Risikoanalyse Cybersicherheit

Inhaltsverzeichnis

1 Einleitung

Die vorliegende Risikoanalyse **Cybersicherheit** soll dabei helfen, die Risiken, die mit der Verarbeitung von Informationen im Allgemeinen und der Verwendung von Informationstechnologie im Speziellen bestehen, transparent und bewertbar zu machen. Als Unterstützung finden Sie in der Vorlage ein geeignetes Beispiel.

Erst wenn Risiken bewertet sind, kann eine sinnvolle Risikostrategie gewählt, und – im Falle der Risikominderung –eine Investition in risikosenkende Maßnahmen beurteilt werden.

Die Cybersicherheitsrisiken treten immer in der eigenen Wertschöpfung auf, sie können nicht auf Dienstleister abgewälzt werden (Vertragsstrafen mindern den Schaden, können aber i.d.R. nicht alle Folgeeffekte auffangen). Eine Entscheidung für eine bestimmte Technologie / einen bestimmten Prozess / eine Kooperation mit einem Unternehmen ist daher immer auch vor dem Hintergrund der damit verbundenen Risiken zu treffen.

Die Risikoanalyse ist ein strukturierter Ansatz, mit dem Risiken im Zusammenhang mit dem Verlust, der Veränderung oder der Nicht-Verfügbarkeit von Informationen sowie von IT-Anwendungen und sonstigen Arbeitsmitteln und -prozessen bestehen. Durch die Risikoanalyse werden die Risiken hinsichtlich ihrer Kritikalität für das Unternehmen bewertet. Dies ermöglicht eine Priorisierung der notwendigen Maßnahmen im Sinne von Effizienz und Wirtschaftlichkeit.

2 Allgemeines

Diese Risikoanalyse sollte pro betrachtete Information durchgeführt werden. Fassen Sie Informationen durchaus zusammen (z. B. Daten über Personen bei Kunden), aber auch nicht zu grob (z. B. Kundendaten).

Betrachtete Informationen	
Verwendet in Geschäftsprozess(en)	
Datum der Analyse	

3 Schutzbedarf

Mögliche Werte sind: NORMAL / HOCH / SEHR HOCH. Personenbezogene Daten haben immer einen Vertraulichkeits-Schutzbedarf von „HOCH“; besondere personenbezogene Daten haben den Vertraulichkeits-Schutzbedarf „SEHR HOCH“ (z.B. Gesundheitsdaten).

Vertraulichkeit		**Verfügbarkeit**		**Integrität**	

4 Mögliche Angreifer

Bitte benennen Sie die wichtigsten **Angreifergruppen**, die Interesse an dem hier betrachteten Informationstyp haben:

Angreifergruppe	Motivation	Handlungsfähigkeit

Mögliche Werte für Motivation und Handlungsfähigkeit sind GERING / MITTEL / HOCH. Die Motivation ist in Bezug auf den hier betrachteten Informationstyp zu bewerten. Die Handlungsfähigkeit wird durch die technisch-/fachliche Kompetenz, die zur Verfügung stehenden

Mittel und den Zugang zur Information gekennzeichnet. Beides kann dazu herangezogen werden, eine Eintrittswahrscheinlichkeit für einen Angriff daraus abzuleiten (z.B. das Maximum der beiden Werte).

5 Mögliche Schäden

Bitte beschreiben Sie die kritischsten Schadensszenarien:

Schadenszenario	Schadensklasse (s. Anlage)

6 Risiken

Beschreiben Sie die entstehenden Risiken:

Nr	Risiko (Schadensszenario, ausgelöst durch…)	Motivation / Handlungs-fähigkeit der Angreifer	Schadens-klasse

7 Risiko-Entscheidung

Bitte dokumentieren Sie hier, wie mit den Risiken umgegangen werden kann. Risiken werden **übergeben**, wenn sie, z.B. gegen eine finanzielle Gegenleistung, von jemand anderem übernommen werden (etwa durch eine Versicherung) – Vorsicht: meist ist diese Risikoübernahme, gedeckelt, es

besteht dann also ein Rest-Risiko. Risiken werden **vermindert**, wenn eine Maßnahme ergriffen wird, um die Eintrittshäufigkeit und/oder den Schaden zu begrenzen. Risiken werden **vermieden**, wenn die Ursache für dieses Risiko nicht weiter existiert (z.B. eine Sammlung von Unternehmensdaten gar nicht erst angelegt wird) – in der Praxis ist das eher selten der Fall.

Nr	Risiko	Über-geben	Ver-mindern	Akzep-tieren	Ver-meiden

Bei „AKZEPTIEREN“ begründen Sie bitte Ihre Entscheidung, bei „ÜBERGEBEN“ beschreiben Sie kurz, wieso die Übergabe an Dritte das Risiko mindert, und welches Restrisiko besteht.

8 Maßnahmen zur Verminderung der Risiken

Bitte beschreiben Sie die wichtigsten Maßnahmen, die die Risiken mindern sollen.

Maßnahme	Wirkt auf Risiken Nr	Verant-wortlich	Kosten	Fertig (wann)

9 Restrisiken

Beschreiben Sie, welche Restrisiken bestehen, wenn Risiken übergeben bzw. Maßnahmen ergriffen wurden. Diese Risiken müssen der Geschäftsleitung bewusst sein, und durch eine Unterschrift bestätigt werden.

Nr	Risiko nach Maßnahmenumsetzung bzw. Übergabe	Eintritts-wahrschein-lichkeit	Schadensklasse

Datum: _____

_____ _____

Geschäftsleitung (Risikoübernahme) IT-Sicherheitsbeauftragter (fachliche Korrektheit)

Anhang

Beschreibung der Schadensklassen:

Schadens-klasse	Beschreibung / Kriterien
niedrig	Geringe Auswirkung auf die Ziele Firma. Kurzfristig negative Auswirkungen auf Geschäftspartner-Beziehungen. Keine nach außen wirksame Beeinträchtigungen des operativen Betriebs. Verstoß gegen interne Richtlinien oder Gesetze ohne personelle/finanzielle Konsequenzen.
mittel	Die Fähigkeit, ein Ziel der Firma zu erreichen, ist beeinträchtigt. Deutlich negative Auswirkungen auf Geschäftspartner-Beziehungen. Kurzfristige Beeinträchtigung des operativen Betriebs. Verstoß gegen interne Richtlinien oder Gesetze mit internen personellen Konsequenzen.
Hoch	Ein strategisches Ziel der Firma wird nicht mehr erreicht. Nachhaltig negative Auswirkungen auf Geschäftspartner-Beziehungen, Vertrauensverlust. Der operative Betrieb ist über mehrere Wochen nicht möglich, die Störungen wirken sich auch auf andere Firmen aus. Eine öffentliche Berichterstattung schädigt das Image der Firma als Ganzes. Verstoß gegen Gesetze mit erheblichen personellen und / oder finanziellen Konsequenzen.
Kritisch	Die Aufrechterhaltung der Firma ist nicht mehr möglich (aus politischen, finanziellen oder anderen Gründen). Die operativen Rückwirkungen betreffen viele, wenn nicht alle Partnerfirmen.