LLOYD'S

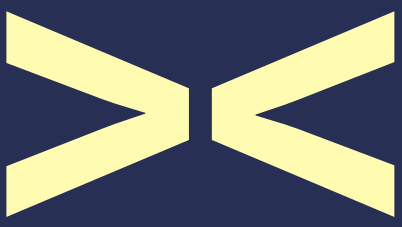
Lücken schließen

Versicherung Ihres Geschäftes gegen zunehmende Cyber-Bedrohungen

Juni 2017

Zusammenfassung

In Zusammenarbeit mit
KPMG und DAC Beachcroft



KPMG

DAC beachcroft

Zusammenfassung

1.1 Überblick

In nur wenigen Jahrzehnten hat das Internet außergewöhnliche Innovationen ermöglicht, durch die neue Geschäftsmodelle und dadurch weltverändernde Unternehmen sowie Millionen Arbeitsplätze geschaffen wurden.

Doch leider hat dieser Fortschritt einen hohen Preis: Digitale Systeme sind von Natur aus anfällig für böswillige Cyberangriffe von Personen oder Gruppen – mit zunehmend ernsten Konsequenzen für Unternehmen in aller Welt. Die Art der Bedrohung verändert sich dabei in einem derart rasanten Tempo, dass die Ergreifung geeigneter Gegenmaßnahmen für Organisationen immer schwieriger wird.

Während die Bedrohung immer komplexer wird, mangelt es vielen Wirtschaftsführern an einem Bewusstsein für Cyber-Gefahren. Einer aktuellen Lloyd's-Umfrage unter mehr als 350 hochrangigen Entscheidungsträgern in Unternehmen aus ganz Europa zufolge sind in den vergangenen fünf Jahren 92 % der Unternehmen auf die eine oder andere Weise Opfer eines Cyberverstoßes geworden. Doch nur 42 % befürchten, dass es in Zukunft noch einmal zu einem Zwischenfall kommen könnte.

Dieser in Zusammenarbeit mit KPMG in Großbritannien, der internationalen Anwaltskanzlei DAC Beachcroft und Lloyd's-Versicherern erstellte Lloyd's-Bericht soll Unternehmen zu einem besseren Verständnis der drohenden Cyberrisiken verhelfen.

Der erste Teil des Berichts nimmt, aufgeschlüsselt nach Sektoren, eine Einschätzung der verschiedenen Cyberbedrohungen vor, denen Unternehmen heutzutage ausgesetzt sind (ein Beispiel für den Finanzdienstleistungssektor sehen Sie hier), und zeigt Wege auf, sie zu entschärfen. Auch werden die gesamten finanziellen Auswirkungen von Datenschutzverletzungen beschrieben und beispielhaft Kosten in Zusammenhang mit vielbeachteten Datenschutzzwischenfällen in jüngster Vergangenheit analysiert.

Der zweite Teil nennt vier Gründe dafür, warum Unternehmen im Umgang mit Cyberrisiken aktiver werden müssen, und gibt dazu fachkundige Empfehlungen der Lloyd's-Cyberversicherer.

Risiken des Finanzdienstleistungssektors

- Hauptrisiko
- Häufige Vorfälle
- Gelegentliche Vorfälle
- Seltene Vorfälle

(Die Anordnung der Farbkreise einer Kategorie ist willkürlich und steht nicht für eine Gewichtung der Häufigkeit der entsprechenden Bedrohungen.)

Die gesamte, in ihrer spartenbezogenen Betrachtung einzigartige Analyse des Berichts finden Sie unter lloyds.com/cyberriskinsight

Untersuchte Sparten:
- Bildung
- Finanzdienstleistungen
- Gesundheitswesen
- Gastgewerbe
- Informationstechnik
- Fertigung
- Medien und Unterhaltung
- Öl und Gas
- Dienstleistungssektor
- Öffentlicher Sektor
- Einzelhandel
- Telekommunikation
- Verkehr
- Versorgungsunternehmen

Den Lloyd's-Bericht „Closing the gap" mit weiteren Informationen zu Cyberrisiken finden Sie in voller Länge unter lloyds.com/closingthegap

1.2 Wichtigste Erkenntnisse

Die Art der gegen Unternehmen gerichteten Cyberangriffe variiert von Branche zu Branche und unterliegt stetigem Wandel. Einige Beispiele:

- Der so genannte CEO Fraud, eine Betrugsmasche, bei der falsche Identitäten genutzt werden, um Unternehmen zur Überweisung von Geld zu veranlassen, greift um sich und hat bereits zu erheblichen finanziellen Schäden geführt.
- Der Finanzdienstleistungssektor ist das bevorzugte Ziel der Angriffe organisierter Cyber-Kriminalität, aber auch der Einzelhandel gerät immer stärker ins Visier.
- Dienstleistungsunternehmen wie Kanzleien und Wirtschaftsprüfungsgesellschaften werden immer häufiger gehackt, um an deren Kunden heranzukommen – oftmals große Konzerne.
- Auch Erpressungstrojaner (Ransomware) und Dienstblockaden (DDoS) richten sich immer häufiger gegen Unternehmen, vor allem im Gesundheitswesen und in der Medien- und Unterhaltungsindustrie.
- Der öffentliche Sektor und der Telekommunikationssektor sind besonders sensibel für Cyberangriffe mit Spionageabsichten.

Unternehmen müssen sich über die Gesamtkosten von Cyberzwischenfällen im Klaren sein, insbesondere über die Folgekosten (z. B. durch den Verlust von Wettbewerbsvorteilen oder Kundenabwanderung). Wenn man diese zu den unmittelbaren Kosten (Kosten für anwaltliche Vertretung und kriminaltechnische Untersuchungen, erpresste Gelder usw.) hinzuzählt, kann die Gesamtrechnung durchaus dramatisch ausfallen.

Es gibt vier Faktoren, die den durch Cyberangriffe angerichteten Schaden noch vergrößern. Umso wichtiger ist es, dass Unternehmen ihre Cyberrisiken mindern und ihre Cybersicherheit erhöhen:

- Höhere Strafen für Unternehmen bei Nichteinhaltung der Vorschriften zur Cybersicherheit gemäß der kommenden europäischen Gesetzgebung.
- Wachsende Bereitschaft der Opfer von Datenschutzverletzungen, gegen die Unternehmen zu prozessieren, in deren Obhut sich die Daten befanden.
- Zunehmende Verantwortung für Cybersicherheit in der Lieferkette.
- Größere Anfälligkeit durch den höheren Vernetzungsgrad von Geräten (Internet der Dinge/ Internet of Things).

1.3 Maßnahmen

Auf dem Lloyd's-Versicherungsmarkt bieten mehr als 70 Versicherer Deckung für Cyberrisiken an. Auf der Grundlage des besonderen Knowhows und Expertenwissens des Lloyd's-Marktes hebt der Bericht vier Möglichkeiten hervor, wie Unternehmen sich auf Cyberangriffe vorbereiten und Cyberrisiken reduzieren können:

1. Verschaffen Sie sich ein klares Bild von den speziellen Gefährdungen für Ihr Unternehmen, darunter die unmittelbaren und langfristigen Kosten – alles von der Reputation, wie sie von Kunden wahrgenommen wird, und dem Wert der Daten in Ihrer Obhut bis hin zu Angriffspunkten in der Lieferkette und Führungskräfte-Profilen.

2. Bewerten Sie gegenwärtige und zukünftige Bedrohungen: beides wird von den Versicherern analysiert, um Ihnen den Versicherungsschutz anzubieten, der Ihre Bedürfnisse optimal erfüllt.

3. Tragen Sie dafür Sorge, dass alle Unternehmensangehörigen, einschließlich der Führungskräfte, umfassend über die Cyberrisiken informiert sind, denen Ihr Unternehmen ausgesetzt ist. Fördern Sie ein entsprechendes Risikomanagement und eine sicherheitsbewusste Unternehmenskultur.

4. Lassen Sie sich beim Abschluss von Cyberversicherungen von Experten beraten, damit Sie sicher sein können, dass Ihre Risiken ausreichend abgedeckt sind.

1.4 Fazit

Die Art der Cyber-Bedrohung wandelt sich beinahe täglich, weshalb die Unternehmen besser auf die Folgen von Cyberzwischenfällen vorbereitet sein müssen. Nicht nur werden die Kosten mit Einführung neuer europäischer Gesetze ansteigen, auch nehmen die Möglichkeiten, wie Unternehmen ins Visier geraten können, zu.

Auch wenn es keinen 100%igen Schutz vor Cyberattacken gibt, können Unternehmen eine ganze Reihe von Maßnahmen ergreifen, um ihr Risiko zu reduzieren und sicherzustellen, dass im Ernstfall die Folgen minimiert werden und das Unternehmen sich möglichst schnell wieder erholt.

Versicherung ist ein wichtiger Baustein in dieser Strategie. Tag für Tag arbeiten die auf Cyber spezialisierten Versicherer des Lloyd's-Marktes weltweit mit Tausenden von Unternehmen, von kleinen und mittleren Unternehmen (sog. KMU's) bis zu Großkonzernen, zusammen, um deren Risiken besser zu verstehen und ihnen die Fachberatung und Deckung anzubieten, die ihrem Bedarf entspricht.

Lesen Sie den vollständigen Lloyd's-Bericht „Closing the gap" über den Umgang mit Cyberrisiken unter **lloyds.com/closingthegap**

Wie die Lloyd's-Versicherer Sie bei der Absicherung gegen Cyberrisiken unterstützen können, erfahren Sie unter **lloyds.com/cybercover**