Muster: Richtlinie zur Risikoanalyse

Version: 0.1
Status: Entwurf

Dokumenteninformationen

Muster: Richtlinie zur Risikoanalyse

###NAME DER ANWENDENDEN ORGANISATION###

Version	0.1
Status	Entwurf
Datum der letzten Änderung	
Verantwortung	
Klassifizierung	S2 intern
Gültigkeitszeit	unbegrenzt
Überarbeitungsintervall	jährlich
Nächste Überarbeitung	
Dateiname	A.0.2 Richtlinie zur Risikoanalyse v[Version].[Dateiendung]
Ablageort	

Änderungsübersicht

Lfd. Nr.	Datum	Version	Änderungen	Durchgeführt von
1		0.1	Neuanlage des Dokuments	
2				
3				
4				
5				
6				
7				

Inhalt

1 Veranlassung 4

2 Methodik 4

3 Gefährdungsübersicht 4

4 Risikoeinstufung 5

4.1 Definition der Auswirkungen (Schadenshöhe) 5
4.2 Definition der Eintrittshäufigkeit 5
4.3 Definition der Risikokategorien 5
4.4 Risikoeinschätzung / - Bewertung 6

5 Risikobehandlung 6

5.1 Vermeidung 6
5.2 Reduktion 6
5.3 Transfer 6
5.4 Akzeptanz 7

6 Revision und Fortschreibung 7

7 Inkrafttreten 7

1 Veranlassung

Den Anforderungen zur Erfüllung des Schutzbedarfes Normal wird in der Regel durch die Umsetzung der Standard-Maßnahmen des BSI-Grundschutzes entsprochen. Eine individuelle Bedrohungs-und Schwachstellenanalyse ist hier entbehrlich.

In bestimmten Fällen muss jedoch explizit eine Risikoanalyse durchgeführt werden, beispielsweise wenn der betrachtete Informationsverbund Zielobjekte enthält, die

- einen hohen oder sehr hohen Schutzbedarf in mindestens einem der drei Grundwerte Vertraulichkeit, Integrität oder Verfügbarkeit haben oder
- mit den existierenden Bausteinen des IT-Grundschutzes nicht hinreichend abgebildet (modelliert) werden können oder
- in Einsatzszenarien (Umgebung, Anwendung) betrieben werden, die im Rahmen des IT-Grundschutzes nicht vorgesehen sind.

Risikoanalysen werden initial und bei wesentlichen Änderungen im Informationsverbund und bei einer sich abzeichnenden grundlegenden Änderung der Gefährdungslage durchgeführt.

Daraus resultierende Maßnahmen werden im erforderlichen Zeitraum umgesetzt und im Informationssicherheitskonzept dokumentiert (Realisierungsplan).

Eine turnusmäßige vollständige Aktualisierung der Risikoanalysen erfolgt nicht.

Risikoanalysen werden zeitlich nach der Umsetzung der IT-Grundschutz-Anforderungen durchgeführt.

2 Methodik

Die in der ###NAME DER ORGANISATION### zur Anwendung kommende Risikoanalyse sieht folgende Schritte vor, die dem BSI-Standard 200-3 entsprechen:

- Erstellung einer Gefährdungsübersicht
  - Zusammenstellung einer Liste von möglichen elementaren Gefährdungen
  - Ermittlung zusätzlicher Gefährdungen, die über die elementaren Gefährdungen hinausgehen und sich aus dem spezifischen Einsatzszenario ergeben
- Risikoeinstufung
  - Risikoeinschätzung (Ermittlung von Eintrittshäufigkeit und Schadenshöhe)
  - Risikobewertung (Ermittlung der Risikokategorie)
- Risikobehandlung
  - Risikovermeidung
  - Risikoreduktion (Ermittlung von Sicherheitsmaßnahmen)
  - Risikotransfer
  - Risikoakzeptanz
- Konsolidierung des Sicherheitskonzepts
  - Integration der aufgrund der Risikoanalyse identifizierten zusätzlichen Maßnahmen in das Sicherheitskonzept

3 Gefährdungsübersicht

Die jeweiligen Experten eines Zielobjektes (z.B. Fach- / IT-Verantwortliche, Anwendungsbetreuer, BfIS) erstellen je Zielobjekt eine Liste der Gefährdungen. Dazu bewerten sie in einem vom BfIS moderierten Workshop die Liste aller elementaren Gefährdungen. Falls es

im BSI-Grundschutz einen passenden Baustein gibt, werden die dort nicht aufgezählten Gefährdungen bewertet.

Die Beteiligten ermitteln über die elementaren Gefährdungen hinausgehende zusätzliche Gefährdungen.

4 Risikoeinstufung

Für jedes ermittelte Zielobjekt ist das sich aus den Gefährdungen ergebende Risiko zu ermitteln.

4.1 Definition der Auswirkungen (Schadenshöhe)

Die möglichen Auswirkungen einer Gefährdung werden wie folgt definiert:

- vernachlässigbar
  Die Schadensauswirkungen sind gering und können vernachlässigt werden.
- begrenzt
  Die Schadensauswirkungen sind begrenzt und überschaubar.
- beträchtlich
  Die Schadensauswirkungen können beträchtlich sein.
- existenzbedrohend
  Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

4.2 Definition der Eintrittshäufigkeit

Die mögliche Eintrittshäufigkeit einer Gefährdung wird wie folgt definiert:

- selten
  Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
- mittel
  Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
- häufig
  Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
- sehr häufig
  Ereignis tritt mehrmals im Monat ein.

4.3 Definition der Risikokategorien

- gering
  Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten einen ausreichenden Schutz.
- mittel
  Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
- hoch
  Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.

- sehr hoch
  Die bereits umgesetzten oder zumindest im Sicherheitskonzept vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung.

4.4 Risikoeinschätzung / - Bewertung

Die jeweiligen Experten eines Zielobjektes (z.B. Fach- / IT-Verantwortliche, Anwendungsbetreuer, BfIS) ermitteln je Gefährdung die Eintrittshäufigkeit und Schadenshöhe.

Die entsprechende Risikokategorie ergibt sich aus folgender Matrix.

Auswirkung	existenzbedrohend	mittel	hoch	sehr hoch	sehr hoch
	beträchtlich	mittel	mittel	hoch	sehr hoch
	begrenzt	gering	mittel	mittel	hoch
	vernachlässigbar	gering	gering	mittel	mittel
		selten	mittel	häufig	sehr häufig
	Eintrittshäufigkeit				

5 Risikobehandlung

Zur Behandlung von Risiken bestehen folgende Möglichkeiten.

5.1 Vermeidung

Das Risiko wird vermieden, indem beispielsweise die Risikoursache durch die Umgestaltung eines Geschäftsprozesses ausgeschlossen wird.

5.2 Reduktion

Das Risiko wird reduziert, indem die Rahmenbedingungen, die zur Risikoeinstufung beigetragen haben, modifiziert werden. In Frage kommt z.B. die Erarbeitung und Umsetzung von ergänzenden Sicherheitsmaßnahmen, die der Gefährdung entgegenwirken.

5.3 Transfer

Das Risiko wird transferiert, indem die Risiken mit anderen Parteien geteilt werden. Dazu können Versicherungen abgeschlossen werden oder Dienstleistungen ausgelagert werden.

5.4 Akzeptanz

Hohe und sehr hohe Risiken werden nicht akzeptiert. Sie sind durch eine entsprechende Behandlung auf ein akzeptiertes Maß zu reduzieren.

Bei mittleren Risiken wird eine Behandlung mit begrenzten Ressourcen durchgeführt. Verbleibende Restrisiken werden akzeptiert, müssen jedoch beobachtet und bei Änderungen neu bewertet werden. Behandelnde Maßnahmen werden vorbereitet.

Geringe Risiken werden ohne Behandlung akzeptiert.

Folgende Ergebnisse der Risikoanalyse werden vom BfIS der Leitung der ###NAME DER ORGANISATION### vorgelegt:

- Der Realisierungsplan (Risikobehandlungsplan), auf Grundlage dessen die Leitung die Maßnahmen zur Behandlung der Risiken initiiert.
- Eine Aufstellung der verbleibenden Restrisiken, deren Akzeptanz durch die Leitung mittels Unterschrift bestätigt wird.

6 Revision und Fortschreibung

Durch eine regelmäßige Revision der Regelungen zur Informationssicherheit und deren Anwendung wird die Informationssicherheit der ###NAME DER ORGANISATION### kontinuierlich sich ändernden Bedingungen angepasst und verbessert.

Diese Richtlinie ist mindestens jährlich auf Aktualität zu prüfen und gegebenenfalls anzupassen. Dafür ist der Beauftragte für Informationssicherheit - in Zusammenarbeit mit dem IS – Sicherheitsteam - zuständig.

7 Inkrafttreten

Diese Richtlinie zur Risikoanalyse der ###NAME DER ORGANISATION### tritt mit Unterzeichnung in Kraft und setzt vorhergehende Versionen außer Kraft.

###ORT###, den ###DATUM###

###NAME LEITUNG DER ORGANISATION###

###FUNKTION###