Datum: 20. Nov. 2023
Version: 1.0

Leitfaden zur IT-Risikoanalyse

im kritischen Sektor Behörden – insbesondere für die Teilbereiche Justiz, Verwaltung und Schulen

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung BWL

Nach Richtlinien vom Bundesamt für wirtschaftliche Landesversorgung – IKT Minimalstandard

Netsafe AG
Heiligkreuzstrasse 2
9008 St. Gallen

1. Einleitung

1.1. Vorwort

Angesichts der zunehmenden Komplexität und Abhängigkeit unserer Gesellschaft von der Informationstechnologie ist es von entscheidender Bedeutung, dass die kritische Infrastruktur im Sektor Behörden eine proaktive Herangehensweise an das IT-Risikomanagement und die Risikoanalyse verfolgen. Dies wird nicht zuletzt durch die jüngste Aktualisierung der nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI) am 16. Juni 2023 durch den Bundesrat der Schweiz unterstrichen. In dieser strategischen Neuausrichtung sind acht entscheidende Massnahmen festgelegt worden, die darauf abzielen, die Versorgungssicherheit in der Schweiz zu gewährleisten und in wesentlichen Sektoren zu verbessern. Ein zentraler Bestandteil dieser Massnahmen besteht darin, die Aufsichts- und Regulierungsbehörden, die für die kritischen Infrastrukturen verantwortlich sind, dazu zu verpflichten, erhebliche Risiken für schwerwiegende Versorgungsstörungen zu identifizieren und geeignete Massnahmen zur Risikoreduzierung zu ergreifen.

Der Hauptzweck dieses Dokuments besteht darin, eine risikoorientierte und bedarfsorientierte Vorsorge- und Abwehrplanung im Bereich der IT-Sicherheit zu ermöglichen. Es soll öffentlichen Verwaltungen und Behörden als IT-Risikoleitfaden dienen und die nationale Strategie zum Schutz kritischer Infrastrukturen unterstützen.

1.2. Positionierung des Dokumentes

Der Leitfaden zur IT-Risikoanalyse positioniert sich als ein unverzichtbares Instrument, das sich auf verschiedene Aspekte konzentriert, um einen ganzheitlichen Ansatz zur Risikobewältigung in der IT-Umgebung zu bieten. Er legt besonderen Wert auf die Einhaltung seiner Vorgaben, um die Integrität und Zuverlässigkeit der Prozesse sowie eine nachhaltige Wertschöpfung sicherzustellen. Das Risikomanagement ist eine kontinuierliche Aufgabe, die eine sorgfältige Dokumentation aller Schritte der Risikoanalyse erfordert, um die Nachvollziehbarkeit der Ergebnisse und eine konstante Verbesserung zu gewährleisten. Besonders in Situationen, in denen statistische oder wissenschaftliche Erkenntnisse fehlen, ist es notwendig, auf fundierte Annahmen und Schätzungen zurückzugreifen. Die Einbindung von Fachleuten mit fundiertem Wissen und Erfahrung ist entscheidend, um die Aussagen und Empfehlungen des Leitfadens auf ein höchstmögliches Mass an Belastbarkeit zu stützen. Insgesamt bildet dieser Leitfaden eine zentrale Grundlage für eine effektive und verantwortungsvolle Bewältigung von IT-Risiken.

Inhaltsverzeichnis

2. Risikomanagement

2.1. Einleitung Risikomanagement

Risikomanagement ist ein zyklischer Vorgang, um bestehende Risiken zu minimieren. Nachdem Risiken identifiziert wurden, erfolgt ihre Analyse und Bewertung sowie deren entsprechende Behandlung. Nach der Umsetzung der Massnahmen wird geprüft, ob das gewollte Ziel erreicht wurde. Ausserdem verändern sich bedeutende Faktoren wie politische Vorgaben, Gefahren und Anfälligkeiten mit der Zeit. Deshalb sind gewonnene Erkenntnisse, verwendete Daten sowie Rahmenbedingungen regelmässig zu prüfen und anzupassen.

Die Risikoanalyse ist ein Kernelement des Risikomanagements und untersucht Schutzgüter, Gefahren und mögliche Schäden, um Entscheidungen zu treffen und Vorsorgepläne zu erstellen. Sie ermittelt Eintrittswahrscheinlichkeit und Schadensausmass bei verschiedenen Gefahrenslagen und kann so bei der Gegenüberstellung der Ergebnisse aus der Analyse und den definierten Schutzzielen feststellen, ob die öffentlichen Verwaltungen in der Schweiz für die erwarteten Schadensszenarien ausreichend vorbereitet sind. Falls Handlungsbedarf besteht, liefert die Risikoanalyse wichtige Hinweise, wo dieser Bedarf liegt.

Der vorliegende Leitfaden orientiert sich bei der Methodik an den internationalen Standards des Risikomanagements und der Risikoanalyse (ISO 31000:2018[5], IEC 31010:2019[6]). Gemäss diesen Standards wird die vergleichende Gegenüberstellung verschiedener Risiken in einer fünfstufigen Risikomatrix abgebildet. Die effektive Durchführung einer umfassenden Risikoanalyse gemäss dieser Methode, erfordert die Konsolidierung einer breiten Palette von Informationen und sollte vorzugsweise auf vorhandenen Daten sowie unter Berücksichtigung interdisziplinärer Erkenntnisse basieren.
Dieser Leitfaden entspricht den gängigen Standards und Normen und wurde unter Einbeziehung bewährter Branchenstandards entwickelt. Dadurch wird sichergestellt, dass die im Bericht präsentierten Informationen und Empfehlungen den etablierten Best Practices und Normen entsprechen.

Berücksichtigte Standards:

- IKT-Minimalstandard vom Bundesamt für Wirtschaft und Landesversorgung (Stand April 2023)[1]
- National Institute of Standards and Technology Framework (NIST)[2]
- BSI-Standard 200-3: Risikomanagement[3]
- Factsheet zum kritischen Teilsektor Parlament, Regierung, Justiz, Verwaltung (Stand Februar 2023)[4]

[1] *IKT-Minimalstandard*. (2023). Bundesamt für wirtschaftliche Landesversorgung BWL. https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html
[2] *NIST Cybersecurity Framework 2.0.* (2023). National Institute of Standards and Technology NIST. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd
[3] *BSI-Standard 200-3*. (2017). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.html?nn=128620
[4] *Factsheet zum kritischen Teilsektor Parlament, Regierung, Justiz, Verwaltung*. (2023). Bundesamt für Bevölkerungsschutz BABS. https://www.babs.admin.ch/de/aufgabenbabs/ski/kritisch.html

- Norm im Risikomanagement (ISO 31000:2018)[5]
- Norm der Risikoanalyse (IEC 31010:2019)[6]
- Norm im Qualitätsmanagement (ISO 9001:2015)[7]

Diese Liste zeigt die angewandten Standards, die bei der Erstellung dieses Dokuments berücksichtigt wurden, und dient als Referenz für die zugrunde liegenden Richtlinien und Verfahren im Zusammenhang mit der IT-Sicherheit dem Risikomanagement.

2.2. Ziele

Das Hauptziel dieses IT-Leitfadens besteht darin, eine risikobasierte Planungsgrundlage bereitzustellen, die Organisationen bei der Vorbereitung auf Katastrophen und Notlagen unterstützt. Dabei liegt der Schwerpunkt auf der Schaffung einer klaren und vergleichbaren Übersicht über die Risiken.
Die Anwendung dieses IT-Leitfadens richtet sich ausschliesslich an die Informationssicherheit und die Schutzziele “Vertraulichkeit”, “Integrität” und “Verfügbarkeit”.

Der Leitfaden zur IT-Risikoanalyse richtet sich primär an Behörden, insbesondere an Justiz, Verwaltungen und Schulen, darüber hinaus auch an andere öffentliche Einrichtungen. Es gilt zu beachten, dass das Bearbeitungsdokument 2.0 eine Ergänzung zum vorliegenden Leitfaden ist und zur praktischen Durchführung der Risikoanalyse anleitet.

Mit diesem Leitfaden werden Identifikation, Planung und Konzeption im Krisenfall besser aufeinander abgestimmt.

[5] *ISO 31000:2018 Risk management — Guidelines*. (2018). International Organization for Standardization ISO. https://www.iso.org/standard/65694.html
[6] *IEC 31010:2019 Risk management — Risk assessment techniques*. (2019). International Organization for Standardization ISO. https://www.iso.org/standard/72140.html
[7] *ISO 9001:2015 Quality management systems — Requirements*. (2015). International Organization for Standardization ISO. https://www.iso.org/standard/62085.html

3. Vorarbeiten zur Risikoanalyse

3.1. Geltungsbereich

Es ist notwendig, einen Umfang (Scope) festzulegen, der alle schutzbedürftigen Elemente einschliesst. Dieser Umfang kann die Informationssicherheit einer gesamten Organisation abdecken, sich auf Teilbereiche erstrecken oder sich auf einzelne Systeme oder Projekte beschränken. Es ist wichtig sicherzustellen, dass keine wesentlichen Bereiche ausgelassen oder übersehen werden, und dass die Voraussetzungen der Institution ergründet und beachtet werden. Hierfür wird eine Übersicht des definierten Umfangs erstellt und relevante Angaben dazu erläutert.
Innerhalb dieses festgelegten Umfangs werden die spezifischen schutzbedürftigen Elemente oder Ziele identifiziert und später in Bezug auf Bedrohungen, Risiken und Schutzmassnahmen analysiert. Es ist ratsam, im Voraus zu überlegen, mit welcher Detaillierungsstufe die Risiken effektiv verwaltet werden sollen, um eine angemessene Anzahl von schutzbedürftigen Elementen festzulegen.

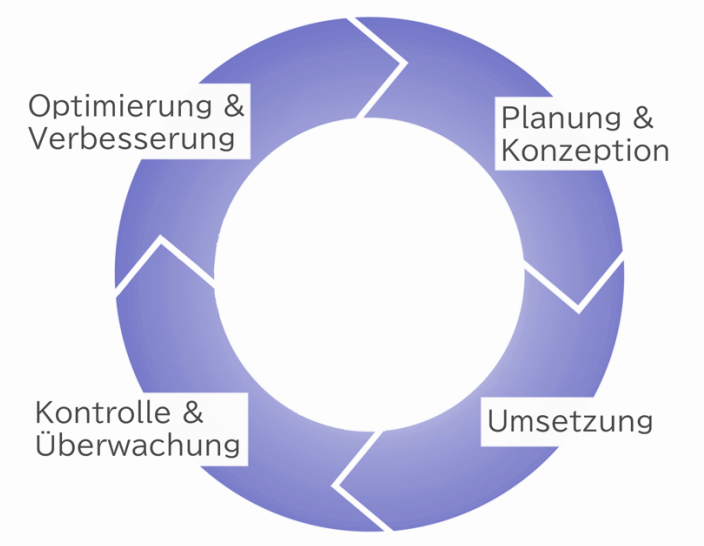

Abbildung 1: Risikomanagement-Zyklus

3.2. Strukturanalyse

Zunächst müssen wichtige Systeme und deren Eigenschaften für die unverzichtbaren Prozesse identifiziert werden. Dazu sind relevante Schadensszenarien zu ermitteln, die die Fortführung der IT-Systeme beeinträchtigen könnten, und deren Schadensausmass zu bewerten. Die erfassten Systeme können entscheidend für benötigte Informationen, Anwendungen und IT-Infrastruktur sein, ohne die die Geschäftsprozesse der Organisation nicht aufrechterhalten werden können. Durch diese strukturierte Betrachtungsweise können Organisationen ein besseres Verständnis für die Interaktionen und Wechselwirkungen innerhalb ihrer IT-Umgebung entwickeln.

Im vorliegenden Leitfaden wird die Strukturanalyse ausschliesslich für einen Teilbereich der Prozesse durchgeführt, die für den Betrieb der IT-Infrastruktur massgebend sind. Innerhalb des Geltungsbereiches werden die Prozesse als schützenswerte Ziele bestimmt und dann einer Schutzbedarfsanalyse unterzogen.

Die detaillierte Methode zur Vorgehensweise bei der Strukturanalyse ist im Bearbeitungsdokument 2.0 beschrieben.

3.3. Feststellung des Schutzbedarfs

Durch die Schutzbedarfsanalyse wird ermittelt, welches Schutzniveau für die Geschäftsprozesse, die verarbeiteten Informationen und die eingesetzte Informationstechnik erforderlich ist. Die während der Strukturanalyse erfassten Informationen, Anwendungen, IT-Systeme, Räumlichkeiten und Kommunikationsnetze werden nun hinsichtlich ihres Schutzbedarfs in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit bewertet. Diese Bewertung erfolgt anhand typischer Schadenszenarien.

Zuerst wird der Schutzbedarf für die Geschäftsprozesse und die zugehörigen Anwendungen ermittelt. Auf dieser Grundlage wird dann der Schutzbedarf für einzelne IT-Systeme, Räumlichkeiten und Kommunikationsverbindungen abgeleitet. Da die Massnahmen zur Sicherung der Vertraulichkeit von Informationen teilweise von denen zur Sicherung der Verfügbarkeit oder Integrität abweichen können, erfolgen die Bewertungen und Ableitungen getrennt für die verschiedenen Grundwerte.

IT-Schutzziele	Definition
Verfügbarkeit	Die zu schützenden Systeme und Daten sind auf Verlangen einer berechtigten Einheit zugänglich und nutzbar.
Integrität	Die verarbeiteten Daten sind richtig und vollständig und die Systeme funktionieren korrekt.
Vertraulichkeit	Schutz der Systeme und Daten vor unberechtigtem Zugriff durch Personen oder Prozesse.

Tabelle 1: IT-Schutzziele

3.4. Ermittlung des IST-Zustandes

Im Kontext der Vorarbeiten zur Risikoanalyse drängt sich unweigerlich die Empfehlung auf, den Minimalstandard für Informations- und Kommunikationstechnologie (IKT) zu berücksichtigen. Der IKT-Minimalstandard ist ein im Rahmen der Nationalen Cyber Strategie (NCS) und vom Bundesamt für wirtschaftliche Landesversorgung entwickelter Cybersecurity-Standard für die Schweiz. Organisationen, die sich an die Vorgaben des Standards halten, weisen ein beachtliches Maturitätsniveau in Bezug auf die Informationssicherheit auf.
Die Umsetzung des IKT-Minimalstandards wird insbesondere Betreibern kritischer Infrastrukturen dringend empfohlen. Dieses Dokument stellt jedoch allen interessierten Unternehmen und Organisationen eine Unterstützung sowie konkrete Anweisungen zur Verfügung, um die eigene IKT-Resilienz zu stärken.

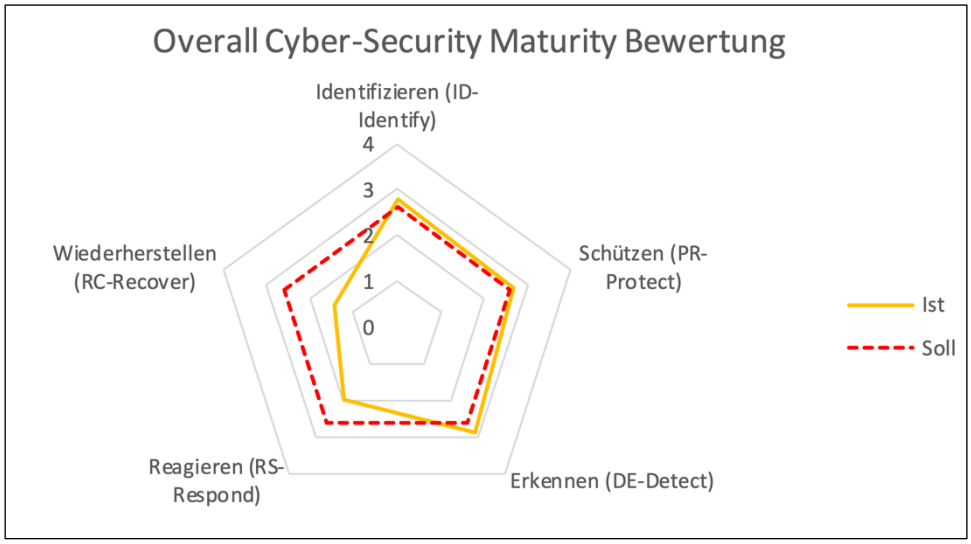

Abbildung 2: Beispiel einer Maturitätsniveau-Bewertung in der Übersicht mittels IKT-Minimalstandard (Bundesamt für wirtschaftliche Landesversorgung BWL, 2023)[1]

Mehr Informationen zum IKT-Minimalstandard sowie die aktuelle Version zum Download stehen auf der Webseite des Bundesamtes für wirtschaftliche Landesversorgung zur Verfügung.

3.5. Prozesse

Eine analytische Betrachtung des Geschäftsprozesses verdeutlicht eine Abfolge von notwendigen Arbeitsvorgängen, die zur Erbringung einer konkreten Leistung einer Organisation erforderlich sind.

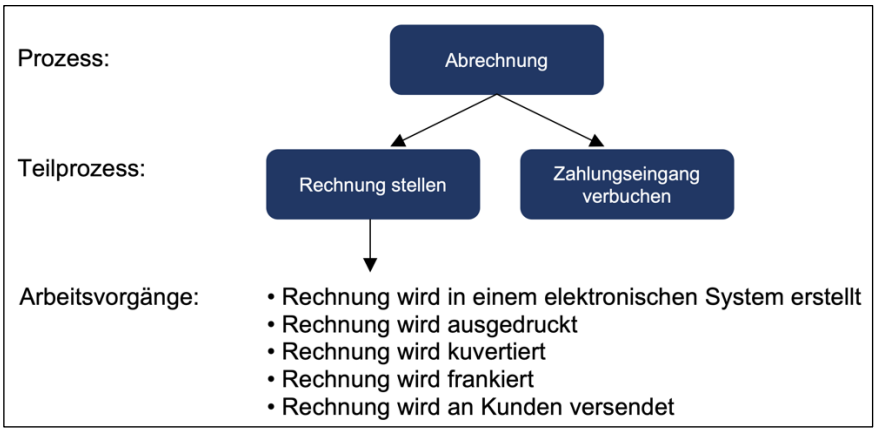

Abbildung 3: Beispiel Arbeitsvorgänge von Prozessen

3.6. Schutzbedarfsanalyse Teilprozesse

Im Folgenden wird auf die Schutzbedarfsanalyse der relevantesten Prozesse und einzelnen Typen von Informationen bzw. Daten eingegangen und die Anwendung eines Schutzbedarfs auf den zu schützenden Prozess definiert.