LLOYD'S

Herausforderung Cyberrisiken Eckdaten für Deutschland

Lesen Sie den vollständigen Lloyd's Bericht „Facing the cyber risk challenge", unter lloyds.com/cyber

Heutzutage sind fast alle Unternehmen, ungeachtet ihrer Größe oder ihres Standorts, auf digitale Technologie angewiesen. Zwar hilft diese Technologie den Unternehmen dabei, effizienter zu arbeiten, reduziert ihre Kosten und erschließt neue Märkte, macht sie aber gleichzeitig viel anfälliger für Cybergefahren.

Unternehmen können Geschäft verlieren, mit Rechtsstreitigkeiten konfrontiert werden, müssen zusehen, wie die Aktienkurse abstürzen und ihr Ruf zerstört wird, wenn sie Opfer eines Cyberangriffs werden.

Auch die Gesetzgebung wird immer strenger. 2018 wird die Europäische Union eine Datenschutz-Grundverordnung mit sehr strengen Auflagen für alle Unternehmen einführen, die mit Daten europäischer Kunden zu tun haben, und empfindliche Geldstrafen für Unternehmen verhängen, die sich nicht an diese Regelungen halten.

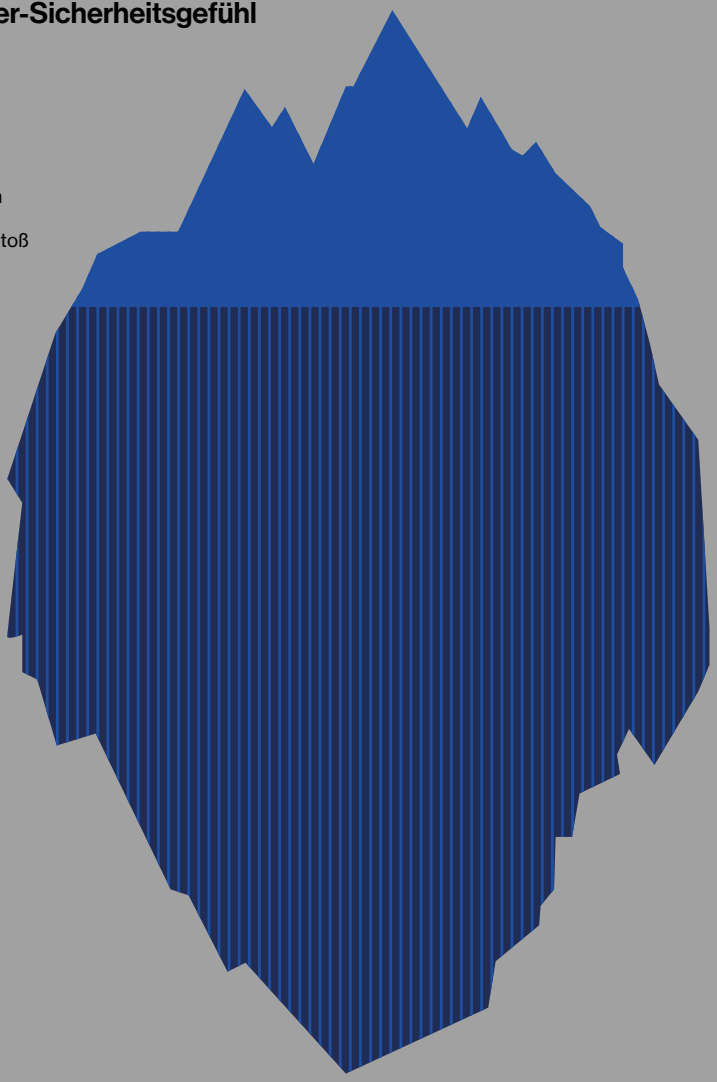
Lloyd's als das globale Zentrum für Cyberversicherungen mit einer ganzen Reihe von Versicherungsprodukten, die zum Schutz vor den Folgen der Cybergefahren beitragen, verfügt über ein besonderes Verständnis für dieses sich schnell verändernde Risikoumfeld.

Wir haben eine Umfrage unter knapp 350 Entscheidungsträgern europäischer Unternehmen mit Umsätzen von über € 250 Millionen in Auftrag gegeben, um herauszufinden, wie sie sich auf die Datenschutz-Grundverordnung vorbereiten und wie sehr sie sich über deren Folgen im Klaren sind, was sie tun, um das Problem Cybersicherheit anzugehen, und ob sie wissen, wie eine Cyberversicherung ihnen beim Schutz ihres Unternehmens helfen kann.*

Falsches Cyber-Sicherheitsgefühl

24%
Unternehmen haben Angst vor einem künftigen Datenverstoß

86%
Unternehmen wurden in den vergangenen fünf Jahren Opfer eines Datenverstoßes



Folgen für die Unternehmen

Folgen, die den deutschen Unternehmen die größten Sorgen bereiten:

52%	Geldstrafen
48%	Gewinnauswirkungen
43%	Aufsichtsbehördliche Untersuchungen
10%	Einige wenige befürchten auch einen Verlust ihrer Kunden nach einem Datenverstoß

Größte Bedrohungen, die nach Ansicht deutscher Unternehmen zu Datenverlust führen könnten

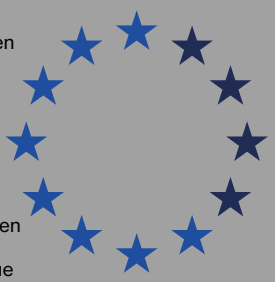
Hackerangriffe zur finanziellen Bereicherung
53%

Menschliches Versagen
50%

Ransomware
47%

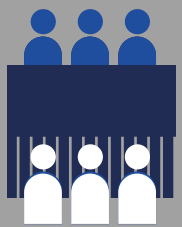
A Eine neue Ära der Cybergesetzgebung

97%
Unternehmen haben schon von der EU-Datenschutz-Grundverordnung gehört



68%
Unternehmen wissen wenig oder gar nichts über die neue EU-Datenschutz-Grundverordnung

Führungsetagen, die Verantwortung übernehmen



47%
Firmenchefs treffen Entscheidungen und erarbeiten Pläne zum Schutz vor Datenverlust

88%
Unternehmen mit Einbindung der Vorstandsebenen in Entscheidungen zum Datenschutz und Aktionsplänen gegen Datenverlust

* Von 350 Entscheidungsträgern aus ganz Europa, die befragt wurden, kamen 34 aus Deutschland

Einschaltung von Experten
Wie eine Versicherung bei Lloyd's helfen kann

Cyber ist aktuell das komplizierteste und größte Risiko für Unternehmen: die Frage ist nur „wann", nicht „ob" ein Unternehmen Opfer eines Cybervorfalls wird.

Bei Lloyd's haben Kunden die größte Auswahl und Vielfalt für ihren Cyberversicherungsbedarf in einem einzigen Markt. 65 Lloyd's Versicherer bieten Versicherungslösungen, die auf die Bedürfnisse eines jeden einzelnen Kunden zugeschnitten werden können.

Der Lloyd's Markt bietet eine Vielfalt an Cyberpolicen zur Deckung aller Eventualitäten, von Geldzahlungen nach einem Cyberangriff und vor Ort Support während der kritischen Phase, bis hin zu Geschäftsunterbrechung, Risikomanagement vor und nach einem Verstoß und Hilfe für die Unternehmen bei der Bewältigung der operativen und finanziellen Folgen und einer möglichen Rufschädigung

Für mehr Informationen und Kontaktdaten von Lloyd's Cybermaklern besuchen Sie unsere Website lloyds.com/cyber

Lloyd's Syndikate, die maßgeschneiderte Cyber-versicherungsprodukte anbieten

65

€ Millionen Kapazität für Cyberversicherung

356*

Typische Cyber-Produkte bei Lloyd's

Benachrichtigungspflicht

Die Deckung umfasst die Kosten für die Benachrichtigung von Dritten (üblicherweise Kunden), die potentiell von einem Datenverstoß betroffen sind. Dies umfasst alle damit verbunden Kosten für PR, Kundendienst und Rechtsfragen. Gedeckt sind auch die Kosten für IT forensische Untersuchungen, um die Ursache des Verstoßes zu ermitteln und überhaupt erst einmal festzustellen, wer zu benachrichtigen ist.

Haftungskosten

Umfasst die Haftung für Kunden, Auftraggeber und Angestellte bei Verlust ihrer vertraulichen, personenbezogenen Daten. Beinhaltet sind auch die Kosten für Klagen und Sammelklagen und alle definierten Rechtskosten.

Regulatorische Kosten

Deckt alle Kosten, die zurückzuführen sind auf den Schutz bei regulatorischen Verstößen.

Einnahmenverlust aufgrund von Netzwerk- und Geschäftsunterbrechung

Deckt die Kosten von Geschäftsausfällen infolge einer Unterbrechung des Betriebs-Computersystems zzgl. aller angefallenen Mehrkosten. Dies beinhaltet die Kosten für die Wiederherstellung der Unternehmens-Webseite, wenn diese abgeschaltet wurde.

Erpressung

Deckt die „Lösegeld"-Kosten, falls ein Dritter Lösegeld verlangt, um nicht vertrauliche Unternehmensdaten öffentlich zu machen oder diesen Schaden zuzufügen. Erpressung erfolgt meistens durch Denial-of-Service-Angriffe.

Rufschädigung

Deckt die finanziellen Verluste durch Kunden, die wegen eines Datenverstoßes ihre Verträge mit einem Unternehmen aufkündigen. Nicht gedeckt sind irgendwelche prognostizierten finanziellen Auswirkungen in der Zukunft, wie beispielsweise Verlust von Neugeschäft an die Konkurrenz.

* Umrechnungskurs zum 12. September 2016

Für mehr Informationen und Kontaktdaten von Lloyd's Cybermaklern besuchen Sie unsere Website lloyds.com/cyber