **gesetzliche Schadensersatzansprüche für Vermögensschäden** in Form einer Haftpflichtversicherung.

- Durch einen Angriff auf das IT-System werden z. B. **falsche Rechnungen und Zahlungsaufforderungen** an Patienten oder Geschäftspartner verwandt. Diesen entstehen dadurch Vermögensschäden, für die das Krankenhaus haften könnte.

- Ein zentrales Problem stellt hier die Beschränkung auf Vermögensschäden dar. Personen- und Sachschäden sind nicht versichert.

Möglichkeiten und Grenzen der Cyber-Versicherung

Assistance

- Nach einer Informationssicherheitsverletzung übernimmt und organisiert der Versicherer bestimmte versicherte notwendige Maßnahmen der **Schadenfeststellung und Schadenbeseitigung**.

- Z.B. Zugriff auf IT-Experten zur Angriffsbeendigung; IT-Forensik; PR-Management; Rechtsanwälte; allg. Krisenmanagement, etc.

- Hier bieten die Versicherungsunternehmen verschiedene Konzepte und Dienstleister an.

Stand der Technik

Problem und Lösung

- Nach der „Stand der Technik“-Klausel hat der Versicherungsnehmer in Hinblick auf die IT-Sicherheit den aktuellen Stand der Technik einzuhalten. Besonders für Organisationen mit facettenreicher IT kann dies eine erhebliche Begrenzung des Versicherungsschutzes darstellen.

- Der „Stand der Technik“ stellt sowohl juristisch als auch tatsächlich einen schwer zu definierenden Begriff dar, der einem Wandel unterliegt.

- Der Versicherungsschutz und der Risikodialog müssen aktiv gestaltet werden, damit das berechtigte Interesse des Versicherers an einem minimierten Risiko für das Krankenhaus auch tatsächlich umsetzbar ist.

Schmerzensgeld

Haftung nach Art. 82 DSG-VO

- Art. 82 Abs. 1 der DSG-VO ermöglicht einen Anspruch auf Ersatz eines immateriellen Schadens bei einem Datenschutzverstoß gegen den Verantwortlichen. Beim Verlust von Gesundheitsdaten ist ein solcher immaterieller Schaden zumindest wahrscheinlich.

- Ein einzelner Anspruch stellt kein existentielles Risiko für eine medizinische Einrichtung dar. Verbinden sich aber viele betroffene Anspruchssteller sind schnell hohe Belastungen denkbar.

- Fraglich ist, ob es sich bei einem Schmerzensgeld um einen Vermögensschaden handelt. Der Versicherungsschutz muss hier bewusst gestaltet werden.

Weiterführend: *Koch/Zellhorn,* VersicherungsPraxis 03/2020, 18.

Bußgeld

z.B. Datenschutzbußgelder i. V. m. Art. 83 DSG-VO

- Die DSG-VO schreibt erhebliche Bußgelder für Verstöße gegen die Datenschutzgesetze vor. Die Höhe eines Bußgelds hängt dabei unter anderem von der Kategorie der betroffenen personenbezogenen Daten ab.

- Einige Versicherungsunternehmen bieten Versicherungsschutz für behördliche Verfahren und darin verhängte Bußgelder nach Datenschutzgesetzen an, **„soweit rechtlich zulässig“**.

- Die rechtliche Wirksamkeit von Versicherungsschutz gegen Bußgelder ist zumindest umstritten. Es besteht demnach keine Rechtssicherheit auch tatsächlich eine Leistung zu erhalten.

Mitteilung des Landesdatenschutzbeauftragten Rheinland-Pfalz v. 03.12.2019

Zusammenfassung

- Die Cyber-Versicherung stellt einen wesentlichen Teil des Risikomanagements medizinischer Einrichtungen dar.
- Die Platzierung des Versicherungsschutzes mit Risikodialog unterstützt die weitergehende Professionalisierung der IT-Sicherheitsstrukturen.
- Die Cyber-Versicherung bietet eine finanzielle Kompensation bei Schäden aufgrund einer Informationssicherheitsverletzung.
- Über die Cyber-Versicherung besteht Zugriff auf top-level externe IT-, Beratungs- und Rechtsdienstleistung.
- Einrichtung, Risikodialog und Vertragsgestaltung verlangen eine enge und professionelle Betreuung und Beratung des Versicherungsnehmers.

Versicherungsmakler. Seit 1927.

Kleist

Cyber-Versicherung für Krankenhäuser

Leo Schulze Schwienhorst
Kleist Versicherungsmakler GmbH
l.schwienhorst@kleist-versicherungsmakler.de
0251 270 767-29