R • M • K
Mit Werten, Werte sichern!

[RMK report]

Neuigkeiten rund um das Versicherungswesen für Kunden & Geschäftspartner der Radloff, Meier & Kollegen Versicherungsmakler GmbH

Cyber-Risiken – reale Fakten zum virtuellen Risiko

[Vernetzte Prozesse führen zu neuen Risiken]

Ein Großteil der wirtschaftlichen Prozesse ist heutzutage vernetzt und hängt von der Informationstechnologie ab. Damit steigt auch stetig das Risiko für Unternehmen, einen Cyber-Schaden zu erleiden, sei es durch einen technischen Fehler, beabsichtigt oder unbeabsichtigt durch einen eigenen Mitarbeiter, einen Angriff von Cyber-Kriminellen oder durch sonstige Ursachen.

Außerdem verschärfen neue Gesetze zunehmend die Haftung von Unternehmen gegenüber Dritten bei Verstößen gegen die Datenschutzgesetze (Data Liability) oder wegen unberechtigter Datenverarbeitung (Cyber Liability).

„Die stetig ansteigende Vernetzung von Daten macht Unternehmen immer anfälliger für Cyber-Schäden."

Unternehmen und ihre Manger stehen vor der Herausforderung, ihre Systeme, Daten und Produktionsanlagen vor Hackerangriffen zu schützen und die Verarbeitung und Speicherung von Daten (insbesondere personenbezogene Daten) sicher zu gestalten.

[Definition Cyber-Risiken]

Das Wort „Cyber" ist derzeit in aller Munde. Doch was bedeutet es eigentlich und welchen Umfang hat es? Ursprünglich stammt der Begriff vom englischen Wort cybernetics, welcher als Vorsilbe für alles, was mit der virtuellen Welt zu tun hat, verwendet wird.

Wichtig ist die Abgrenzung der Begriffe „Cyber-Risiken" und „IT-Risiken", welche fälschlicherweise oft synonym verwendet werden. Während das IT-Risiko sich allerdings eher auf materielle IT-Anlagen bezieht, geht das Cyber-Risiko viel weiter und umfasst zusätzlich Risiken, die durch die Vernetzung von Daten und die Verarbeitung von digitalen Daten entstehen.

Als drei zentrale Cyber-Risiken können Verletzungen im Zusammenhang mit **Datenverfügbarkeit** (Daten gehen verloren), **Datenintegrität** (Daten werden verändert) und **Datenvertraulichkeit** (Daten sind für Unberechtigte zu erreichen) aufgeführt werden.

[Schadenszenarien]

Die möglichen Schadenszenarien, welche sich durch Cyber-Risiken ergeben, sind vielseitig und komplex. In Unternehmen können die Bereiche IT- und Datensicherheit, Datenschutz, Compliance, Reputation sowie Haftungsrisiken betroffen sein, wobei ein Schadenereignis sich meist auf mehrere Bereiche auswirkt. Systematisieren

lassen sich die Schadenszenarien durch die Unterscheidung der Ursache und der Schadenart.

Ursächlich für das Auftreten eines Cyber-Vorfalls können aus Sicht des Unternehmens sowohl **interne als auch externe Faktoren** sein.

Mögliche interne Schadenverursacher sind beispielsweise technische Defekte, Stromausfälle oder Mitarbeiter. Letztere können hierbei beabsichtigt handeln und zum Beispiel Daten stehlen oder auch unbeabsichtigt ein System falsch ausführen oder Malware (Schadsoftware) in das Unternehmenssystem bringen und so den Zugriff auf sensible Daten ermöglichen.

Externe Ursachen finden sich zum Beispiel in Form von externen Netzangriffen, welche in zahlreiche Varianten existieren. Dazu zählen gestohlene personenbezogene Datensätze, lahmgelegte Websites durch DOS-Attacken, Missachtung von Datenschutzgesetzen, Hacker-Attacken auf Produktionsanlagen und Cloud-Speicher, Wirtschaftsspionage und Verbreitung von Malware (Viren, Würmer etc.), Identitätsdiebstahl oder Social Engineering, Phishing und viele mehr.

„Cyber-Schäden können durch diverse Ursachen innerhalb und außerhalb des Unternehmens entstehen."

Bei der Art des Schadens ist nach **Eigen- und Fremdschaden zu unterscheiden.**

Unter erstere fallen beispielsweise Kosten für Datenwiederherstellung, Benachrichtigungen bei Datenschutzrechtsverletzungen, Forensik, Reputationsmanagement, Betriebsunterbrechungsschäden, Erpressung, Rechtsberatung, Schäden wegen Netzwerkangriffen durch Dritte (Hackerangriffe) und Schäden wegen Datenmissbrauchs durch Dritte.

Aufgrund ständiger Verschärfung von rechtlichen Regulationen rücken auch die Fremdschäden immer mehr in den Fokus, beispielsweise in Form von Ansprüchen Dritter wegen Verstößen gegen Datenschutzgesetze, Ansprüchen Dritter wegen unberechtigter Datenverarbeitung oder Vermögensschäden durch die Weitergabe von Malware.

„Auch verschärfte gesetzliche Regularien erhöhen das Risiko für Unternehmen."

[Relevanz]

Das Thema Cyber-Risiken ist derzeit allgegenwärtig. Doch wie relevant ist es tatsächlich für Unternehmen? Die Faktoren **Häufigkeit, Schadenhöhe** sowie **rechtliche Rahmenbedingungen** zeigen deutlich die stets wachsende Relevanz dieses Themas. Die Meldungen zu konkreten Cyber-Vorfällen häufen sich, betroffen sind hierbei nicht mehr nur Konzerne, sondern mehr und mehr auch der Mittelstand. Laut eigenen Angaben waren bisher bereits knapp 60 % der deutschen Unternehmen Opfer einer Cyber-Attacke, vor drei Jahren waren es nur 27 %. Die Tendenz ist demnach stark steigend. Die Dunkelziffer dürfte dabei deutlich höher liegen, da viele Cyber-Angriffe nicht öffentlich gemacht werden.

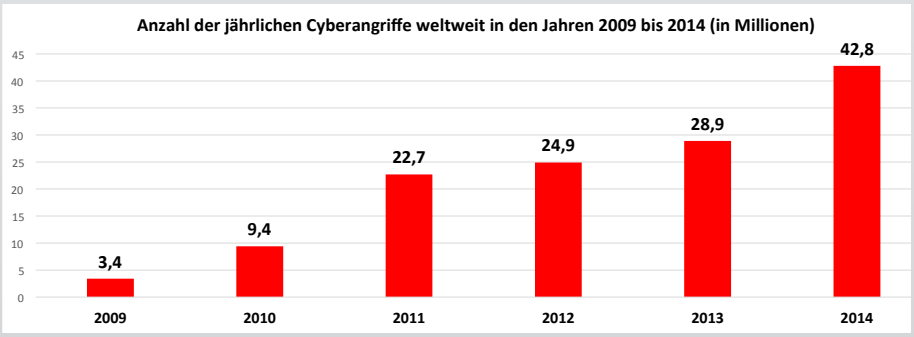
Viele nationale und internationale Unternehmen sehen in den Cyber-Risiken das größte finanzielle Risiko für ihre zukünftige Geschäftstätigkeit.

(Quellen: KPMG, e-crime-Studie 2015 sowie www.bitcom.org, Artikel „Digitale Angriffe auf jedes zweite Unternehmen", April 2015).

„Bereits knapp 60 % der deutschen Unternehmen waren Opfer einer Cyber-Attacke, Tendenz steigend."

Die Schadenhöhe im Zusammenhang mit Cyber kann für viele Unternehmen existenzbedrohend sein. So belaufen sich etwa die durchschnittlichen Kosten eines Datenschutzvorfalls für deutsche Unternehmen etwa auf 4,8 Mio. USD, die Kosten für einen durchschnittlichen Cyber-Schaden auf 128.000 € bis 609.000 €.

Konkrete Schadenszenarien könnten so aussehen: Bei einem DOS-Angriff auf einen Online-Shop ist dieser für 48 Stunden nicht zu erreichen, Aufwendungen für Forensik sind nötig und Schäden im

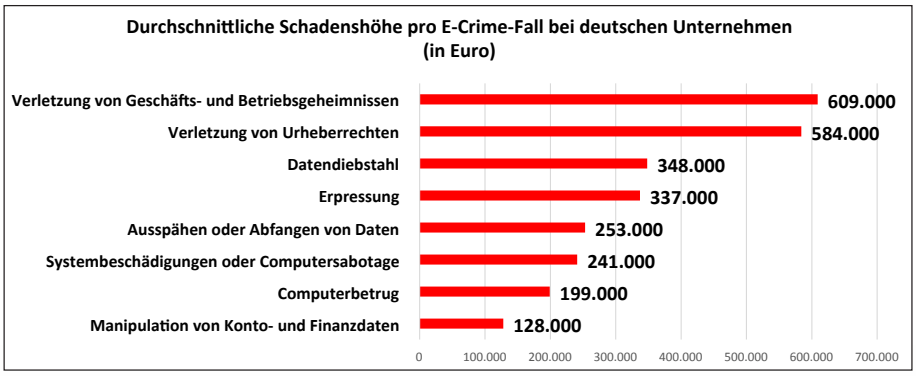


Quelle: PwC/Statista 2015

Zusammenhang mit Umsatzeinbußen und Reputation entstehen. Die endgültige Schadenhöhe kann sich auf 185.000 € belaufen. Auch möglich wäre ein Fall, in dem personenbezogene Daten bei einem Hackerangriff gestohlen werden oder durch einen liegengelassenen Laptop auf einer Geschäftsreise verloren gehen. Kunden und Behörden müssen gemäß BDSG benachrichtigt werden, Bußgelder aufgrund einer Datenschutzverletzung fallen an, ebenso Kosten für Forensik und Umsatzeinbußen und Reputationsschäden. Die Schadenhöhe könnte hier bei 1,25 Mio. € liegen. Ein weiterer konkreter Schadenfall ist die Infizierung eines Hochregallagers mit einem Virus, wodurch die Ortung der eingelagerten Ware nicht mehr möglich ist. Es kommt zu einem Betriebsunterbrechungsschaden, außerdem fallen Kosten der Datenwiederherstellung und Vertragsstrafen im B2B-Bereich an. Die Schadenhöhe kann sich laut Rechenbeispiel auf 695.000 € belaufen.

(Quellen: KPMG e-crime-Studie 2015 sowie ACE-European Group Limited Direktion für Deutschland)

Zusätzliche Brisanz erhält das Thema durch stetig angepasste rechtliche Rahmenbedingungen, welche die Unternehmenshaftung gegenüber Dritten im Zusammenhang mit Datenvorfällen immer weiter verschärfen. Aus den Vorschriften der §§ 42a, 43 und 44 BDSG können beispielsweise durch Bußgelder und Geldstrafen bei einem Cyber-Vorfall Kosten in Höhe von mehreren Hunderttausend Euro entstehen. Zudem liegt hier eine verschuldensunabhängige Haftung vor, was die Relevanz für Unternehmen noch weiter erhöht, denn ein unverschuldeter Cyber-Angriff kann jeden treffen.



Quelle: KPMG, e-crime 2015/Statista 2015

„Unternehmen können auch ohne Verschulden in Haftung genommen werden."

[Versicherungslösung: Cyber-Policen]

Trotz bester IT-Sicherheit ist ein 100%iger Schutz gegen Cyber-Risiken nicht möglich. Eine zusätzliche Absicherung bieten Cyber-Policen, die im Gegensatz zu üblichen Industrieversicherungen wie Haftpflicht oder Betriebsunterbrechung ausreichende Deckung bieten. Versicherbar sind sowohl Eigen- als auch Drittschäden im Zusammenhang mit Verletzungen von Datenverfügbarkeit, Datenintegrität und Datenvertraulichkeit.

Mögliche Deckungsbausteine umfassen beispielsweise:

- Ertragsaufall/ Betriebsunterbrechung
- Erpressung
- Sachverständigenkosten/Forensik
- Datenwiederherstellung
- Rufschädigung/Krisenmanagement
- Datenschutzverletzungen
- Internetbetrug

Aus den diversen Möglichkeiten der Absicherung ergibt sich, dass Cyber-Policen extrem vielfältig sind und genau zu den Risiken eines Unternehmens passen müssen. Standardlösungen sind wenig sinnvoll, notwendig ist eine sorgfältige Risikoanalyse zur Angebotserstellung.

[Fazit]

Cyber-Risiken sind vielfältig, komplex und dynamisch, außerdem gewinnen sie stetig an Relevanz. Cyber-Policen können gewisse Cyber-Risiken finanziell absichern, Voraussetzung ist hier eine genaue Risikoanalyse und eine individuelle Deckung statt einer Standardlösung.

Christina Engels-Müller

Master of Law (LL.M.)

R • M • K

Mit Werten, Werte sichern!

[RMKreport]

ANSCHRIFT
Radloff, Meier & Kollegen
Versicherungsmakler GmbH
Bartholomäusstraße 26 C
D-90489 Nürnberg

KOMMUNIKATION
Fon +49 (09 11) 37 65 03-0
Fax +49 (09 11) 37 65 03-33
info@r-m-k.de · www.r-m-k.de

GESCHÄFTSFÜHRER
Versicherungsfachwirt
Manfred Radloff
Versicherungsbetriebswirt (DVA)
Rudolf Meier

VERMITTLERREGISTER
IHK München
Register-Nr. D-QXUY-IAYYV-85