Schützen Sie Ihr Unternehmen optimal gegen IT-Risiken/ **Risiko-Check IT.**

Maßstäbe / **neu definiert**

Einleitung

Die Abhängigkeit der Unternehmen von einer funktionsfähigen IT steigt und damit die Ansprüche an die Notfallplanung bzw. das Business Continuity Management. Gleichzeitig steigen rechtliche Anforderungen z. B. an den Datenschutz. Auch die Bedrohungslage durch Schadsoftware, Hackerangriffe etc. hat sich in den letzten Jahren verschärft. Eine absolute Sicherheit ist dabei praktisch nicht möglich, zumindest nicht ohne eine erhebliche Einschränkung der Arbeitsfähigkeit zu akzeptieren.

Damit gewinnt ein gutes Risikomanagement an Bedeutung. Sicherheitslücken müssen identifiziert, bewertet und durch technische wie organisatorische Maßnahmen behandelt werden. Ein Hilfsmittel ist die Einordnung von Risiken in eine Risikomatrix, wie sie die rechts abgebildete Grafik zeigt. Möglichkeiten der Risikobehandlung sind die Vermeidung von Risiken, die Verminderung oder die Risikoübertragung z. B. auf Versicherungen bis hin zur Selbstübernahme des Restrisikos.

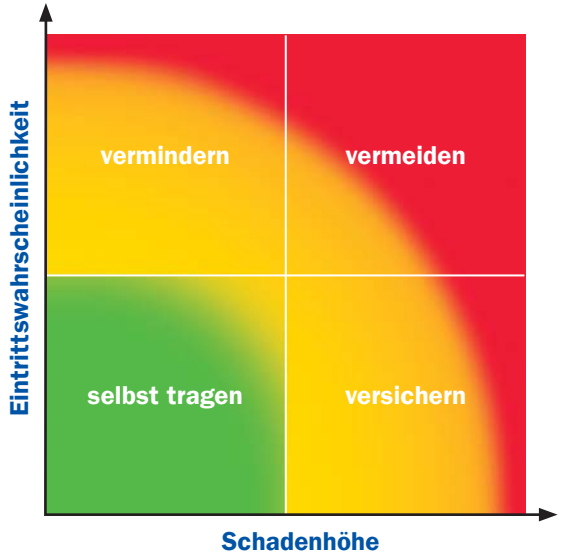
Ihre
AXA Versicherung AG
51171 Köln
www.axa.de/Geschäftskunden

Für die Auswahl eines geeigneten und optimalen Versicherungsschutzes soll der vorliegende „Risiko-Check IT“ eine Hilfestellung bieten.

Er ermöglicht u. a. den Nachweis der Forderung des Grundschutz-Kataloges des BSI, Modul M 6.16 „Abschließen von Versicherungen“, z. B. im Rahmen einer Zertifizierung.

Mit dem „Risiko-Check IT“ werden grundsätzliche Versicherungsmöglichkeiten aufgezeigt (ohne dabei einen Anspruch auf Vollständigkeit erheben zu wollen). Es gelten die jeweiligen tatsächlich vereinbarten Versicherungsbedingungen (z. B. zu Versicherungssummen, Ausschlüssen, Obliegenheiten).

Der „Risiko-Check IT“ bietet eine gute Grundlage für ein Gespräch mit Ihrem Versicherungsvermittler. Er ist **nicht** anwendbar auf IT-Dienstleister; hierfür existiert ein separater Risiko-Check.



Allgemeine Unternehmensdaten

Firma: _____

Inhaber/Geschäftsführer: _____

Homepage: _____

Straße: _____

PLZ/Ort: _____

Telefon: _____

Fax: _____

E-Mail: _____

Betriebsbeschreibung:

_____

_____

_____

_____

_____

_____

Aktueller Jahresumsatz: _____ EUR

Anzahl Mitarbeiter: _____

Datenschutz-Hinweis und Bestätigung des Kunden
Einwilligungserklärung: Ich bin damit einverstanden, dass mein zuständiger Vermittler und AXA Versicherung AG die zum Risiko-Check IT erforderlichen Unternehmens- und personenbezogenen Daten erheben, speichern und zum Zweck der Prüfung der Versicherbarkeit sowie zur Beratung und im Falle der Antragsstellung auch zur Risikoprüfung verarbeiten dürfen.

_____

Ort, Datum Betriebsinhaber/Bevollmächtigter

Notizen: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Risiko-Check IT

1 Betriebsunterbrechung durch Ausfall der IT bzw. des internen Netzwerks oder des Zugangs zum Internet

Der Ausfall der IT kann verschiedene Ursachen haben und je nach Ursache kann sich auch die maximale Ausfalldauer unterscheiden. Auch der mögliche Versicherungsschutz zur Minderung der finanziellen Auswirkung ist je nach Ursache zu unterscheiden.

Die Schadenhöhe kann über die Zeitdauer multipliziert mit den Ausfallkosten je Zeiteinheit abgeschätzt werden. Dabei ist einzurechnen, dass ggf. die Betriebsunterbrechung in den Tagen und Wochen danach wieder ganz oder teilweise durch Mehrumsatz kompensiert werden kann. Zur Ermittlung einer angemessenen Versicherungssumme sollte der jeweils mögliche Maximalschaden bestimmt werden.

	Potenzielles Risiko	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Ausfall infolge eines Sachschadens durch Brand, Rauch, Diebstahl, Vandalismus, Sabotage, Erdbeben, Wasser, Überspannung, Bedienungsfehler etc.**		Sachversicherung (z. B. Elektronikversicherung) mit entsprechender darauf aufsetzender Betriebsunterbrechungsversicherung bzw. Mehrkostenversicherung	**Es ist in der Deckung darauf zu achten, welche Gefahren in der jeweiligen Police tatsächlich versichert sind!** Ausfall der IT kann durch einen Sachschaden an der Klimaanlage verursacht sein. Möglichkeit der Mitversicherung in der Elektronikversicherung gegeben, wenn die Klimaanlage in die Deckung eingeschlossen ist. Betriebsunterbrechung durch längere Unterbrechung der öffentlichen Stromversorgung: Möglichkeit der Mitversicherung in der Elektronikbetriebsunterbrechungsversicherung
B	**Ausfall durch Schadsoftware**		**Nicht versicherbar**	
C	**Ausfall durch zielgerichtete DoS-Attacke[1] bzw. Hacker-Angriffe** (z. B. Manipulation der Webseite)		Vertrauensschadenversicherung: Deckung der Kosten für Datenwiederherstellung und der Mehrkosten Siehe auch 4 A und B **Kosten der Betriebsunterbrechung sind nicht versicherbar.**	
D	**Ausfall des Internetzugangs** (externe Ursachen)		**Nicht versicherbar**	Haftung des Netzbetreibers gemäß § 44a Telekommunikationsgesetz in begrenzter Höhe Ggf. Anspruchsmöglichkeiten prüfen (z. B. wenn durch Bauarbeiten verursacht)
E	**Durch Ausfall verursachter Reputationsschaden**		**Kosten für Rufwiederherstellung etc. sind nicht versicherbar**	

[1] DoS = Denial of Service – Ausfall durch eine hohe Anzahl von Anfragen/Zugriffen auf den Server/Rechner

Risiko-Check IT

2 Datenlöschung/Datenverlust

Neben der Datenlöschung ist auch die Änderung oder der Zugangsverlust von Daten bzw. die Störung der Datenintegrität möglich.
Ein derartiger Datenverlust kann in eine Betriebsunterbrechung münden (siehe Punkt 1). Bei allen Versicherungsmöglichkeiten wird Datensicherung vorausgesetzt.

	Potenzielles Risiko	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Löschung eigener Daten aufgrund eines Sachschadens am Datenträger**		Sachinhalts- bzw. Elektronikversicherung (mit Daten- oder Softwareversicherung): Kosten für Datenwiederherstellung	
B	**Löschung oder Veränderung eigener Daten aufgrund einer Manipulation oder Fehlbedienung** (ohne vorausgehenden Sachschaden!)		Elektronikversicherung mit Softwareversicherung (Kosten für die Wiederherstellung) Vertrauensschadenversicherung bei vorsätzlicher Handlung (Wiederherstellungs- und Mehrkosten)	Zielgerichteter Hackerangriff ist versicherbar.
C	**Verlust eigener Daten aufgrund Schadsoftware (Malware)** (ohne vorausgehenden Sachschaden!)		**Bei nicht zielgerichteten Angriffen nicht versicherbar** Vertrauensschadenversicherung bei vorsätzlicher Handlung (Wiederherstellungs- und Mehrkosten), siehe Punkt 4 A und B!	
D	**Verlust fremder Daten**		Haftpflichtversicherung Ggf. Straf-Rechtsschutz (siehe Punkt 3 B)	Auf Ausschlüsse in den Versicherungsbedingungen achten!
E	**Zugangsverlust**		**Nicht versicherbar**	

Risiko-Check IT

3 Verstoß gegen Daten-, Urheber- und sonstige Schutzgesetze

Bei Umgang mit personenbezogenen Daten können sich Verstöße gegen das Datenschutzgesetz ergeben, z. B. durch unbeabsichtigte Veröffentlichung von Kundendaten im Internet. Urheber- oder sonstige Schutzgesetze können insbesondere bei der Gestaltung von Webseiten verletzt werden. Hierunter fallen auch Filesharing-Vorwürfe.

	Potenzielles Risiko	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Verstöße gegen das Bundesdaten-schutzgesetz (BDSG)**		Sofern für Schutzgesetzverletzung Deckung besteht: ■ Haftpflichtversicherung ■ Rechtsschutzversicherung (Daten-Rechtsschutz, Straf-Rechtsschutz)	
B	**Ermittlungsverfahren wegen des Vorwurfs eines strafrechtlich relevanten Verstoßes** ■ **gegen das UWG**[2)] ■ **gegen das Urheberrecht** ■ **gegen §§ 202a, 202b, 202c, 303a und 303b StGB** (sogenannte Hackerparagrafen)		Straf-Rechtsschutzversicherung	
C	**Aus Verstößen sich ergebende Haftpflichtansprüche Dritter**		Vermögensschadenhaftpflichtversicherung	Ggf. ist Deckung auf bestimmte Schutzgesetze eingeschränkt! Deckungseinschränkung ggf. auch auf bestimmte Branchen

[2)] UWG = Gesetz gegen unlauteren Wettbewerb

Risiko-Check IT

4 Kosten für Schäden durch Missbrauch und Manipulation

Daten in Unternehmen können einen hohen Wert haben. Bei einem Diebstahl von entsprechenden Daten, bei Werksspionage oder auch im Falle der illegalen Nutzung von Daten zum Zwecke der Bereicherung durch Mitarbeiter oder durch Angreifer von außen können dem Unternehmen entsprechende Schäden entstehen.

	Potenzielles Risiko	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Zielgerichtete und vorsätzliche Hackerangriffe mit Bereicherungsabsicht** (z. B. Telefonhacking)		Vertrauensschadenversicherung, sofern unmittelbare Bereicherung **Datendiebstahl z. B. zum Zwecke des Kreditkartenmissbrauchs ist nicht versicherbar**	Voraussetzungen beachten wie Firewall, Änderung von Passwörtern etc.
B	**Zielgerichtete und vorsätzliche Hackerangriffe ohne Bereicherungsabsicht** (z. B. zur Rufschädigung durch Manipulation der Webseite)		Vertrauensschadenversicherung für Wiederherstellungs- und Mehrkosten **Wiederherstellung des guten Rufs ist nicht versicherbar**	Voraussetzungen beachten wie Firewall, Änderung von Passwörtern etc.
C	**Diebstahl eigener Daten und Unterschlagung durch eigene Mitarbeiter** („Vertrauenspersonen“[3])		Vertrauensschadenversicherung	EDV-Service-Personal wird mit versichert, auch wenn dieses nur online tätig wird
D	**Diebstahl fremder Daten auf eigenen Rechnern durch eigene Mitarbeiter**		Der unmittelbare Schaden des Dritten ist durch Vertrauensschadenversicherung versicherbar	**Entgangener Gewinn des Dritten ist nicht versicherbar, da kein unmittelbarer Schaden** Da es sich um Vorsatzschäden handelt, greift bei Schäden Dritter nicht die Haftpflichtversicherung
E	**Nicht zielgerichtete Angriffe auf die EDV durch Schadsoftware oder DoS-Attacke**		**Nicht versicherbar**	

[3] Vertrauenspersonen sind sämtliche zum Zeitpunkt der Schadenverursachung aufgrund eines Arbeits- oder Dienstvertrages Beschäftigte.

Risiko-Check IT

5 Schäden durch vom Unternehmen verbreitete Schadsoftware (Viren, Trojaner etc.)

Über Internetseiten, Software, E-Mails oder auch über vom Unternehmen verteilte Datenträger (z. B. Werbegeschenke!) kann das Unternehmen Ausgangspunkt für die Verbreitung von Viren, Trojanern etc. sein, die bei den Kunden entsprechende Schäden verursachen. Diese können durch das mögliche Kumul ggf. empfindliche Höhen erreichen. Hierbei ist in der Regel die Haftpflichtversicherung angesprochen. Zur Durchsetzung von derartigen Haftpflichtansprüchen werden eine aktuelle Antivirensoftware und Firewalls vorausgesetzt.

	Potenzielles Risiko	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Schäden wie Datenverlust, Ausfall der IT, Sachschäden etc. bei Dritten durch Schadsoftware**		Haftpflichtversicherung	Auf Ausschlüsse in den Versicherungsbedingungen achten Ggf. bestehen Regressmöglichkeiten, wenn die Quelle der Schadsoftware bestimmt werden kann.

Risiko-Check IT

6 Zugangserpressung / Napping

Werden Zugangsdaten z. B. zu externen Datenspeichern wie Cloud Computing oder E-Mail-Accounts gestohlen (z. B. durch sogenanntes „Phishing“), kann dies zu einem Erpressungsversuch führen. Der Zugang wird erst nach Zahlung eines Lösegelds wieder freigegeben. Auch Datendiebstahl kann zum Zwecke der Erpressung einer Nicht-Veröffentlichung genutzt werden.

	Potenzielles Risiko	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Betriebsunterbrechung durch Zugangsstörung/Ausfall des E-Mail-Verkehrs**		Nicht versicherbar	
B	**Lösegeldzahlung**		Nicht versicherbar	