Landesamt für Sicherheit in der Informationstechnik

Infoblatt zum Umgang mit Risiken

Für Betreiber von kritischen Infrastrukturen

DOKUMENTINFORMATIONEN

Erstellt am:	26.07.2023	
Version	1.0	
Seitenanzahl	8	© 2023 Landesamt für Sicherheit in der Informationstechnik

INHALT

Vorwort

Im Umfeld einer Organisation existieren viele verschiedene Arten von Risiken. Durch das Voranschreiten der Digitalisierung sowie Veränderungen innerhalb des Unternehmens und in dessen Umfeld können bestehende Risiken wachsen oder neue hinzukommen. Daher ist es wichtig, sich mit den aktuellen und zukünftigen Gefährdungen auseinanderzusetzen, denn aus einer Gefährdung kann für die Organisation schnell ein ernstzunehmendes Risiko entstehen. Tritt ein Risiko ein, können wichtige Geschäftsprozesse beeinflusst, gehemmt oder sogar zum Erliegen gebracht werden.

In der Risikobetrachtung müssen daher die Prozesse der Organisation betrachtet, die möglichen Risiken identifiziert und deren Auswirkung analysiert werden. Anschließend werden geeignete Maßnahmen getroffen, um die Risiken zu vermeiden und deren Auswirkung zu verringern oder ausschließen zu können. Die Behandlung von Risiken ist keine einmalige Aufgabe, sondern ein Prozess, der in regelmäßigen zeitlichen Abständen oder bei größeren Veränderungen durchgeführt werden muss, denn die möglichen Gefährdungen verändern sich. Die Gefährdungslage und die daraus resultierenden Risiken müssen deshalb regelmäßig neu bewertet und der Maßnahmenplan aktualisiert werden. Welches Vorgehen oder welche Methode zur Behandlung von Risiken genutzt wird, können die Verantwortlichen selbst entscheiden. Wichtig dabei ist, dass Risiken erkannt und behandelt werden, um mögliche Schäden für die Organisation zu vermeiden.

In diesem „Infoblatt“ stellen wir Ihnen einen einfachen Ablauf vor, den Sie für die Identifikation, Analyse, Bewertung und Behandlung von Risiken nutzen können. Dieser sollte auf Ihre Organisation angepasst und bei Bedarf erweitert werden. Weiterführend können auch Methoden wie die Business Impact Analyse, FMEA (Fehlermöglichkeits- und Einflussanalyse) oder etablierte Standards wie ISO 31000 und dem Standard 200-3 (Risikomanagement) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) genutzt werden, um eine Risikobehandlung durchzuführen.

Hinweis für Betreiber kritischer Infrastrukturen:
„Dabei ist zu berücksichtigen, dass gegenüber allgemeinen Risikomanagementansätzen ein unbehandeltes Risiko durch eigenständige dauerhafte Risikoakzeptanz durch den Betreiber oder Versicherung gegen Risiken in der Regel keine zulässige Option im Sinne des BSIG ist.“
(BSI: Anforderungskatalog zur Konkretisierung der Kriterien des § 8a Absatz 1 BSIG)

Allgemeine Herangehensweise

Der Umgang mit Risiken bedeutet, sich proaktiv mit möglichen Gefährdungen und Vorfällen zu befassen und auseinanderzusetzen. Dies sollte ein Teil des Controlling-Prozesses sein und stetig wiederholt werden. Dieser Prozess kann in vier wesentliche Phasen unterteilt und durchlaufen werden. Zuerst müssen die Risiken identifiziert werden: Dabei ist es wichtig anhand möglichst realistischer Vorfallszenarien Bedrohungen zu erkennen, die daraus folgenden Risiken für das eigene Unternehmen abzuleiten und anschließend zu analysieren. Bei der Analyse werden besonders die Ursache und der mögliche Schaden für das Unternehmen betrachtet. Nach der Analyse folgt die Bewertung der Risiken. Ein Risiko wird grundlegend definiert durch den möglichen Schaden und dessen Eintrittswahrscheinlichkeit: Risiko = Schaden x Eintrittswahrscheinlichkeit. Bei der Bewertung werden genau diese beiden Kriterien beurteilt. Mit dieser Erkenntnis kann das weitere Vorgehen bei der Behandlung von Risiken entschieden werden. Durch eine wiederholte Anwendung dieses Prozesses können neue Risiken erkannt, bestehende Risiken überwacht und die Wirksamkeit von

Abbildung: Prozess Risikocontrolling

Gegenmaßnahmen beobachtet werden. Wenn ersichtlich wird, dass Gegenmaßnahmen nicht die erforderliche Wirkung entfalten, muss entsprechend nachgesteuert werden.

Risikoidentifikation

Bei der Risikoidentifikation geht es in erster Linie darum, potentielle, aber vor allem auch realistische, Vorfälle zu benennen, die Risiken für das Unternehmen bewirken. Hierfür muss eine geeignete Form gefunden werden, um mit dem richtigen Teilnehmerkreis diese Vorfälle zu besprechen und die daraus folgenden Risiken abzuleiten. Teilnehmer sollten neben den Beauftragten für die Risikoanalyse und den Geschäftsleitern auch die Verantwortlichen des jeweiligen Themengebiets sein. Die Erkenntnisse aus diesem Schritt werden in einer geeigneten Form dokumentiert, beispielsweise in der Tabelle zur Behandlung der Risiken. Diese finden Sie als Mustervorlage in der Anlage.

Risikoanalyse

In der Risikoanalyse werden die im vorherigen Schritt identifizierten Risiken gruppiert und zusammengeführt, Ursachen benannt und negative Auswirkungen für das Unternehmen sowie übergreifende Auswirkungen auf andere Themengebiete und Prozesse aufgeführt.
Risiken können mehrere Ursachen sowie Auswirkungen haben. Die Erkenntnisse aus diesem Schritt werden in einer geeigneten Form in die Dokumentation aufgenommen, beispielsweise in die Tabelle zur Behandlung der Risiken.

Risikobewertung

Die Bewertung des Risikos muss einem geregelten vordefinierten Ablauf folgen; die im Vorfeld durchlaufenen Schritte sind dabei essentiell, um Risiken zu benennen und zu analysieren. Für die Bewertung werden objektive Kriterien benötigt, die im Vorfeld individuell für das Unternehmen festgelegt und definiert werden müssen. Diese sollen dabei helfen, Risiken immer gleich zu bewerten, um unabhängig vom jeweiligen Bewerter ein konsistentes Ergebnis zu erzielen.

Risiko = Schaden x Eintrittswahrscheinlichkeit

Ein Risiko setzt sich aus zwei Faktoren zusammen: der Eintrittswahrscheinlichkeit und der Auswirkung bzw. dem Schaden bei Eintritt. Für die beiden Faktoren werden jeweils Kriterien ausgewählt und diese in verschiedene Stufen unterteilt. Zur Beurteilung dieser Kriterien können Erfahrungswerte aus dem Unternehmen oder der Branche herangezogen werden, beispielsweise können Störungs- bzw. Ausfallstatistiken von Systemen und deren Auswirkung hierfür verwendet werden. Das Unternehmen kann frei entscheiden, wie viele Stufen und Kriterien für die Unterteilung und Bewertung nötig sind. Ob die Benennung der einzelnen Stufen mit Buchstaben, Zahlen oder Wörtern, wie zum Beispiel „unwahrscheinlich“, „möglich“, „wahrscheinlich“, „sehr wahrscheinlich“ oder „niedrig“, „mittel“, „hoch“ erfolgt, ist unerheblich. Wichtig ist nur, dass diese Stufen mit Kriterien belegt und definiert sind und somit für eine objektive Beurteilung der Risiken genutzt werden können. Zusätzlich wird den Stufen jeweils ein aufsteigender Wert zugeordnet, beginnend mit dem günstigsten Fall (Wert = 1) zu dem ungünstigsten Fall (Wert = Anzahl der Stufen). Die Multiplikation dieser beiden Werte ergibt den Risikowert. Diese Zahl gibt Auskunft darüber, wie dringlich ein potentielles Risiko behandelt werden muss und kann in einer Risikomatrix visuell dargestellt werden. Es ist zu empfehlen, eine gleiche Anzahl von Stufen für die Eintrittswahrscheinlichkeit und Auswirkung zu nutzen, um eine gleichmäßige Risikomatrix zu erhalten. Die Anzahl der Stufen sollte für das Unternehmen angemessen sein: Je mehr Stufen definiert werden, desto schwieriger wird die Einordnung der Risiken.

Die **Eintrittswahrscheinlichkeit** eines Schadensereignisses beschreibt den Erwartungswert für das Eintreten dieses Schadensereignisses in der Zukunft.

Eintrittswahrscheinlichkeit		
Stufe (Wert)	**Beschreibung**	**Häufigkeit**
1	Alle fünf Jahre könnte ein Vorfall eintreten.	selten
2	Höchstens einmal im Jahr ein tritt ein Vorfall ein.	mittel
3	Höchstens einmal pro Monat tritt ein Vorfall ein.	häufig
4	Mehrmals im Monat tritt ein Vorfall ein.	sehr häufig

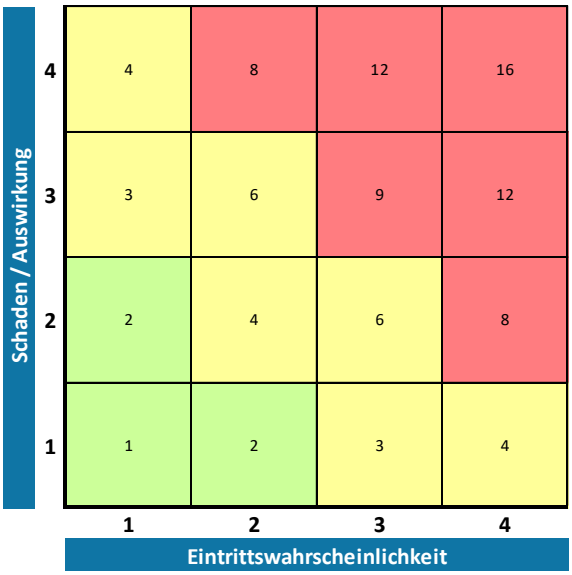
Tabelle: Bewertungskriterium Eintrittswahrscheinlichkeit

Auswirkung bzw. Schaden: Der Schaden, der entsteht, wenn die Bedrohung eintritt und sich auf das Unternehmen auswirkt.

Schaden und Auswirkung						
Stufe (Wert)	**Beschreibung**	**Personen**	**Umwelt**	**Ausfallzeit**	**Ver- / Entsorgung**	**Sachwerte**
1	gering und vernachlässigbare Schadens-auswirkung	keine	keine	< 4 Std	keine	< 10000€
2	begrenzte und überschaubare Scha-densauswirkung	leichte	leichte	< 2 Tage	leichte Störung	< 25000€
3	beträchtlich Schadensauswirkungen	mittlere	mittlere	< 5 Tage	mittlere Störung	< 50000€
4	existenzbedrohendes Schadensauswir-kungen	hoch	hoch	>= 5 Tage	Totalausfall	>=50000€

Tabelle: Bewertungskriterium „Schaden und Auswirkung“

Diese Kriterien sind für jede Risikobewertung gleich zu nutzen und zu dokumentieren. Die Erkenntnisse aus diesem Schritt werden in einer geeigneten Form in die Dokumentation aufgenommen, beispielsweise in die Tabelle zur Behandlung der Risiken.



Risikotoleranz auf Grundlage des Risikowerts
1 bis 2: Kein Handlungsbedarf (Beobachten)
3 bis 6: Beobachten und Maßnahmen definieren
ab 7: Maßnahmen definieren und anwenden, um Risiko zu verringern

Abbildung: Risikomatrix

Risikobehandlung

Bei der Behandlung von Risiken geht es darum, die Auswirkung des Risikos und den daraus entstehenden Schaden zu minimieren. Dabei sollten Maßnahmen getroffen werden, die die Einflussfaktoren eines Risikos, Eintrittswahrscheinlichkeit und Auswirkung bzw. Schaden, behandeln und verringern. Es gibt folgende Möglichkeiten der Risikobehandlung. Man kann Risiken:

- vermeiden, indem man den Eintritt des Risikos vermeidet, beispielsweise durch die Auswahl eines anderen Produktes, bei dem dieses Risiko nicht existiert.
- reduzieren, indem man Maßnahmen trifft, die den Schaden und/oder die Eintrittswahrscheinlichkeit verringern.
- verlagern, an Dienstleister auslagern oder durch Versicherungen absichern.
- akzeptieren, dabei muss das Risiko weiterhin beobachtet und gegebenenfalls neu behandelt werden. Dies kann eine Möglichkeit sein, wenn die Kosten für die Maßnahmen im Verhältnis zum Nutzen für das Unternehmen zu hoch sind.

Hinweis für Betreiber kritischer Infrastrukturen:
„Dabei ist zu berücksichtigen, dass gegenüber allgemeinen Risikomanagementansätzen ein unbehandeltes Risiko durch eigenständige dauerhafte Risikoakzeptanz durch den Betreiber oder Versicherung gegen Risiken in der Regel keine zulässige Option im Sinne des BSIG ist.“
(BSI: Anforderungskatalog zur Konkretisierung der Kriterien des § 8a Absatz 1 BSIG)

Grundsätzlich muss jedes Risiko behandelt werden. Abhängig von der Risikotoleranz muss das Unternehmen im Vorfeld Grenzen festlegen, bis wann ein Risiko akzeptiert werden kann und ab wann ein konkreter Handlungsbedarf besteht. Anhand der Risikowerte können beispielsweise drei Bereiche abgegrenzt werden, die verschiedene Anforderungen an die Behandlung der Risiken mit sich bringen (siehe Abbildung: Risikomatrix). Ist der Wert eines Risikos für das Unternehmen zu hoch, müssen geeignete Maßnahmen getroffen werden mit dem Ziel, das Risiko zu minimieren. Die Wirksamkeit der getroffenen Maßnahmen ist mittels einer Neubewertung des Risikos zu prüfen. Liegt dabei der Risikowert weiterhin in einem für das Unternehmen nicht akzeptablen Bereich, so müssen weitere Maßnahmen getroffen und dieser Teilprozess so oft wiederholt werden, bis das gewünschte Ergebnis erzielt wird.
Alle getroffenen Maßnahmen, die bei der Behandlung der Risiken erarbeitet und umgesetzt werden, sind in einem Maßnahmenplan zu dokumentieren, beispielsweise in der „Tabelle zur Behandlung der Risiken“.

Mustervorlage: „Tabelle zur Behandlung der Risiken“

Für den in diesem Dokument beschriebenen Prozess zum Umgang mit Risiken haben wir eine Mustervorlage erstellt. Diese soll Ihnen bei der Behandlung von Risiken helfen und als Grundlage für die Dokumentation der Erkenntnisse aus den einzelnen Phasen dienen. Dieses Musterdokument kann von Ihnen an die individuellen Gegebenheiten Ihrer Organisation angepasst und als Maßnahmenplan zur Behandlung von Risiken genutzt werden. Es ist nach den hier beschriebenen Phasen aufgebaut und zur Veranschaulichung mit folgenden Anwendungsbeispielen befüllt.

Anwendungsbeispiel 1: Unerlaubte Zugangsrechte nach personellen Veränderungen:
Das Risiko bei einem Personalwechsel in einer Abteilung mit speziellen Ressourcen besteht darin, dass bei einem Wechsel von Mitarbeitern Berechtigungen zur Nutzung dieser mitgenommen werden. Oftmals wird dabei auch das Zurücknehmen von Berechtigungen schlichtweg vergessen. Dadurch können Personen Ressourcen nutzen, für die sie keine Berechtigungen mehr haben sollten. Durch die Mitnahme von Berechtigungen oder Zugängen zu bestimmten Systemen von Fachabteilungen könnten unerlaubte Veränderungen durchgeführt werden. Für die „Eintrittswahrscheinlichkeit“ haben wir in diesem Beispiel die Stufe 2 von 4 gewählt, da bei fehlenden Vorgaben und Prozessen oftmals der Entzug der Berechtigungen übersehen wird. Für den Wert der „Auswirkung bei Eintritt“ haben wir ebenfalls die Stufe 2 von 4 gewählt. Beim Wechsel von Personen mit höheren Befugnissen ist dieser Wert für die „Auswirkung bei Eintritt“ gegebenenfalls höher zu wählen. Das Risiko „Unerlaubte Zugangsrechte nach personellen Veränderungen“ kann durch Erstellung und Umsetzung eines Personalwechselkonzepts reduziert werden, welches Vergabe und Entzug von erforderlichen Zugangs- und Zugriffsrechten bei Wechsel der Aufgabenbereiche bzw. Ausscheiden regelt.

Anwendungsbeispiel 2: Stromausfall oder Spannungsspitzen:
Durch Spannungsspitzen oder Ausfall der Energieversorgung können IT-Systeme beeinträchtigt werden oder komplett ausfallen, auch Schäden an IT-Geräten können hierbei entstehen. Für die „Eintrittswahrscheinlichkeit“ haben wir hier in diesem Beispiel die Stufe 2 von 4 gewählt, da das Stromnetz, an das die Liegenschaft angebunden ist, jederzeit durch externe Einflüsse gestört werden kann. Für den Wert der „Auswirkung bei Eintritt“ haben wir die höchstmögliche Stufe 4 von 4 gewählt, da IT-Systeme ohne Stromanbindung nicht funktionieren und möglicherweise Schaden nehmen können. Beschädigungen von Datenträgern sind dabei nicht auszuschließen. Dieses Risiko kann durch den Einsatz einer USV-Anlage oder Netzersatzanlage reduziert werden. Ein Datensicherungskonzept verringert das Risiko eines Datenverlustes bei defekten Festplatten.

Begriffserklärung

Gefährdung
… bedeutet die Möglichkeit, dass ein Schutzobjekt räumlich wie auch zeitlich mit einer Gefahrenquelle zusammentreffen kann. Dies lässt die dahinterstehende Gefahr wirksam werden und führt zu einem Schaden.

Bedrohung
… ist ein Ereignis, durch das ein Schaden entstehen kann.
In der Informationstechnik bezieht sich der Schaden auf die Beeinträchtigung der Schutzziele (Verfügbarkeit, Integrität und Vertraulichkeit).

Risiko
… ist die Prognose des Eintritts künftiger Ereignisse, Schaden im negativen Fall (Gefahr), oder im positiven Fall eines möglichen Nutzens (Chance).
Risiken stellen mögliche Abweichungen von geplanten Zielen dar und werden allgemein als Kombination aus Eintrittswahrscheinlichkeit und den Schaden bei einem Eintritt des Ereignisses angesehen. Kurzgesagt: Risiko = Schaden x Eintrittswahrscheinlichkeit

Vorfall
… ist ein Ereignis oder Geschehen, das plötzlich eintritt und sich für die Beteiligten meist unangenehm auswirkt.

Gefahr
… ist die Möglichkeit eines drohenden Schadens, der eintreten kann.