Geschäftskunden

Ich möchte Cyber- und IT-Risiken systematisch erkennen, bewerten und versichern.

o-Check IT

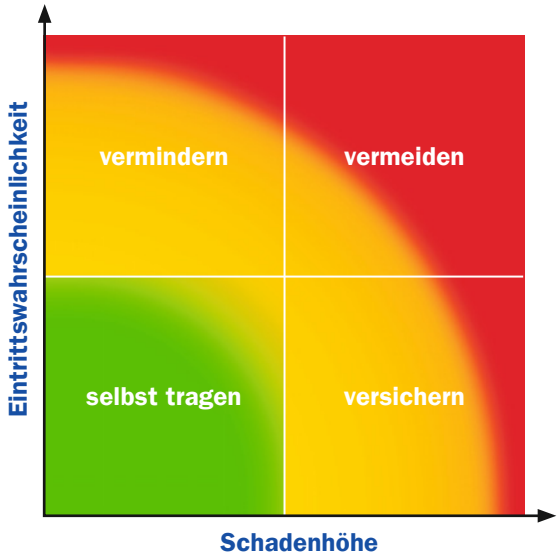
omanagement

Maßstäbe / neu definiert

Einleitung

Die Abhängigkeit der Geschäftsprozesse von IT-Systemen, Daten und dem Zugang zum Internet steigt und damit die Anforderungen an das Risikomanagement. Gleichzeitig verschärfen sich die rechtlichen Regelungen z. B. bezüglich Datenschutz oder IT-Sicherheit allgemein. Dabei hat sich die Bedrohungslage durch intelligente Hacker-Angriffe und Schadsoftware in den letzten Jahren weiter verschärft. Eine absolute Sicherheit ist nicht möglich.

Damit gewinnt ein angemessenes und zielgerichtetes Handeln bezogen auf IT- und Datensicherheit an Bedeutung. Risiken müssen identifiziert, bewertet und durch technische wie organisatorische Maßnahmen reduziert werden. Als Hilfsmittel für die Priorisierung von Risiken dient beispielsweise eine Risikomatrix wie sie die rechts abgebildete Grafik zeigt. Für die an die Analyse anschließende Risikobewältigung können Vermeidung, Verminderung, Übertragung z. B. durch Versicherung, bis hin zur Selbsttragung des Restrisikos gewählt werden.



Für die systematische Identifizierung von IT- und Cyber-Risiken und zur Auswahl eines geeigneten Versicherungsschutzes bietet dieser „Risiko-Check IT“ Hilfestellung an. Dabei wird insbesondere auf die Cyber-Versicherung ByteProtect von AXA aber auch auf andere Versicherungsmöglichkeiten eingegangen.

Der Risiko-Check ermöglicht den Nachweis der Forderung des Grundschutz-Kataloges des BSI, Modul M 6.16 „Abschließen von Versicherungen“ im Rahmen einer Zertifizierung. Er kann außerdem in das betriebliche Risikomanagement integriert werden.

Dieser „Risiko-Check IT“ erhebt keinen Anspruch auf Vollständigkeit. Im konkreten Fall sind natürlich stets die jeweiligen tatsächlich vereinbarten Versicherungsbedingungen (z. B. Versicherungsumfang, Ausschlüsse) zu berücksichtigen. Außerdem ist zu beachten, dass bestimmte Versicherungsprodukte nicht für jede Branche bzw. Tätigkeit eines Unternehmens angeboten werden und auch regionale Einschränkungen bestehen können.

Der „Risiko-Check IT“ bietet darüber hinaus eine gute Grundlage bzw. einen Leitfaden für ein Gespräch mit Ihrem Versicherungsvermittler.

Ihre
AXA Versicherung AG
51171 Köln
www.AXA.de/it-check

Allgemeine Unternehmensdaten

Firma: _____

Inhaber/Geschäftsführer: _____

Homepage: _____

Straße: _____

PLZ/Ort: _____

Telefon: _____

E-Mail: _____

Notizen:

Betriebsbeschreibung:

Aktueller Jahresumsatz: _____ EUR

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

Formular zurücksetzen

TIPP: Sie wollen wissen, wo Sie hinsichtlich IT-Sicherheit stehen? Machen Sie den Quick-Check im Internet. https://www.vds-quick-check.de

Risiko-Check IT

1 Betriebsunterbrechung durch Ausfall der IT, der Webseite oder des Zugangs zum Internet

Der Ausfall der IT kann verschiedene Ursachen haben und je nach Ursache kann sich auch die Ausfalldauer unterscheiden. Es wird empfohlen, den Einfluss eines EDV-/Internet-Ausfalls auf die Geschäftsprozesse im Rahmen einer Business-Impact-Analyse zu untersuchen.

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. Dabei sind ggf. auch Mehrkosten zu berücksichtigen, die üblicherweise in Betriebsunterbrechungsversicherungen mitversichert sind.

	Ursache/Gefahr	Mögliche Schadenhöhe[1]	Versicherungsmöglichkeit	Anmerkungen
A	**Sachschaden** Ausfall in Folge eines Sachschadens durch: Brand, Rauch, Diebstahl, Vandalismus, Sabotage, Erdbeben, Wasser, Überspannung/ Blitzschlag, Überhitzung, Bedienungsfehler etc.		Sachversicherung (z. B. Elektronikversicherung) mit entsprechender darauf aufsetzender Betriebsunterbrechungs- bzw. Mehrkostenversicherung.	Es ist darauf zu achten, welche Gefahren in der jeweiligen Police tatsächlich versichert sind! Ausfall der IT kann auch durch einen Sachschaden an der Klimaanlage verursacht sein. Möglichkeit der Mitversicherung in der Elektronikversicherung ist gegeben, wenn die Klimaanlage in diese Deckung eingeschlossen ist.
B	**Stromausfall** Ausfall als Folge einer Unterbrechung der öffentlichen Stromversorgung.		Ggf. Möglichkeit der Mitversicherung in der Maschinenbetriebsunterbrechungsversicherung.	Ausschlüsse z. B. für höhere Gewalt beachten!
C	**Cyber-/Hacker-Angriff** Angriff mit Hilfe von eingeschleuster Schadsoftware, Übernahme von IT-Steuerungen, Zugriff auf IT-Systeme etc.		**ByteProtect:** Baustein A d)[3]	Durch weit verbreitete Schadsoftware besteht ggf. hohes Kumulrisiko für den Versicherer. Daher sollte auf entsprechende Ausschlüsse oder Beschränkung auf „zielgerichtete“ Angriffe geachtet werden.
D	**DoS-Angriff[2]** Ausfall durch DoS-Attacke		**ByteProtect:** Baustein A c)[3]	Angriffe können die IT-Systeme des Unternehmens, aber auch die Web-Seite oder IT-Ressourcen, die bei Dritten gehostet werden, treffen!

[1] In dieser Spalte können Sie ihre eigene Schadenschätzung eintragen, quantitativ oder auch qualitativ (z. B. hoch, mittel, gering)
[2] DoS = Denial of Service – Ausfall durch eine hohe Anzahl von Anfragen/Zugriffen auf den Server/Rechner
[3] Zur Übersicht der Bausteine von ByteProtect wird auf die Tabelle im Anhang verwiesen

Risiko-Check IT

E	**Ausfall des Internets bzw. der Telekommunikation oder der Webseite** aufgrund externer Ursachen (z. B. Bauarbeiten, Verlust von Zugriffsrechten, Sperrungen)		**ByteProtect:** Baustein A a) Insbesondere relevant, wenn Standorte über Datenleitung von zentralen IT-Ressourcen abhängig sind.	Haftung des Netzbetreibers gemäß § 44 a Telekommunikationsgesetz nur in begrenzter Höhe. Ausschluss für höhere Gewalt (z. B. Sturm, Überschwemmung), Stromausfall und zu geringe Bandbreite beachten.
F	**Bedienungsfehler (Human error)** Ausfall aufgrund eines Bedienungsfehlers eines Mitarbeiters (z. B. falsche Befehlseingabe), ohne dass es dabei zu einem Sachschaden gekommen ist.		**ByteProtect:** Baustein A b)	
G	**Manipulation** Ausfall aufgrund einer absichtlichen Handlung eines Mitarbeiters.		**ByteProtect:** Baustein A e)	
H	**Ausfall externer IT-Ressourcen** Ausfall einer ausgelagerten IT-Dienstleistung (z. B. Cloud-Computing).		**ByteProtect:** Baustein A f)	IT-Dienstleister sind namentlich zu benennen. Hohes Kumulrisiko für den Versicherer. Kein Versicherungsschutz bei Insolvenz

Risiko-Check IT

2 Datenlöschung/Datenveränderung

Neben der Datenlöschung ist auch die Änderung von Daten und Programmen bzw. die Störung der Datenintegrität zu berücksichtigen. Mit dem Begriff „Daten“ werden im Folgenden Software und Daten zusammengefasst. Versichert sind jeweils die Kosten zur Wiederherstellung von Daten und Programmen auf eigenen und fremden IT-Systemen. Hierzu kann auch die Wiederherstellung der eigenen Webseite gehören.

Bei allen Versicherungsmöglichkeiten wird die regelmäßige Datensicherung vorausgesetzt. Folge des Datenverlustes kann eine Betriebsunterbrechung sein – siehe dazu Punkt 1!

	Ursache/Gefahr	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Sachschaden** Löschung oder Veränderung **eigener** Daten aufgrund eines Sachschadens am Datenspeicher.		Sachinhalts- bzw. Elektronikversicherung mit Daten- oder Softwareversicherung.	
B	**Hacker-Angriff** Löschung oder Veränderung **eigener** Daten aufgrund eines Cyber-/Hacker-Angriffs (z. B. auf eigene Webseite).		Vertrauensschadenversicherung bei vorsätzlicher Handlung eigener Mitarbeiter und von Dritten **ByteProtect:** Baustein C	Ohne vorausgehenden Sachschaden! Das Löschen von Daten wird dabei nicht als Sachschaden angesehen Ggf. Einschränkung auf zielgerichtete Angriffe oder Ausschluss für Schadsoftware beachten!
C	**Bedienungsfehler und Manipulation** Löschung oder Veränderung **eigener** Daten aufgrund eines Bedienungsfehlers oder einer Manipulation durch Mitarbeiter.		Elektronikversicherung mit Softwareversicherung Manipulation ist auch durch eine Vertrauensschadenversicherung versicherbar, sofern ein reiner Vermögensschaden entstanden ist.	
D	**Schadsoftware** Löschung oder Veränderung **eigener** Daten aufgrund Schadsoftware (Malware).		**ByteProtect**: Baustein C Zum Teil auch in der Softwareversicherung oder der Vertrauensschadenversicherung eingeschlossen (oft niedriges Sublimit).	
E	**Löschung oder Veränderung fremder Daten**		Haftpflichtversicherung, sofern eine gesetzliche Haftung vorliegt. Löschung wird rechtlich zum Teil als Sachschaden angesehen! **ByteProtect:** Baustein H	Auf Ausschlüsse in den Versicherungsbedingungen achten! Ggf. strafrechtliche Relevanz beachten!

Risiko-Check IT

3 Datenschutzverletzung

Bei Umgang mit personenbezogenen Daten können sich Verstöße gegen das Datenschutzgesetz ergeben, z. B. durch unbeabsichtigte Veröffentlichung von Kundendaten im Internet. Die Folge sind ggf. Kosten für Forensik und Information der betroffenen Personen sowie der Behörden.

	Ursache/Gefahr	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Unberechtigter Zugriff** Zugriff Dritter auf Daten, die auf der EDV des Unternehmens oder bei einem IT-Dienstleister gespeichert sind (z. B. durch einen Hacker-Angriff).		**ByteProtect:** Baustein E Rechtsschutzversicherung	Über ByteProtect sind über Baustein E Informations-, Beratungs- und Kreditüberwachungskosten versicherbar.
B	**Diebstahl von Datenträgern** Verlust von Datenträgern durch Einbruch bzw. Diebstahl.		**ByteProtect:** Baustein E Rechtsschutzversicherung	
C	**Sonstiger Verlust von Datenträgern** Verlust von Datenträgern aus sonstigen Gründen, z. B. Verlust eines Laptops mit sensiblen Daten.		**ByteProtect:** Baustein E Rechtsschutzversicherung	
D	**Ermittlungsverfahren** wegen des Vorwurfs eines strafrechtlich relevanten Verstoßes: ■ Z. B. gegen §§ 202a, 202b, 202c, 303a und 303b StGB (Hackerparagrafen)		Strafrechtsschutzversicherung **ByteProtect:** Baustein H (passive Strafrechtsschutzversicherung)	
E	**Haftpflichtansprüche** Aus den genannten Ereignissen/Schäden sich ergebende Haftpflichtansprüche Dritter.		Haftpflichtversicherung (auf Mitversicherung von Vermögensschäden achten!) **ByteProtect:** Baustein H	

Risiko-Check IT

4 Cyber-Betrug

Daten in Unternehmen können einen hohen Wert haben. Bei einem unberechtigten Zugriff auf entsprechende Daten 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.

Bei der Auswahl der Versicherung sollte darauf geachtet werden, dass auch Rechtsverfolgungskosten mitversichert sind.

	Ursache/Gefahr	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Manipulation der Webseite** (z. B. Webshops, Angebotstools etc.) zum Zwecke der Bereicherung		Vertrauensschadenversicherung **ByteProtect:** Baustein F	
B	**Manipulation des Online-Bankings** bzw. von Online-Zahlungssystemen/Anwendungs-programmen durch Dritte über das Internet		Vertrauensschadenversicherung, sofern unmittelbare Bereicherung erfolgte **ByteProtect:** Baustein F	
C	**Identitätsdiebstahl** Betrug mit Hilfe von Phishing oder Pharming bzw. Social Engineering (z. B. Fake President)		Vertrauensschadenversicherung, sofern unmittelbare Bereicherung erfolgte **ByteProtect:** Baustein F	
D	**Diebstahl und Unterschlagung durch eigene Mitarbeiter („Vertrauenspersonen“)**		Vertrauensschadenversicherung	EDV-Servicepersonal wird mitversichert, auch wenn dieses nur online tätig wird.
E	**Diebstahl fremder Daten auf eigenen Rechnern durch eigene Mitarbeiter**		Der unmittelbare Schaden des Dritten ist durch-Vertrauensschadenversicherung versicherbar. Haftpflichtversicherung (z. B. Internet-Zusatz-baustein) **ByteProtect:** Baustein H (Ansprüche Dritter)	**Entgangener Gewinn des Dritten ist in der Vertrauensschadenversicherung nicht versicher-bar, da dies keinen unmittelbaren Schaden darstellt!**

Risiko-Check IT

5 Cyber-Spionage

Daten und Informationen stellen für den wirtschaftlichen Erfolg von Unternehmen zunehmend einen entscheidenden Wettbewerbsvorteil dar. Entsprechend steigt das Interesse von Wettbewerbern, auf diese Daten auch über das Internet zuzugreifen.

	Schäden/Folgekosten	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Gewinnausfall aufgrund von Spionage** über das Internet (Wettbewerbsnachteile)		Nicht versicherbar, da Kausalität und Höhe des Schadens nicht oder nur sehr eingeschränkt nachweisbar ist.	
B	**Rechtsverfolgungskosten**		Rechtsschutzversicherung	
C	**Forensik/Sachverständigenkosten**		**ByteProtect:** Baustein B	Zeitliche Bestimmung des Versicherungsfalles zu beachten – bei ByteProtect ist dies die Schaden-feststellung!

Risiko-Check IT

6 Haftpflichtansprüche durch die Nutzung des Internets

Über manipulierte 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. Weitere Szenarien sind der Verlust von Daten Dritter oder die illegale Nutzung von Zugängen zu EDV-Systemen von Kunden oder Lieferanten etc.

	Schäden/Folgekosten	Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Schäden Dritter durch Schadsoftware** Kosten durch Datenverlust, Ausfall der IT, Sachschäden, Reinigungsaufwand		Haftpflichtversicherung (meist stark eingeschränkt auf Datenwiederherstellungskosten) **ByteProtect:** Baustein H (auch für weitere Folgekosten des Dritten!)	Auf Ausschlüsse in den Versicherungsbedingungen achten! Ggf. bestehen Regressmöglichkeiten, wenn die Quelle der Schadsoftware bestimmt werden kann.
B	**Schäden durch Verlust, Veränderung oder Nichtverfügbarkeit von Daten Dritter** Neben Datenschutzverletzungen kann es sich hierbei auch um sensible Betriebsgeheimnisse wie Rezepturen, Patente, Preislisten etc. handeln (Intellectual Property)		Vermögensschaden-Haftpflichtversicherung **ByteProtect:** Baustein H (Ansprüche Dritter)	
C	**Schäden durch Verletzung von Schutzrechten** Hierzu zählen insbesondere Urheberrechte, Namensrechte, Wettbewerbsrecht etc. – besonders bei der Gestaltung von Webseiten und der Nutzung von WLANs relevant		Haftpflichtversicherung (meist stark eingeschränkt auf bestimmte Rechtsverletzungen) **ByteProtect:** Baustein H (ausgeschlossen sind Schäden aufgrund Verletzung von Patent-, Lizenz- und Kartellrecht)	
D	**Schäden durch Ausnutzung von Zugängen des Unternehmens auf IT-Ressourcen Dritter durch Hacker** Z. B. Zugang zu Kunden-Portalen, Aufschaltungsmöglichkeiten auf fremde EDV-Systeme, Fern-Wartung		**ByteProtect:** Baustein H	

Risiko-Check IT

7 Reputationsschaden

Durch Veröffentlichung und Verbreitung von negativen Meldungen im Internet, z. B. in sozialen Medien, kann es leicht zu einer Rufschädigung mit entsprechenden Kunden- und Umsatzverlusten kommen. Auch Sicherheitsvorfälle, die ggf. nur Kunden des Unternehmens bekannt werden, können zu einem Verlust der Geschäftsbeziehung führen. Aufgrund des drohenden Gewinn- bzw. Umsatzausfalls kommt es daher auf ein rasches und professionelles Krisenmanagement mit entsprechender Kommunikation an.

Schadenart		Mögliche Schadenhöhe	Versicherungsmöglichkeit	Anmerkungen
A	**Kunden- und Umsatzverlust**		Aufgrund Unsicherheiten in der Bestimmung von Kausalität und Umfang des Schadens wird hier von Seiten AXA keine Versicherungsmöglichkeit angeboten.	
B	**Krisen- und Reputationsmanagement** Beratungs- und Kommunikationskosten zur Vermeidung einer Rufschädigung oder zur Wiederherstellung des guten Rufs.		**ByteProtect:** Baustein D	Versichert sind z. B. Kosten für Rechtsberatung, Kommunikationsberatung, Call-Center, Web-Bereinigung, Pressearbeit etc

Risiko-Check IT

ByteProtect – Übersicht der Bausteine

Baustein A	Ertragsausfall
a)	Ausfall Telekommunukation/Internet/Webseite
b)	Bedienungsfehler
c)	DoS-Attacke
d)	Hackerangriff
e)	Manipulation durch eigene Mitarbeiter
f)	Ausfall der IT-Dienstleistung
Baustein B	Sachverständigenkosten / Forensik
Baustein C	Wiederherstellung von Daten und Programmen
Baustein D	Rufschädigung und Krisenmanagement
Baustein E	Datenschutzverletzung
Baustein F	Internet-Betrug
Baustein G	Erpressung
Baustein H	Cyber-Haftpflicht

71007831 (3.16)