Effektiver Schutz kritischer Infrastrukturen: Ein Praxisleitfaden

DAS BSI GRUNDSCHUTZ PRAXISBUCH

MAIK JESCHKE

Impressum

Titel: Das BSI-Grundschutz Praxisbuch

Autor: Maik Jeschke

Erstveröffentlichung: 1. Juli 2023

ISBN: 9783757823511

VORWORT

In einer zunehmend digitalisierten Welt spielt die Sicherheit unserer Informations- und Kommunikationstechnologie eine immer wichtigere Rolle.
Ob es sich um eine kleine Organisation, ein mittelständisches Unternehmen oder einen global agierenden Konzern handelt – die Sicherheit ihrer digitalen Infrastruktur und Daten ist von entscheidender Bedeutung. Cyberbedrohungen, Datenlecks und Systemausfälle können nicht nur finanzielle Verluste verursachen, sondern auch den guten Ruf eines Unternehmens nachhaltig schädigen.
Hier setzt der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) an. Seit seiner Einführung vor mehr als zwanzig Jahren hat sich der IT-Grundschutz als eine umfassende und pragmatische Methodik zur Identifizierung und Minimierung von Risiken in der IT-Sicherheit etabliert.
Die umfangreichen Kataloge des IT-Grundschutzes bieten eine fundierte und erprobte Grundlage zur Umsetzung effektiver Sicherheitsmaßnahmen in allen Bereichen der Informationsverarbeitung.
Mit dem IT-Grundschutz bietet das BSI einen systematischen Ansatz, der sowohl technische als auch organisatorische Aspekte der Informationssicherheit berücksichtigt. Dabei stehen vor allem die Praxisnähe und die Adaptierbarkeit für verschiedenste Unternehmensgrößen und Branchen im Fokus.
Dieses Handbuch soll Ihnen dabei helfen, die Methoden und Maßnahmen des IT-Grundschutzes besser zu verstehen und erfolgreich in Ihrem eigenen Umfeld anzuwenden.
Dabei ist es egal, ob Sie bereits erste Erfahrungen in der IT-Sicherheit gesammelt haben oder ob Sie sich als Neuling auf diesem Gebiet befinden – die vorgestellten Konzepte und Prozesse sind so gestaltet, dass sie sowohl von Experten als auch von Einsteigern verstanden und umgesetzt werden können.
In einer Welt, in der die Digitalisierung voranschreitet und die Cyber-Bedrohungen zunehmen, bietet der IT-Grundschutz des BSI ein zuverlässiges Werkzeug, um unsere wertvollen digitalen Ressourcen zu schützen. Es liegt an uns, diesen Werkzeugkasten effektiv zu nutzen und so einen Beitrag zur Sicherheit unserer Informationsgesellschaft zu leisten.

Ihr *Maik Jeschke*

Grundlagen

Informationssicherheit

Die Sicherheit unserer Informationen und Daten ist von zentraler Bedeutung in unserer digitalisierten Welt. Es geht darum, sie vor allen Arten von Bedrohungen zu schützen, um ihre Vertraulichkeit, Integrität und Verfügbarkeit zu gewährleisten. Das BSI Grundschutzkompendium [^1] bietet hierfür wertvolle Leitlinien und Empfehlungen. Besonders im Kontext von KRITIS, den kritischen Infrastrukturen, ist Informationssicherheit von großer Bedeutung. Denn ein Sicherheitsvorfall in diesen Bereichen kann weitreichende Folgen für die Gesellschaft und das Funktionieren des Staates haben. Daher ist es unerlässlich, geeignete Sicherheitsmaßnahmen zu implementieren und ständig zu überprüfen, um ein hohes Sicherheitsniveau zu gewährleisten.

Sonderstellung BSI-KritisV

Die KRITIS-Verordnung ist ein Teil des deutschen IT-Sicherheitsgesetzes und definiert spezifische Anforderungen an die IT-Sicherheit von Organisationen und Unternehmen, die essenzielle Dienstleistungen erbringen und daher als kritisch für das Funktionieren der Gesellschaft angesehen werden. Die KRITIS-Verordnung betrifft zehn Sektoren: Energie, Wasser, Ernährung, IT und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr, Staat und Verwaltung, Medien und Kultur sowie die städtische Abfallentsorgung.

Als IT-Dienstleister gehören Sie zur KRITIS, wenn Sie essenzielle Dienstleistungen für einen oder mehrere der genannten Sektoren erbringen und diese Sektoren ohne Ihre Dienste nicht funktionieren könnten. Darüber hinaus wird ein Unternehmen als kritisch betrachtet, wenn ein Ausfall oder eine Beeinträchtigung seiner Dienste erhebliche Versorgungsengpässe, Gefährdungen der öffentlichen Sicherheit oder andere dramatische Auswirkungen hätte.

BÖFI

"Betriebliche Öffentliche Fachinformationsinfrastrukturen" (BÖFIs) sind Informationsinfrastrukturen, die für die Allgemeinheit von besonderem Interesse sind. Sie erfüllen wichtige Funktionen im Bereich der wissenschaftlichen Information und/oder der kulturellen Bildung und sind daher für das Funktionieren der Gesellschaft wichtig. Ein IT-Dienstleister könnte als BÖFI eingestuft werden, wenn seine Dienste für die Aufrechterhaltung dieser Funktionen wesentlich sind.

UNBÖFI

UNBÖFI steht für "Unternehmen und Anbieter von Technischen Diensten" und ist eine weitere Kategorie von Einrichtungen, die durch das IT-Sicherheitsgesetz 2.0 abgedeckt werden. Sie umfasst eine breite Palette von

Unternehmen und Dienstleistern, die nicht unbedingt als KRITIS oder BÖFI eingestuft werden, aber dennoch wichtige Funktionen erfüllen und daher bestimmte IT-Sicherheitsanforderungen erfüllen müssen.

Das IT-Sicherheitsgesetz 2.0, das im Mai 2021 in Deutschland verabschiedet wurde, hat den Anwendungsbereich des IT-Sicherheitsgesetzes erweitert und zusätzliche Kategorien von Unternehmen und Organisationen in den Geltungsbereich aufgenommen.

Gemäß §7 des IT-Sicherheitsgesetzes 2.0 werden nun auch "Unternehmen und Anbieter von Technischen Diensten" (UNBÖFIs) erfasst. Diese Unternehmen, die zuvor nicht unter das Gesetz fielen, sind nun verpflichtet, bestimmte IT-Sicherheitsstandards einzuhalten.

Die genaue Definition der betroffenen Unternehmen und Anbieter technischer Dienste variiert, aber im Allgemeinen bezieht sich der Begriff auf Unternehmen, die Dienstleistungen in den Bereichen Cloud Computing, soziale Netzwerke und Online-Marktplätze anbieten. Einige Beispiele könnten große Tech-Unternehmen wie Google oder Facebook sein, aber auch kleinere Unternehmen, die ähnliche Dienstleistungen anbieten, können betroffen sein.

Darüber hinaus umfasst das IT-Sicherheitsgesetz 2.0 auch "Digitale Dienste" - Unternehmen, die Online-Suchmaschinen, Online-Marktplätze oder Cloud-Computing-Dienste anbieten. Auch diese Unternehmen müssen bestimmte Sicherheitsanforderungen erfüllen und Vorfälle, die die Sicherheit ihrer Dienste beeinträchtigen, melden.

Schließlich sind auch Betreiber Kritischer Infrastrukturen (KRITIS) weiterhin vom IT-Sicherheitsgesetz betroffen. Diese Unternehmen erbringen essenzielle Dienstleistungen in Sektoren wie Energie, Wasser, Ernährung, IT und Telekommunikation, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr, Staat und Verwaltung sowie Medien und Kultur.

Kritischen Infrastrukturen

KRITIS steht für kritische Infrastrukturen und umfasst solche Versorgungsdienstleister, bei deren Beeinträchtigung mit besonders schwerwiegenden Folgen für Wirtschaft, Staat und Gesellschaft zu rechnen ist. Wer genau darunter fällt, wird in der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV) geregelt.

Nach der Verordnung ist eine Kritische Dienstleistung nach § 1 Nr. 3 BSI-KritisV

- „eine Dienstleistung zur Versorgung der Allgemeinheit [...], deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.“

Hintergrund der Auswahl dieser Dienstleister sind die besonders schwerwiegenden Folgen für Wirtschaft, Staat und Gesellschaft, sollte es tatsächlich zu einer Beeinträchtigung kommen. Ob man als Betreiber einer kritischen Infrastruktur anzusehen ist, richtet sich auch nach einem Schwellenwert, der für jeden Sektor anhand einer Berechnungsformel errechnet wird. Der Regelschwellenwert beträgt 500.000 versorgte Personen.

Konkrete Beispiele, wer betroffen ist

Ganz konkret ist der Kreis der Betroffenen viel weiter als oftmals angenommen. Viele Betreiber kritischer Infrastrukturen laufen somit Gefahr nicht zu erkennen, dass sie die gesetzlichen Anforderungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) erfüllen müssen. Zur Veranschaulichung der abstrakten Begriffe sind folgende Beispiele zu nennen:

- Aus dem Sektor Energie, Bereich Verteilung von Fernwärme fällt die Versorgung von 25.000 angeschlossenen Haushalten bereits unter die Verordnung. Dies gilt im Sektor Energie ebenso

für ein Tankstellennetz, das 420.000 Millionen Liter Kraftstoff pro Jahr verteilt.

- Im Sektor Ernährung, Bereich Lebensmittelhandel nennt die Verordnung beim Inverkehrbringen von Lebensmittel die Grenze von 434.500 t Speisen pro Jahr, bzw. 350 Millionen Liter nicht-alkoholischer Getränke.

- Falls das noch nicht genug Zahlen sind, hier noch ein Beispiel aus dem Sektor Gesundheit, Bereich Apotheken: Ab 4.650.000 abgegebenen Packungen pro Jahr fallen auch Apotheken unter die Kritisverordnung.

Gemäß § 7 BSI-KritisV werden bestimmte Unternehmen und Einrichtungen im Bereich des Finanz- und Versicherungswesens als Kritische Infrastrukturen eingestuft. Dazu gehören beispielsweise:

- Kreditinstitute: Banken, Sparkassen, Genossenschaftsbanken und andere Finanzinstitute, die Dienstleistungen im Bereich der Geldanlage, Kreditvergabe und Zahlungsabwicklung anbieten.

- Wertpapierhandelsunternehmen: Unternehmen, die den Handel mit Wertpapieren ermöglichen, wie Börsen, Wertpapierhandelsbanken oder Online-Broker.

- Versicherungsunternehmen: Unternehmen, die Versicherungsleistungen anbieten, einschließlich Schadensversicherungen, Lebensversicherungen, Krankenversicherungen usw.

- Zahlungsdienstleister: Unternehmen, die Zahlungsdienste wie elektronische Zahlungen, Kartenzahlungen, Überweisungen und andere Finanztransaktionen abwickeln.

- Clearingstellen: Einrichtungen, die als zentrale Schnittstelle für den Ausgleich und die Abwicklung von Finanztransaktionen fungieren, insbesondere im Bereich des Derivatehandels.

Schwellenwerte

Das IT-Sicherheitsgesetz 2.0 legt für verschiedene Sektoren und Bereiche unterschiedliche Schwellenwerte fest, um zu bestimmen, welche Unternehmen als Kritische Infrastrukturen (KRITIS) oder als Betreiber öffentlicher Fachinformationsinfrastrukturen (BÖFI) gelten und damit spezielle Anforderungen an die IT-Sicherheit erfüllen müssen.

Für den Finanzsektor beziehen sich diese Schwellenwerte in der Regel auf Aspekte wie das Volumen der abgewickelten Transaktionen, die Anzahl der Kunden oder andere Kennzahlen, die die Bedeutung des Unternehmens für das Funktionieren des Finanzsystems und die Gesellschaft insgesamt widerspiegeln.

Die spezifischen Schwellenwerte für den Finanzsektor sind in der Kritischen Infrastrukturen Verordnung (KRITIS-V) festgelegt. Zum Zeitpunkt meines Wissensstands (September 2021) gelten folgende Schwellenwerte im Finanzsektor für KRITIS-Einrichtungen:

- Kreditinstitute und Finanzdienstleistungsinstitute mit einer Bilanzsumme von mehr als 30 Milliarden Euro.

- Börsen und Betreiber von Handelsplattformen, über die Finanzinstrumente im Sinne des § 2 Absatz 1 des Wertpapierhandelsgesetzes gehandelt werden, die eine durchschnittliche Anzahl von 1 Million Transaktionen pro Tag im Jahresdurchschnitt ausführen.

- Zentrale Gegenparteien, die eine durchschnittliche Anzahl von 1 Million Clearing-Transaktionen pro Tag im Jahresdurchschnitt ausführen.

- Abwicklungsunternehmen, die eine durchschnittliche Anzahl von 1 Million Abwicklungstransaktionen pro Tag im Jahresdurchschnitt ausführen.

- Betreiber eines Systems zur Ausgabe von Zahlungsmitteln in Form von elektronischem Geld mit mehr als 10 Millionen Zahlungskonten.

Das IT-Sicherheitsgesetz 2.0 hat in Deutschland den Geltungsbereich des IT-Sicherheitsgesetzes erweitert, um auch Unternehmen und Organisationen zu erfassen, die in Sektoren von "erheblicher volkswirtschaftlicher Bedeutung" tätig sind. Dies ist ein Anliegen, das sich auf die Wertschöpfung, Rüstung und andere Branchen bezieht, die für die Wirtschaft und die nationale Sicherheit von besonderer Bedeutung sind.

Das Gesetz legt besondere Sicherheitsanforderungen für Unternehmen in diesen Bereichen fest. Es erfordert, dass diese Unternehmen angemessene technische und organisatorische Maßnahmen ergreifen, um die Sicherheit ihrer IT-Systeme, -Komponenten und -Prozesse zu gewährleisten. Es erfordert auch, dass sie einen Mindeststandard an IT-Sicherheit einhalten und bei schwerwiegenden Sicherheitsvorfällen das Bundesamt für Sicherheit in der Informationstechnik (BSI) informieren.

- Wertschöpfung: In diesem Bereich sind Unternehmen von Bedeutung, die eine erhebliche Rolle in der Wirtschaft spielen und deren Ausfall oder Beeinträchtigung erhebliche wirtschaftliche Auswirkungen haben könnte. Es könnte sich um Unternehmen in verschiedenen Branchen handeln, einschließlich, aber nicht beschränkt auf, Produktion, Dienstleistungen und Handel.

- Rüstung: Dieser Sektor umfasst Unternehmen, die zur Verteidigungsfähigkeit des Landes beitragen. Dies könnte Hersteller von militärischer Ausrüstung, Lieferanten von Verteidigungstechnologie und andere Unternehmen, die direkt oder indirekt zur nationalen Sicherheit beitragen, betreffen.

- Gefahrenstoffe: Die Kategorie der "Gefahrenstoffe" stellt im Kontext des IT-Sicherheitsgesetzes einen wichtigen Bereich dar, da die Informations- und Kommunikationstechnologie (IKT) in diesen Unternehmen oft kritische Funktionen zur Sicherheit und Kontrolle ausführt.
  Gefahrenstoffe umfassen eine Vielzahl von Materialien, einschließlich, aber nicht beschränkt auf, Chemikalien, radioaktive Stoffe, biologische Materialien und explosive Materialien, die ein erhebliches Risiko für die Gesundheit und Sicherheit der Menschen oder die Umwelt darstellen können. Unternehmen, die mit solchen Gefahrenstoffen arbeiten, sind oft stark reguliert und müssen strenge Sicherheitsmaßnahmen einhalten. Dies schließt auch die IT-Sicherheit ein, da die Kontrollsysteme für diese Stoffe oft computergesteuert sind und ein Sicherheitsverstoß katastrophale Folgen haben könnte.

Nach dem IT-Sicherheitsgesetz 2.0 müssen diese Unternehmen eine Reihe von Sicherheitsmaßnahmen einhalten, um die Integrität und Sicherheit ihrer IT-Systeme zu gewährleisten. Dazu gehört unter anderem die Implementierung von Sicherheitsmanagementsystemen, die regelmäßige Überprüfung und Aktualisierung ihrer Sicherheitsmaßnahmen, die Meldung von Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Durchführung regelmäßiger Sicherheitsaudits.

IT-Grundschutz Vorgehensweise

Strukturanalyse

Bei der Vorgehensweise des IT-Grundschutzes wird eine Strukturanalyse durchgeführt, um die relevanten Elemente und Komponenten des Informationssicherheitsmanagementsystems (ISMS) zu identifizieren. Im Rahmen der IST-Analyse werden verschiedene Aspekte erfasst:

- Abläufe und Prozesse: Hier werden die Hauptgeschäftsprozesse, Kernprozesse und unterstützenden Prozesse des Unternehmens erfasst. Dies umfasst die Identifikation und Dokumentation der Abläufe und Prozesse, die für den Betrieb der IT-Systeme und die Sicherheit der Informationen relevant sind.
- Anwendungen: Es werden alle relevanten Softwareanwendungen und Dienste erfasst, die im Unternehmen eingesetzt werden. Dazu gehören sowohl Standardsoftware als auch individuell entwickelte Anwendungen. Es ist wichtig, alle Anwendungen zu identifizieren, um mögliche Schwachstellen und Risiken zu erkennen.
- Systeme: Dieser Bereich umfasst die Hardwarekomponenten des IT-Systems, einschließlich Server, virtuelle Server und andere technische Systeme. Es ist wichtig, alle relevanten Systeme zu erfassen, um eine umfassende Sicherheitsbewertung durchführen zu können.
- Gebäude und Räume: Hier werden die Räume, Gebäude und Grundstücke erfasst, in denen sich die IT-Infrastruktur befindet. Dies beinhaltet die Identifikation von sicherheitsrelevanten Merkmalen wie Zugangskontrollen, Brandschutzmaßnahmen und physischer Schutz der Räumlichkeiten.

Die Strukturanalyse bildet die Grundlage für die weiteren Schritte im Rahmen des IT-Grundschutzes. Auf Basis der erfassten Informationen können Schwachstellen und Risiken identifiziert sowie geeignete Schutzmaßnahmen entwickelt und umgesetzt werden, um die Informationssicherheit im Unternehmen zu gewährleisten.

Grundlage der Strukturanalyse

ERFASSUNG GRUNDLEGENDER ANGABEN (IST ANALYSE)

Bei der Vorgehensweise des IT-Grundschutzes werden grundlegende Angaben erfasst, um einen Überblick über das Unternehmen und seine IT-Infrastruktur zu erhalten. Diese grundlegenden Angaben dienen als Ausgangspunkt für die weiteren Schritte im IT-Grundschutz. Hier sind einige der grundlegenden Angaben, die erfasst werden sollten:

- Unternehmensprofil: Hier werden Informationen über das Unternehmen selbst erfasst, wie z.B. Name, Rechtsform, Größe, Organisationsstruktur, Standorte usw. Diese Angaben helfen dabei, das Unternehmen und seine spezifischen Anforderungen besser zu verstehen.

- Verantwortliche Personen: Es werden die für den IT-Grundschutz verantwortlichen Personen identifiziert, z.B. IT-Sicherheitsbeauftragter, Datenschutzbeauftragter oder andere relevante Ansprechpartner. Diese Personen spielen eine wichtige Rolle bei der Umsetzung des IT-Grundschutzes und der Koordination von Sicherheitsmaßnahmen.

- Geschäftsprozesse: Es werden die wesentlichen Geschäftsprozesse des Unternehmens erfasst. Dazu gehören Kernprozesse, Hauptgeschäftsprozesse und unterstützende Prozesse. Diese Angaben helfen dabei, die kritischen Bereiche zu identifizieren, in denen Informationen

geschützt werden müssen.

- IT-Infrastruktur: Es werden Informationen über die IT-Infrastruktur des Unternehmens erfasst, wie z.B. Server, Netzwerke, Betriebssysteme, Datenbanken, Anwendungen, mobile Geräte usw. Diese Angaben ermöglichen es, die technischen Komponenten zu verstehen, die geschützt werden müssen.
- Schutzbedarf: Es wird der Schutzbedarf der Informationen ermittelt. Dazu gehört die Klassifizierung der Informationen nach ihrer Vertraulichkeit, Integrität und Verfügbarkeit. Diese Klassifizierung hilft dabei, geeignete Schutzmaßnahmen zu identifizieren und prioritäre Handlungsbedarfe festzulegen.

Gruppierungen

Bei der Vorgehensweise des IT-Grundschutzes werden Gruppierungen vorgenommen, um eine effiziente und zielgerichtete Umsetzung der Sicherheitsmaßnahmen zu ermöglichen. Diese Gruppierungen dienen dazu, ähnliche Elemente zusammenzufassen, um den Aufwand zu reduzieren und eine einheitliche Vorgehensweise zu gewährleisten. Hier sind einige Gruppierungen, die im Rahmen des IT-Grundschutzes relevant sind:

- Ziele: Die Gruppierung nach Zielen erfolgt, um ähnliche Ziele zu erreichen und die Komplexität zu reduzieren. Zum Beispiel können IT-Systeme, die das Ziel der Vertraulichkeit haben, zusammengefasst werden, um entsprechende Sicherheitsmaßnahmen gezielt umzusetzen.

- Standardisierung: Die Gruppierung nach Standardisierung dient dazu, ähnliche Systeme oder Komponenten zu identifizieren, um eine einheitliche Vorgehensweise bei der Implementierung von Sicherheitsmaßnahmen zu gewährleisten. Dadurch kann der Aufwand reduziert werden, da gleiche Maßnahmen auf mehrere Elemente angewendet werden können.

- Reduzierung möglicher Schwachstellen: Hier werden ähnliche Elemente zusammengefasst, um mögliche Schwachstellen zu reduzieren. Zum Beispiel können ähnliche Server-Konfigurationen oder Netzwerkkomponenten in einer Gruppe zusammengefasst werden, um gezielte Sicherheitsmaßnahmen anzuwenden und potenzielle Risiken zu minimieren.

- Aufwandsreduktion: Diese Gruppierung zielt darauf ab, den Aufwand bei der Umsetzung von Sicherheitsmaßnahmen zu reduzieren. Elemente mit ähnlichen administrativen und infrastrukturellen Rahmenbedingungen werden zusammengefasst, um einheitliche Maßnahmen anzuwenden und den Aufwand für die Implementierung und Überwachung zu minimieren.

Server & Infrastruktur

Nr.	Beschreibung	Betriebssystem	Zielobjektkürzel	Standorte	Anzahl	Eigentümer
SRV1	Hyper-V Server Infrastruktur	Windows Server 2022		SRV-R1.1		
SRV2	Hyper-V Server Schulungsumget	Windows 10 Pro		SRV-R2.2		
SRV3	Backup Server	Windows Server 2022		SVR-R.1.1	1	
FW1	Firewall	Sophos XG Home		SVR-R.1.1	1	
NET1	Router	tbf			1	
NET2						
NET3						
NET4						
NET5	Switch	HP ProCurve		Rack	1	
NET6						
NET7	NAS	Synology DSM	Tank	Rack	1	
NET8						

Clients

Nr.	Beschreibung	Plattform	Zielobjektkürzel	Standorte	Anzahl	Eigentümer
CL01	PC Client	Windows 10				
CL02	NB Client	MacOS				
CL03	PC Client	Windows 11				
CL04	NB Client	Windows 11				

TAB. 1: BEISPIEL FÜR EINE IST-ANALYSE

Zusätzlich zu diesen Gruppierungen werden bei IT-Systemen weitere Faktoren berücksichtigt, wie ähnliche Konfigurationen, Einbindung in das Netzwerk, ähnliche Anwendungen und ein vergleichbarer Schutzbedarf. Diese Faktoren tragen dazu bei, eine kohärente und gezielte Sicherheitsstrategie für ähnliche IT-Systeme zu entwickeln.

Durch die Gruppierung von ähnlichen Elementen im IT-Grundschutz wird eine effiziente und zielgerichtete Umsetzung von Sicherheitsmaßnahmen ermöglicht, wodurch die Informationssicherheit verbessert und der Aufwand optimiert wird.

Die Erfassung dieser grundlegenden Angaben ist der erste Schritt im IT-Grundschutz. Auf dieser Grundlage können anschließend weitere Schritte wie die Gefährdungsanalyse, Maßnahmenplanung und -umsetzung sowie regelmäßige Überprüfungen und Aktualisierungen des IT-Grundschutzes erfolgen.

Tabelle für die Strukturanalyse

Kategorie	Beschreibung	Betroffene Abteilungen (Abkürzung)	Relevanz für Informationssicherheit
Organisatorische Strukturen	Geschäftsführung (GF), Qualitätsmanagement (QMA), Entwicklung (ENT), Vertrieb und Marketing (MAR), Einkauf (EIN), Produktion (PRO), Finanzen und Personal (FIP)	Alle	Hoch: Organisatorische Strukturen sind entscheidend für die Bestimmung von Zuständigkeiten und Verantwortlichkeiten in Bezug auf Informationssicherheit.
Standort	Am Hillenholz 22, 38229 Salzgitter	Alle	Mittel: Physische Standorte beherbergen die IT-Infrastruktur und Arbeitsplätze und sind daher relevant für Sicherheitsbetrachtungen.
IT-Systeme	Server (Serverraum), Arbeitsstationen (Alle	Alle, IT wird durch einen	Hoch: IT-Systeme beherbergen und verarbeiten die meisten,

	Abteilungen), mobile Geräte (Alle Abteilungen)	externen Dienstleister betreut	wenn nicht alle Informationen des Unternehmens. Es ist entscheidend, diese zu schützen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten.
Netzwerke	Firmeninternes LAN (Alle Abteilungen), WLAN für Mitarbeiter und Gäste (Alle Abteilungen), VPN für remote Zugriff (GF, ENT, PRO, MAR, FIP)	Alle, besonders das IT-Team und externe Dienstleister	Hoch: Netzwerke sind die Hauptverbindungswege für den Zugriff auf IT-Systeme und -Anwendungen. Sie müssen sicher gestaltet und verwaltet werden, um unerlaubten Zugriff und andere Bedrohungen zu verhindern.
Anwendungen	CAD-Software für die Produktentwicklung (ENT), ERP-System für die Produktion (PRO), CRM-System für das Kundendatenmanagement (MAR)	Entwicklungsabteilung (ENT), Produktionsabteilung (PRO), Vertrieb und Marketing (MAR)	Hoch: Anwendungen sind oft das Hauptziel von Cyberangriffen. Sie müssen regelmäßig auf Sicherheitslücken überprüft und gepatcht werden.

TAB. 2 STRUKTURANALYSE (IST ANALYSE) AM BEISPIEL DER SZ ROBOTIK GMBH

Die Umsetzung des IT-Grundschutzes erfordert eine umfassende Analyse dieser Strukturen und Prozesse, um geeignete Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Diese Maßnahmen müssen dann kontinuierlich überwacht und angepasst werden, um den sich ständig ändernden Bedrohungslandschaften gerecht zu werden.

Diese Tabelle bietet eine detailliertere Übersicht über die Struktur der SZ Robotik GmbH und zeigt auf, welche Abteilungen und Systeme relevant für die Informationssicherheit sind.

Schutzbedarfsfeststellung

Schutzbedarfskategorien

Die Schutzbedarfskategorien nach IT-Grundschutz des BSI (Bundesamt für Sicherheit in der Informationstechnik) sind in drei Stufen unterteilt:

Normal (Niedrig): Bei dieser Kategorie geht man davon aus, dass die Beeinträchtigung der Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit nur zu geringfügigen Schäden führen würde. Dies könnte etwa der Fall sein, wenn ein nicht geschäftskritisches System ausfällt und dieses schnell wiederhergestellt werden kann oder keine sensiblen Daten verloren gehen bzw. offenbart werden.

Hoch: Hier wird davon ausgegangen, dass die Beeinträchtigung der Schutzziele zu erheblichen Schäden führen könnte. Dies wäre beispielsweise der Fall, wenn geschäftskritische Systeme ausfallen und dies den

Betrieb beeinträchtigt, oder wenn sensible Daten wie persönliche Kundendaten oder Geschäftsgeheimnisse verloren gehen oder offengelegt werden.

Sehr hoch: In dieser Kategorie würde die Beeinträchtigung der Schutzziele zu katastrophalen Schäden führen. Dies könnte z.B. der Fall sein, wenn lebenserhaltende Systeme ausfallen oder wenn hochsensible Daten wie nationale Sicherheitsdaten verloren gehen oder offengelegt werden.

Kritische Infrastrukturen könnten in der Regel in die Kategorien "Hoch" oder "Sehr hoch" fallen, da ein Ausfall oder eine Kompromittierung dieser Infrastrukturen erhebliche oder sogar katastrophale Auswirkungen haben kann. Das könnte z.B. Krankenhäuser, Energieversorgungsunternehmen oder Banken betreffen.

Es ist wichtig zu beachten, dass die Einstufung des Schutzbedarfs stark von den spezifischen Umständen abhängt und daher sorgfältig auf der Grundlage einer umfassenden Risikoanalyse durchgeführt werden muss.

Die Einstufung des Schutzbedarfs basiert auf den potenziellen Auswirkungen, die die Kompromittierung eines bestimmten Assets auf die Organisation hätte. Bei der Bewertung des Schutzbedarfs eines Assets müssen Sie überlegen, wie sich ein Sicherheitsvorfall auf die Verfügbarkeit, Integrität und Vertraulichkeit des Assets auswirken würde.
Es gilt: Wenn der Schutzbedarf hoch oder sehr hoch ist, muss eine Risikoanalyse angefertigt werden.

Einstufung des Schutzbedarf

Lassen Sie uns einige Assets der SZ Robotik GmbH betrachten und ihren potenziellen Schutzbedarf analysieren.

Produktentwicklungsprozesse: Diese sind von zentraler Bedeutung für die Fähigkeit des Unternehmens, wettbewerbsfähige Produkte zu entwickeln. Wenn diese Prozesse gestört würden, könnte dies erhebliche negative Auswirkungen auf das Geschäft haben. Daher könnte der Schutzbedarf als "hoch" eingestuft werden.

Produktionssysteme: Diese Systeme sind direkt für die Herstellung der Produkte verantwortlich. Eine Kompromittierung dieser Systeme könnte die Produktion zum Stillstand bringen und erhebliche finanzielle Verluste verursachen. Daher könnte der Schutzbedarf als "sehr hoch" eingestuft werden.

CRM-Software: Diese Software enthält potenziell sensible Kundendaten und ist für das Management von Kundenbeziehungen unerlässlich. Eine Verletzung der Vertraulichkeit dieser Daten könnte rechtliche Konsequenzen haben und das Vertrauen der Kunden untergraben. Daher könnte der Schutzbedarf als "sehr hoch" eingestuft werden.

Firmengebäude: Das Firmengebäude beherbergt alle physischen Ressourcen des Unternehmens, einschließlich Mitarbeiter, Ausrüstung und physische Datenspeicher. Schäden oder Verluste könnten erhebliche finanzielle Auswirkungen haben und die Geschäftsprozesse stören. Daher könnte der Schutzbedarf als "hoch" eingestuft werden.

Die oben genannten Einschätzungen sind jedoch nur beispielhaft und erfordern eine gründliche Analyse und Bewertung durch Experten, um den genauen Schutzbedarf zu ermitteln. Für eine umfassende Schutzbedarfsfeststellung sollten Sie einen IT-Sicherheitsexperten konsultieren, der mit den spezifischen

Gegebenheiten Ihres Unternehmens vertraut ist.

Vererbung

Die Bestimmung des Schutzbedarfs in der Informationssicherheit ist ein iterativer Prozess, der sowohl die direkte Erhebung des Schutzbedarfs als auch die Berücksichtigung von Abhängigkeiten zwischen verschiedenen Assetklassen umfasst. Dieser Prozess wird als "Vererbung" bezeichnet.

Die Vererbung von Schutzbedarfen beruht auf der Beobachtung, dass der Schutzbedarf eines bestimmten Prozesses oder einer bestimmten Information sich auf diejenigen Systeme, Anwendungen und andere Assets ausdehnt, die zur Verarbeitung dieser Prozesse oder Informationen genutzt werden. Dabei gilt das Prinzip der Maximumsvererbung: Der höchste Schutzbedarf der primären Assets (wie Prozesse und Informationen) wird auf die sekundären Assets (wie Anwendungen, IT-Systeme, Räume, Kommunikationsverbindungen, industrielle Kontrollsysteme und andere Geräte) vererbt.

Dieser Vererbungsprozess kann auch zu einem Kumulationseffekt führen. Wenn zum Beispiel ein IT-System mehrere Anwendungen mit unterschiedlichem Schutzbedarf bedient, kann es notwendig sein, das IT-System entsprechend dem höchsten Schutzbedarf einer seiner Anwendungen zu schützen.

Gleichzeitig kann es einen Verteilungseffekt geben. Das heißt, wenn ein IT-System nur einen geringen Anteil an einer Anwendung mit hohem Schutzbedarf trägt, muss das System möglicherweise nicht entsprechend dem hohen Schutzbedarf dieser Anwendung geschützt werden.

Im Kontext der SZ Robotik GmbH könnte beispielsweise der Prozess der Produktentwicklung als primäres Asset mit hohem Schutzbedarf eingestuft werden, da er wichtige Geschäftsgeheimnisse und innovative Technologien beinhaltet. Daraus ergibt sich, dass die IT-Systeme und Anwendungen, die zur Unterstützung dieses Prozesses genutzt werden, ebenfalls einen hohen Schutzbedarf haben könnten. Gleichzeitig könnte der Reinigungsraum als sekundäres Asset einen niedrigeren Schutzbedarf haben, da er nicht direkt mit den Kernprozessen des Unternehmens verbunden ist.

Modellierung

(Auswahl der Sicherheitsanforderungen)

Die Modellierung oder Auswahl der Sicherheitsanforderungen ist ein weiterer entscheidender Schritt im IT-Grundschutzprozess. In dieser Phase werden die Sicherheitsanforderungen für die Assets definiert, die in den vorherigen Schritten identifiziert wurden. Es ist wichtig zu beachten, dass diese Anforderungen in direktem Zusammenhang mit dem ermittelten Schutzbedarf stehen - je höher der Schutzbedarf, desto strenger sind in der Regel die Sicherheitsanforderungen.

Zunächst gilt es, die für das Unternehmen relevanten Prozess- und Systembausteine aus dem BSI IT-Grundschutz-Kompendium auszuwählen. Das BSI-Grundschutz-Kompendium stellt eine umfangreiche Sammlung von Sicherheitsanforderungen und Maßnahmenempfehlungen dar, die auf verschiedene Prozesse und Systeme angewendet werden können. Es ist in Bausteine gegliedert, die verschiedene Bereiche abdecken, wie beispielsweise Geschäftsprozesse, IT-Systeme, Anwendungen, Netzwerke und Gebäude.

Jeder Baustein im BSI-Grundschutz-Kompendium enthält eine Reihe von Standard-Sicherheitsanforderungen, die sich aus den allgemein anerkannten Best Practices der IT-Sicherheit ableiten. Einige dieser Anforderungen sind generisch und gelten für alle Arten von Assets, während andere spezifischer sind und nur auf bestimmte Arten von Prozessen oder Systemen anwendbar sind.

Die Modellierung der Sicherheitsanforderungen erfordert daher eine sorgfältige Analyse der ausgewählten Bausteine, um zu ermitteln, welche Sicherheitsanforderungen für die spezifischen Assets und Prozesse des Unternehmens relevant sind. Dabei ist es wichtig, sowohl technische als auch organisatorische Aspekte zu berücksichtigen und sicherzustellen, dass die ausgewählten Sicherheitsanforderungen effektiv umgesetzt und kontinuierlich überprüft werden können. Dabei ist es entscheidend, dass die gewählten Maßnahmen im Kontext des Unternehmens umsetzbar sind und den Betriebsablauf nicht unnötig beeinträchtigen.

IT-Grundschutz-Management

Der Systembaustein "IT-Grundschutz-Management" ist ein Element, das Sie niemals ausschließen sollten. Er ist ein essenzieller Teil des IT-Grundschutz-Konzepts und legt den Fokus auf die organisatorischen und managementbezogenen Aspekte der Informationssicherheit.

Dieser Baustein beinhaltet die Themen:

- Informationssicherheitsleitlinie: Die Entwicklung und Umsetzung einer Leitlinie für Informationssicherheit, die den Umgang mit und den Schutz von Informationen im Unternehmen regelt.
- Informationssicherheitsorganisation: Die Etablierung einer Struktur und eines Prozesses für die Verwaltung der Informationssicherheit im Unternehmen.
- Personal und Sicherheit: Die Sicherstellung, dass das Personal ausreichend in Sicherheitsfragen geschult ist und die Sicherheitsvorgaben befolgt.
- Notfallvorsorge: Die Entwicklung und Umsetzung eines Plans für den Umgang mit Sicherheitsvorfällen und Notfällen.
- Betrieb des ISMS: Der fortlaufende Betrieb und die Weiterentwicklung des Informationssicherheits-Managementsystems (ISMS).

Dieser Systembaustein stellt sicher, dass das Unternehmen eine effektive Struktur und Strategie für die Informationssicherheit hat und dass die Anforderungen an die Informationssicherheit erfüllt werden können. Es stellt auch sicher, dass das Unternehmen auf Sicherheitsvorfälle und Notfälle vorbereitet ist und dass das Personal die Bedeutung der Informationssicherheit versteht und die Sicherheitsvorgaben befolgt.

Zusammenfassend lässt sich sagen, dass der Systembaustein "IT-Grundschutz-Management" von grundlegender Bedeutung für die Umsetzung eines effektiven Informationssicherheitsmanagements ist und daher in keiner IT-Grundschutz-Betrachtung ausgeschlossen werden sollte.

Prozess und Systembausteine

Im BSI-Grundschutzkompendium sind die Bausteine auf eine bestimmte Weise strukturiert, um ein umfassendes Verständnis und eine effiziente Umsetzung von Informationssicherheitsmaßnahmen zu unterstützen. Jeder Baustein im Kompendium ist wie folgt aufgebaut:

- Beschreibung: Hier werden der Inhalt und Zweck des Bausteins im Allgemeinen dargelegt. Dieser Abschnitt ist weiter in folgende Unterabschnitte gegliedert:
- Einleitung: Hier wird ein Überblick über den Baustein und seine Bedeutung für die Informationssicherheit gegeben.
- Zielsetzung: In diesem Teil wird das spezifische Ziel des Bausteins detailliert erläutert.

- Abgrenzung und Modellierung: Hier wird der Umfang des Bausteins definiert und erklärt, wie er sich in das Gesamtmodell der Informationssicherheit einfügt.
- Spezifische Gefährdungsgrundlage: In diesem Abschnitt werden die spezifischen Risiken und Gefahren aufgezeigt, die der Baustein zu adressieren sucht.
- Anforderungen: Im Anforderungsteil werden die Maßnahmen dargestellt, die notwendig sind, um das im Baustein definierte Ziel zu erreichen. Bitte beachten Sie, dass diese keine konkreten Maßnahmen sind, sondern eher Richtlinien und Vorgaben, die die Umsetzung leiten sollen. Die Anforderungen sind unterteilt in:
- Zuständigkeiten: Hier wird bestimmt, wer für die Implementierung der jeweiligen Anforderungen verantwortlich ist.
- Basis-Anforderungen: Diese repräsentieren die grundlegenden Voraussetzungen, die erfüllt sein müssen, um das Ziel des Bausteins zu erreichen.
- Standard-Anforderungen: Diese Anforderungen gehen über die Basisanforderungen hinaus und werden in der Regel für die meisten Implementierungen benötigt.
- Anforderungen bei erhöhtem Schutzbedarf: Diese Anforderungen gelten für Szenarien, in denen ein erhöhter Schutzbedarf besteht. Sie sind in der Regel strenger als die Standardanforderungen.

Auf der Website des BSI gibt es eine Seite mit den IT-Grundschutz-Bausteinen (Edition 2023). Dort können Sie die Bausteine im PDF- oder MS-Word-Format als ZIP-Datei herunterladen.

Unterschiede und Anwendung der Bausteine

Im BSI-Grundschutzkompendium werden System- und Prozessbausteine verwendet, um ein umfassendes Verständnis und eine effiziente Umsetzung von Informationssicherheitsmaßnahmen zu ermöglichen. Der Unterschied zwischen den beiden liegt in ihrer Ausrichtung und dem Anwendungsbereich.

- Systembausteine beziehen sich auf IT-Systeme, Anwendungen, Netzwerke, Gebäude und andere technische Komponenten. Sie bieten spezifische Anforderungen und Maßnahmenempfehlungen, die auf technische Aspekte der Informationssicherheit abzielen. Diese Bausteine ermöglichen die gezielte Absicherung von IT-Systemen und unterstützen bei der Umsetzung von Best Practices, um Sicherheitsrisiken zu minimieren.
- Prozessbausteine hingegen konzentrieren sich auf die Sicherung von Geschäftsprozessen, organisatorischen Abläufen und Managementaspekten. Sie umfassen Richtlinien, Verfahren und Maßnahmen zur Steuerung und Absicherung der Prozesse. Diese Bausteine zielen darauf ab, die organisationale Ebene der Informationssicherheit zu unterstützen, indem sie klare Verantwortlichkeiten, Sicherheitsleitlinien und Notfallpläne festlegen.

Die Kombination von System- und Prozessbausteinen im BSI-Grundschutzkompendium ermöglicht eine ganzheitliche Betrachtung der Informationssicherheit. Die Bausteine dienen als Orientierung und bieten einen Rahmen für die Umsetzung von Sicherheitsmaßnahmen, die den spezifischen Anforderungen eines Unternehmens gerecht werden. Durch die gezielte Anwendung der Bausteine kann eine umfassende und angemessene Sicherheitsstrategie entwickelt und umgesetzt werden, um die Informationssicherheit zu gewährleisten.

Kategorien der Systembausteine

Die Bausteine im BSI-Grundschutzkompendium sind in verschiedene Kategorien gegliedert, um die Umsetzung der Informationssicherheit in Schichten oder Stufen zu unterstützen. Eine solche Gliederung erfolgt in der Regel nach den Kategorien "Strategie", "Basis-Absicherung", "Standard-Absicherung" und "Kern-Absicherung". Die Kategorie "Strategie" umfasst Bausteine, die sich mit der Entwicklung einer umfassenden Informationssicherheitsstrategie und -politik für das Unternehmen befassen. Hier werden die grundlegenden Leitlinien und Ziele für die Informationssicherheit festgelegt und die Verantwortlichkeiten sowie die organisatorischen Strukturen definiert.

Die Bausteine der "Basis-Absicherung" dienen als Grundlage für die Umsetzung von Mindeststandards und grundlegenden Sicherheitsmaßnahmen. Sie umfassen beispielsweise die Sicherung von physischen Zugängen, die Schulung der Mitarbeiter in Sicherheitsfragen und die Implementierung von grundlegenden Netzwerksicherheitsmaßnahmen. In der Kategorie "Standard-Absicherung" finden sich Bausteine, die spezifische Anforderungen für bestimmte Bereiche wie IT-Systeme, Anwendungen oder Kommunikationsinfrastrukturen abdecken. Diese Bausteine bieten detailliertere Sicherheitsmaßnahmen und Empfehlungen, die über die Mindeststandards hinausgehen und an die spezifischen Anforderungen der Organisation angepasst werden können. Die Bausteine der "Kern-Absicherung" sind besonders anspruchsvoll und umfassen Sicherheitsmaßnahmen für kritische Systeme und Prozesse. Hier werden spezifische Schutzanforderungen für hochsensible Daten, kritische Infrastrukturen oder besondere Bedrohungen definiert. Diese Bausteine stellen sicher, dass die essentiellen Elemente der Informationssicherheit angemessen geschützt sind. Die Gliederung der Bausteine nach Strategie, Basis-Absicherung, Standard-Absicherung und Kern-Absicherung bietet Unternehmen eine strukturierte Herangehensweise an die Informationssicherheit. Sie ermöglicht eine schrittweise Implementierung von Sicherheitsmaßnahmen, beginnend mit den grundlegenden Anforderungen und schrittweise fortgeschrittenen Maßnahmen, um die Informationssicherheit kontinuierlich zu verbessern und an die spezifischen Bedürfnisse des Unternehmens anzupassen.

IT-Grundschutzcheck (Soll-Ist-Vergleich)

Der IT-Grundschutzcheck Teil 1, auch bekannt als Soll-Ist-Vergleich, ist eine wichtige Methode, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen wird. Dieser Check dient dazu, den Ist-Zustand der Informationssicherheit in einem Unternehmen mit den angestrebten Sicherheitszielen (Soll-Zustand) zu vergleichen. Durch den Abgleich der tatsächlich implementierten Sicherheitsmaßnahmen mit den empfohlenen Maßnahmen des BSI können Schwachstellen und Abweichungen identifiziert werden. Der IT-Grundschutzcheck Teil 1 umfasst unter anderem eine umfassende Risikoanalyse, bei der potenzielle Bedrohungen und deren Auswirkungen bewertet werden. Ziel ist es, eine konsolidierte Übersicht über den aktuellen Sicherheitsstatus zu erhalten und darauf aufbauend geeignete Maßnahmen zur Verbesserung der Informationssicherheit zu ergreifen. Der IT-Grundschutzcheck Teil 1 bildet somit eine solide Grundlage für ein effektives Informationssicherheitsmanagement gemäß den Standards des BSI.

Eine Modellierung nach der Standardabsicherung nach BSI Grundschutz für die entsprechenden Bausteine könnte folgendermaßen aussehen:

- SYS 1.1 (Insider-Bedrohung):

- Maßnahmen überprüfen: Zugriffsbeschränkungen implementieren und Benutzersitzungen überwachen.
- Bewertung der Wirksamkeit: Prüfen Sie, ob die Zugriffsbeschränkungen ausreichend sind und ob die Überwachung der Benutzersitzungen verdächtige Aktivitäten erkennen kann.
- Konformitätsprüfung: Sicherstellen, dass die implementierten Maßnahmen den empfohlenen Standards entsprechen.

- SYS 1.9 (Datenverlust):
  - Maßnahmen überprüfen: Implementierung von Backup- und Recovery-Mechanismen.
  - Bewertung der Wirksamkeit: Überprüfen ob regelmäßige Backups durchgeführt werden und ob ein Wiederherstellungsplan vorhanden ist.
  - Konformitätsprüfung: Stellen Sie sicher, dass die implementierten Maßnahmen den empfohlenen Standards entsprechen.
- SYS 2.1 (Systemausfall):
  - Maßnahmen überprüfen: Implementierung von Redundanz- und Failover-Mechanismen.
  - Bewertung der Wirksamkeit: Prüfen ob die implementierten Mechanismen den Ausfall des Terminalservers verhindern oder schnell wiederherstellen können.

Konformitätsprüfung: Sicherstellen, dass die implementierten Maßnahmen den empfohlenen Standards entsprechen.

Zielobjekt	Systembausteine	Gefährdung	Eintrittshäufigkeit	Auswirkung	Risiko	Risikobehandlungsoption	Erläuterung zur Risikobehandlung
Mailserver	SRV 1.1	Schadsoftware	Hoch	Hoch	Hoch	Implementierung eines aktuellen Virenschutzprogramms auf dem Mailserver	Regelmäßige Aktualisierung des Virenschutzprogramms und Durchführung von automatischen Scans zur Erkennung und Entfernung von Schadsoftware.
	APP 5.2	Unberechtigter Zugriff	Mittel	Hoch	Hoch	Umsetzung einer Zugriffskontrolle mit Berechtigungsstufen	Festlegung von Berechtigungsstufen für Benutzerkonten, um unberechtigten Zugriff zu verhindern. Regelmäßige Überprüfung und Aktualisierung der Zugriffsrechte.
Webserver	SRV 1.1	Denial-of-Service-Angriffe	Mittel	Hoch	Hoch	Implementierung einer DDoS-Schutzlösung	Einrichtung einer DDoS-Schutzlösung, die den Webserver vor übermäßigem Datenverkehr und DDoS-Angriffen schützt.
	APP 5.3	Webanwendungsschwachstellen	Hoch	Hoch	Hoch	Durchführung von regelmäßigen Sicherheitsaudits und Patch-Management	Regelmäßige Überprüfung der Webanwendungen auf Schwachstellen und Aktualisierung mit Sicherheitspatches, um Angriffsvektoren zu minimieren.
Terminalserver	SRV 1.1	Unberechtigter Zugriff	Hoch	Hoch	Hoch	Implementierung einer sicheren Authentifizierungsmethode	Verwendung von starken Passwortrichtlinien, Zwei-Faktor-Authentifizierung und regelmäßige Überprüfung der Benutzerkonten und Zugriffsrechte.
	SYS 1.1	Insider-Bedrohung	Mittel	Hoch	Hoch	Implementierung von Zugriffsbeschränkungen und Überwachung der Benutzersitzungen	Einschränkung des Zugriffs auf autorisierte Benutzer, Überwachung und Protokollierung der Benutzersitzungen, um verdächtige Aktivitäten zu erkennen.
	APP 5.3	Fehlkonfiguration	Niedrig	Hoch	Hoch	Implementierung von Konfigurationsrichtlinien und regelmäßige Überprüfung der Einstellungen	Festlegung von Konfigurationsrichtlinien, regelmäßige Überprüfung der Konfigurationseinstellungen und Durchführung von Sicherheitsaudits.

TAB. 3: MODELLIERUNG NACH STANDARDABSICHERUNG FÜR EIN ZIELOBJEKT. HIER AM BEISPIEL EINES MAILSERVERS, WEBSERVERS UND EINES TERMINAL SERVERS

Risikoanalyse

Einführung in die Risikoanalyse

Die Risikoanalyse spielt eine entscheidende Rolle im Rahmen des BSI-Grundschutzes und ist ein wesentlicher Bestandteil eines umfassenden Informationssicherheitsmanagementsystems. Dieses Kapitel gibt einen Überblick über die Bedeutung der Risikoanalyse im Kontext des BSI-Grundschutzes, erläutert die Zielsetzung der Risikoanalyse und verdeutlicht deren Nutzen für die Informationssicherheit. Zudem wird ein Überblick über den Prozess der Risikoanalyse gegeben, um den Lesern ein grundlegendes Verständnis dieser wichtigen Methode zur Identifizierung und Bewertung von Risiken zu vermitteln.

Bedeutung der Risikoanalyse

(IM RAHMEN DES BSI-GRUNDSCHUTZES)

Die Risikoanalyse bildet die Grundlage für die Festlegung geeigneter Schutzmaßnahmen im Rahmen des BSI-Grundschutzes. Sie ermöglicht eine systematische Identifizierung und Bewertung von Risiken für die Informationssicherheit und dient als Grundlage für die Auswahl und Umsetzung von geeigneten Schutzmaßnahmen. Die Risikoanalyse unterstützt Unternehmen und Organisationen dabei, ihre Infrastrukturen und Informationen angemessen abzusichern und gezielte Maßnahmen zur Risikominderung zu ergreifen.

Zielsetzung der Risikoanalyse

(UND DEREN NUTZEN FÜR DIE INFORMATIONSSICHERHEIT)

Die Zielsetzung der Risikoanalyse besteht darin, die relevanten Risiken für die Informationssicherheit zu identifizieren, zu bewerten und zu behandeln. Durch die systematische Analyse von Bedrohungen, Schwachstellen und Schutzbedarf können Organisationen eine fundierte Grundlage für ihre Sicherheitsentscheidungen schaffen. Die Risikoanalyse ermöglicht es, potenzielle Risiken zu erkennen, angemessene Schutzmaßnahmen zu ergreifen und Ressourcen effektiv einzusetzen, um die Informationssicherheit zu gewährleisten. Sie trägt zur Risikominderung bei und unterstützt die Organisation dabei, Sicherheitsvorfälle zu verhindern oder adäquat darauf zu reagieren.

Überblick über den Prozess der Risikoanalyse

Der Prozess der Risikoanalyse besteht aus mehreren aufeinanderfolgenden Schritten, die systematisch durchgeführt werden, um eine fundierte Bewertung der Risiken zu ermöglichen. Der genaue Ablauf kann je nach Kontext und spezifischen Anforderungen variieren, jedoch folgt er im Allgemeinen den grundlegenden Prinzipien des BSI-Grundschutzes. Im Folgenden wird ein Überblick über die typischen Schritte des Risikoanalyseprozesses gegeben:

- Identifikation von Assets: Erfassung und Klassifizierung der zu schützenden Informationen und Systeme.

- Identifikation von Bedrohungen: Identifizierung potenzieller Bedrohungen, die auf die Assets einwirken können.
- Identifikation von Schwachstellen: Erkennung von Sicherheitslücken und Schwachstellen in den Assets und den zugrunde liegenden Systemen.
- Bewertung der Eintrittshäufigkeit: Bewertung der Wahrscheinlichkeit, mit der Bedrohungen auf die Schwachstellen treffen können.
- Bewertung der Auswirkung: Bewertung des Schadenspotenzials, den die Bedrohungen bei Ausnutzung der Schwachstellen verursachen können.
- Risikobewertung: Kombination der Eintrittshäufigkeit und der Auswirkung, um das Gesamtrisiko zu bewerten.
- Risikobehandlung: Ableitung von Maßnahmen zur Risikominderung und Entwicklung eines Maßnahmenplans.
- Überwachung und Aktualisierung: Kontinuierliche Überwachung der Risikolage, Aktualisierung der Risikobewertung und Anpassung der Maßnahmen, wenn erforderlich.

Der Prozess der Risikoanalyse ist ein iterativer Prozess, der regelmäßig wiederholt werden sollte, um Veränderungen in der Risikolage angemessen zu berücksichtigen und sicherzustellen, dass die implementierten Schutzmaßnahmen weiterhin effektiv sind.

Dieses Kapitel bietet einen Einstieg in die Risikoanalyse im Rahmen des BSI-Grundschutzes. Es betont die Bedeutung der Risikoanalyse für die Informationssicherheit, erläutert die Zielsetzung der Risikoanalyse und gibt einen Überblick über den Prozess der Risikoanalyse. In den folgenden Kapiteln werden die einzelnen Schritte des Risikoanalyseprozesses detaillierter behandelt, um den Lesern eine umfassende Anleitung zur Durchführung einer Risikoanalyse nach dem BSI-Grundschutzkompendium zu bieten.

Grundlagen der Risikoanalyse

Die Grundlagen der Risikoanalyse sind entscheidend, um ein fundiertes Verständnis der Methoden und Konzepte zu entwickeln. Dieses Kapitel legt den Fokus auf die Definition von Risiko und anderen relevanten Begriffen wie Schutzbedarf, Bedrohung und Schwachstelle. Es erläutert die Bedeutung des Risikomanagements für die Informationssicherheit und zeigt auf, wie die Risikoanalyse in den Gesamtprozess des BSI-Grundschutzes integriert ist.

Definition von Risiko und relevanter Begriffe

Risiko wird definiert als die Kombination der Eintrittshäufigkeit eines Schadensereignisses und der damit verbundenen Auswirkung. Es repräsentiert die Möglichkeit, dass Bedrohungen auf Schwachstellen treffen und Schaden verursachen können. Dabei können folgende Begriffe unterschieden werden:

- Schutzbedarf: Der Schutzbedarf beschreibt den Wert und die Bedeutung von Assets (Informationen, Systeme, Prozesse), die vor Bedrohungen geschützt werden sollen. Er kann in Kategorien wie Vertraulichkeit, Integrität und Verfügbarkeit unterteilt werden.
- Bedrohung: Eine Bedrohung bezeichnet eine potenzielle Gefahr, die auf Assets einwirken und Schaden verursachen kann. Beispiele für Bedrohungen sind Malware, Hackerangriffe, Naturkatastrophen oder menschliches Fehlverhalten.

- Schwachstelle: Eine Schwachstelle ist eine Sicherheitslücke oder eine verwundbare Stelle in einem System oder einer Komponente, die von einer Bedrohung ausgenutzt werden kann, um unerlaubten Zugriff zu erlangen oder Schaden zu verursachen.

Bedeutung des Risikomanagements für die Informationssicherheit

Das Risikomanagement ist ein zentraler Bestandteil des Informationssicherheitsmanagements und dient dazu, Risiken zu identifizieren, zu bewerten, zu behandeln und zu überwachen. Es ermöglicht eine systematische Herangehensweise an die Risikominderung und trägt dazu bei, sicherheitsrelevante Entscheidungen zu treffen und Ressourcen effektiv einzusetzen.

Das Risikomanagement umfasst folgende Schritte:

- Risikoanalyse: Identifikation, Bewertung und Klassifizierung von Risiken im Hinblick auf die Informationssicherheit.
- Risikobehandlung: Auswahl und Umsetzung geeigneter Maßnahmen zur Risikominderung oder -vermeidung.
- Risikoüberwachung: Kontinuierliche Überwachung der Risikosituation und Anpassung der Maßnahmen bei Bedarf.

Durch ein effektives Risikomanagement können Organisationen ihre Informationssicherheit verbessern, potenzielle Schäden minimieren und die Verfügbarkeit, Integrität und Vertraulichkeit ihrer Informationen gewährleisten.

Integration der Risikoanalyse

(In den Gesamtprozess des BSI-Grundschutzes)

Die Risikoanalyse ist ein integraler Bestandteil des BSI-Grundschutzes und eng mit den anderen Phasen des Prozesses verbunden. Sie bildet die Grundlage für die Ableitung und Umsetzung geeigneter Schutzmaßnahmen. Die Risikoanalyse ist in folgende Schritte des BSI-Grundschutzprozesses integriert:

- Bestandsaufnahme: Erfassung der zu schützenden Assets und deren Schutzbedarf.
- Bedrohungsanalyse: Identifikation und Bewertung von Bedrohungen, die auf die Assets einwirken können.
- Schwachstellenanalyse: Identifikation und Bewertung von Schwachstellen in den Assets und den zugrunde liegenden Systemen.
- Maßnahmenauswahl: Ableitung von Schutzmaßnahmen basierend auf den Ergebnissen der Risikoanalyse.
- Maßnahmenumsetzung: Implementierung der ausgewählten Schutzmaßnahmen zur Risikominderung.
- Überprüfung: Kontinuierliche Überprüfung und Aktualisierung der implementierten Maßnahmen im Rahmen der Risikobewertung.

Die Risikoanalyse ist somit ein entscheidender Schritt im Gesamtprozess des BSI-Grundschutzes und unterstützt die gezielte Absicherung von Informationen und Systemen entsprechend ihrer Bedeutung und den identifizierten Risiken.

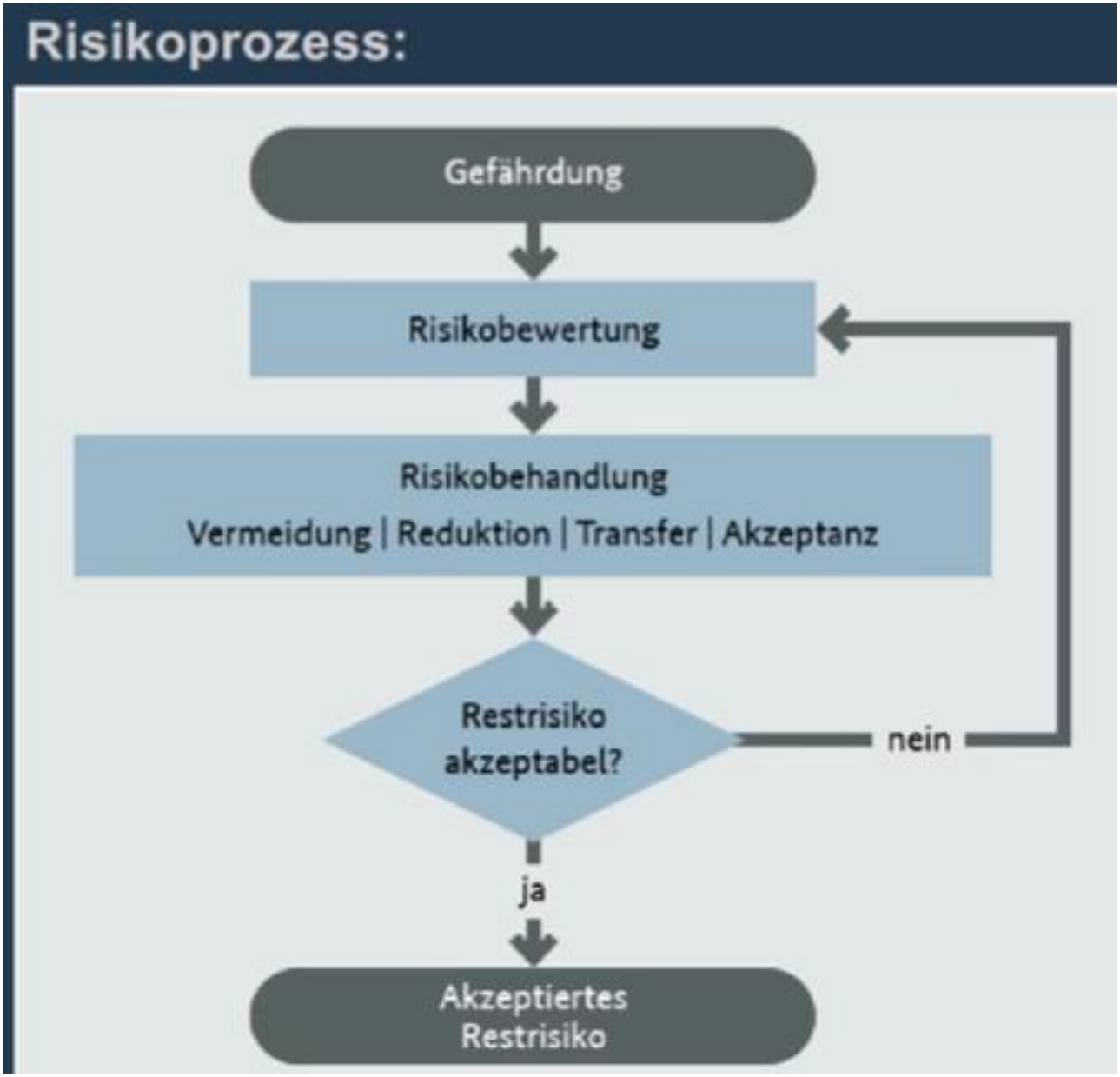

ABB. 1: RISIKOPROZESS

Dieses Kapitel hat einen Einblick in die Grundlagen der Risikoanalyse gegeben. Es definiert Risiko und verwandte Begriffe wie Schutzbedarf, Bedrohung und Schwachstelle. Zudem hebt es die Bedeutung des Risikomanagements für die Informationssicherheit hervor und zeigt auf, wie die Risikoanalyse in den Gesamtprozess des BSI-Grundschutzes integriert ist. In den folgenden Kapiteln werden die einzelnen Schritte der Risikoanalyse detaillierter behandelt, um den Lesern eine praxisnahe Anleitung zur Durchführung einer Risikoanalyse im Rahmen des BSI-Grundschutzes zu bieten.

Durchführung einer Risikoanalyse nach dem BSI-Grundschutz

Die Durchführung einer Risikoanalyse nach dem BSI-Grundschutz umfasst mehrere Schritte, die systematisch durchgeführt werden, um eine umfassende Bewertung der Risiken zu ermöglichen. Dieses Kapitel beschreibt die Schritte der Risikoanalyse, nämlich die Identifikation, Bewertung, Behandlung und Überwachung von Risiken. Darüber hinaus werden Methoden und Ansätze zur Identifikation von Bedrohungen, Schwachstellen und Schutzbedarf erläutert. Zudem werden verschiedene Methoden zur

Bewertung von Risiken vorgestellt, wie beispielsweise die Verwendung einer Risikomatrix oder einer Risikobewertungsmatrix.

Schritte der Risikoanalyse

Die Risikoanalyse besteht aus den folgenden Schritten:

Identifikation von Risiken

In diesem Schritt werden potenzielle Risiken für die Informationssicherheit identifiziert. Hierbei werden Bedrohungen, Schwachstellen und der Schutzbedarf der Assets berücksichtigt. Es werden Informationen gesammelt, um eine umfassende Übersicht über mögliche Risiken zu erhalten.

Bewertung von Risiken

Nach der Identifikation werden die Risiken bewertet. Dies beinhaltet die Bewertung der Eintrittshäufigkeit und der Auswirkung jedes Risikos. Die Eintrittshäufigkeit gibt an, wie wahrscheinlich ein Risiko eintritt, während die Auswirkung den potenziellen Schaden beschreibt. Die Bewertung erfolgt oft auf einer numerischen Skala, um eine Vergleichbarkeit und Priorisierung der Risiken zu ermöglichen.

Behandlung von Risiken

Nach der Bewertung der Risiken werden geeignete Maßnahmen zur Risikominderung oder -vermeidung entwickelt. Die Auswahl der Maßnahmen erfolgt auf der Grundlage der Bewertungsergebnisse. Es werden konkrete Handlungspläne erstellt, um die identifizierten Risiken anzugehen und zu reduzieren.

Überwachung von Risiken

Die Überwachung der Risiken ist ein kontinuierlicher Prozess, um sicherzustellen, dass die implementierten Maßnahmen wirksam sind und die Risikosituation angemessen berücksichtigt wird. Es werden Mechanismen eingerichtet, um Änderungen in der Risikolage zu erkennen und bei Bedarf Anpassungen vorzunehmen.

Methoden und Ansätze

(ZUR IDENTIFIKATION VON BEDROHUNGEN, SCHWACHSTELLEN UND SCHUTZBEDARF)

Es gibt verschiedene Methoden und Ansätze zur Identifikation von Bedrohungen, Schwachstellen und Schutzbedarf. Hier sind einige gängige Ansätze:

- Expertenwissen: Erfahrene Fachleute aus den relevanten Bereichen identifizieren aufgrund ihres Fachwissens und ihrer Erfahrung potenzielle Bedrohungen, Schwachstellen und Schutzbedarf.
- Checklisten: Vorgefertigte Checklisten können verwendet werden, um systematisch mögliche Bedrohungen, Schwachstellen und Schutzbedarf zu erfassen und zu bewerten.
- Szenarien: Die Entwicklung von Szenarien ermöglicht es, potenzielle Bedrohungen und Schwachstellen zu visualisieren und deren Auswirkungen auf die Assets zu analysieren.
- Schwachstellenanalysen: Durch die Untersuchung von Systemen, Anwendungen oder Infrastrukturen können Schwachstellen identifiziert werden.
- Interviews und Workshops: Durch Gespräche mit relevanten Stakeholdern können wertvolle Informationen über mögliche Bedrohungen, Schwachstellen und Schutzbedarf gewonnen werden.

- Literaturrecherche: Die Analyse von Fachliteratur, Best Practices und branchenspezifischen Standards kann wichtige Erkenntnisse über Bedrohungen und Schwachstellen liefern.

Methoden zur Bewertung von Risiken

Für die Bewertung von Risiken stehen verschiedene Methoden zur Verfügung. Hier sind zwei häufig verwendete Methoden:

- Risikomatrix: Eine Risikomatrix ist eine zweidimensionale Matrix, die die Eintrittshäufigkeit und die Auswirkung von Risiken bewertet. Die Risiken werden in Kategorien wie "gering", "mittel" und "hoch" eingestuft, um eine Priorisierung zu ermöglichen.
- Risikobewertungsmatrix: Eine Risikobewertungsmatrix kombiniert die Bewertung der Eintrittshäufigkeit und der Auswirkung von Risiken mit Gewichtungsfaktoren, um das Gesamtrisiko zu berechnen. Die Gewichtungsfaktoren spiegeln die Bedeutung und Priorität der Schutzbedarfskategorien wider.

Diese Methoden dienen dazu, eine objektive Bewertung der Risiken zu ermöglichen und eine Grundlage für die Auswahl von Maßnahmen zur Risikominderung zu schaffen.

Dieses Kapitel hat die Schritte der Risikoanalyse nach dem BSI-Grundschutz beschrieben, einschließlich der Identifikation, Bewertung, Behandlung und Überwachung von Risiken. Zudem wurden Methoden und Ansätze zur Identifikation von Bedrohungen, Schwachstellen und Schutzbedarf erläutert. Weiterhin wurden verschiedene Methoden zur Bewertung von Risiken, wie die Risikomatrix und die Risikobewertungsmatrix, vorgestellt. Durch die Anwendung dieser Schritte und Methoden kann eine fundierte Risikoanalyse durchgeführt werden, um die Informationssicherheit effektiv zu gewährleisten.

Risikobewertung und Risikobewertungsfaktoren

Die Risikobewertung spielt eine zentrale Rolle in der Risikoanalyse und hilft dabei, die identifizierten Risiken zu quantifizieren und zu priorisieren. In diesem Kapitel wird erläutert, wie die Risikobewertung durchgeführt wird und welche Faktoren dabei berücksichtigt werden sollten. Insbesondere wird auf die Risikobewertungsfaktoren des BSI-Grundschutzes eingegangen, die eine wichtige Grundlage für die Bewertung der Risiken bilden.

Durchführung der Risikobewertung

Die Risikobewertung umfasst die Kombination der Bewertung der Eintrittshäufigkeit und der Auswirkung von Risiken, um das Gesamtrisiko zu ermitteln. Dabei ist es wichtig, eine standardisierte Vorgehensweise zu verwenden, um eine Vergleichbarkeit der Risikobewertungen zu ermöglichen. Ein häufig verwendetes Verfahren ist die Verwendung einer Risikomatrix oder einer Risikobewertungsmatrix.

Die Risikobewertung kann auf einer qualitativen oder quantitativen Basis durchgeführt werden. Bei einer qualitativen Bewertung werden die Risiken anhand von Kategorien wie "gering", "mittel" und "hoch" eingestuft. Bei einer quantitativen Bewertung werden numerische Werte für Eintrittshäufigkeit und Auswirkung verwendet, um das Gesamtrisiko zu berechnen.

Es ist wichtig zu beachten, dass die Risikobewertung immer im Kontext der spezifischen Organisation und ihrer individuellen Risikotoleranz erfolgen sollte. Die Bewertungskriterien und -maßstäbe sollten entsprechend angepasst werden, um den spezifischen Anforderungen gerecht zu werden.

Risikobewertungsfaktoren des BSI-Grundschutzes

Der BSI-Grundschutz definiert eine Reihe von Risikobewertungsfaktoren, die als Grundlage für die Bewertung der Risiken dienen. Diese Faktoren berücksichtigen die Vertraulichkeit, Integrität und Verfügbarkeit der Assets und ermöglichen eine umfassende Bewertung der Risiken im Kontext der Informationssicherheit.

Die Risikobewertungsfaktoren des BSI-Grundschutzes umfassen:

- Vertraulichkeit: Der Schutz vor unbefugtem Zugriff auf Informationen und Systeme, um die Vertraulichkeit zu gewährleisten.
- Integrität: Der Schutz vor unbefugten Änderungen oder Manipulationen von Informationen und Systemen, um die Integrität sicherzustellen.
- Verfügbarkeit: Der Schutz vor Ausfällen oder Unterbrechungen von Informationen und Systemen, um die Verfügbarkeit zu gewährleisten.

Diese Risikobewertungsfaktoren dienen dazu, die Bewertung der Eintrittshäufigkeit und der Auswirkung von Risiken im Hinblick auf die relevanten Schutzbedarfskategorien zu unterstützen. Sie ermöglichen eine differenzierte Betrachtung der Risiken und eine präzisere Priorisierung der Maßnahmen zur Risikominderung.

Bei der Durchführung der Risikobewertung nach dem BSI-Grundschutz ist es wichtig, die spezifischen Anforderungen und die Risikotoleranz der Organisation zu berücksichtigen und die Risikobewertungsfaktoren entsprechend anzupassen.

Dieses Kapitel hat die Durchführung der Risikobewertung und die relevanten Risikobewertungsfaktoren behandelt. Es wurden verschiedene Ansätze zur Durchführung der Risikobewertung, wie die Verwendung von Risikomatrizen, erläutert. Darüber hinaus wurden die Risikobewertungsfaktoren des BSI-Grundschutzes, nämlich Vertraulichkeit, Integrität und Verfügbarkeit, vorgestellt. Durch die Anwendung dieser Konzepte können Organisationen eine fundierte Risikobewertung durchführen und angemessene Maßnahmen zur Risikominderung ableiten.

Risikobehandlung und Maßnahmenplanung

Die Risikobehandlung ist ein wesentlicher Schritt in der Risikoanalyse, um die identifizierten Risiken zu reduzieren oder zu vermeiden. In diesem Kapitel wird erläutert, wie die Risikobehandlung durchgeführt wird und wie ein Maßnahmenplan entwickelt wird, um die identifizierten Risiken gezielt anzugehen. Es werden verschiedene Aspekte der Risikobehandlung und Maßnahmenplanung betrachtet, um eine effektive Risikominderung zu gewährleisten.

Risikobehandlung

Die Risikobehandlung umfasst die Auswahl und Umsetzung geeigneter Maßnahmen zur Reduzierung oder Vermeidung der identifizierten Risiken. Dabei sollten folgende Schritte berücksichtigt werden:

Maßnahmenauswahl

Auf Grundlage der Risikobewertungsergebnisse werden Maßnahmen zur Risikominderung identifiziert. Hierbei ist es wichtig, dass die ausgewählten Maßnahmen angemessen sind, um die identifizierten Risiken zu adressieren. Die Maßnahmen können technischer, organisatorischer oder personeller Natur sein und sollten den Schutzbedarf der Assets berücksichtigen.

Maßnahmenumsetzung

Nach der Auswahl der Maßnahmen erfolgt die Umsetzung in der Praxis. Es müssen konkrete Handlungspläne entwickelt werden, um die Maßnahmen zu implementieren. Hierbei sollten Zuständigkeiten, Zeitpläne und Ressourcen klar definiert werden, um eine effektive Umsetzung zu gewährleisten.

Überprüfung der Maßnahmenwirksamkeit

Es ist wichtig, regelmäßig zu überprüfen, ob die implementierten Maßnahmen die gewünschte Wirkung erzielen. Eine kontinuierliche Überwachung und Bewertung der Maßnahmen ermöglicht es, Schwachstellen oder mögliche Verbesserungspotenziale zu identifizieren und entsprechende Anpassungen vorzunehmen.

Maßnahmenplanung

Die Maßnahmenplanung ist ein zentraler Aspekt der Risikobehandlung. Ein gut durchdachter Maßnahmenplan dient dazu, die identifizierten Risiken effektiv zu adressieren und einen klaren Fahrplan für deren Umsetzung zu bieten. Bei der Planung der Maßnahmen sollten folgende Aspekte berücksichtigt werden:

Priorisierung der Maßnahmen

Es ist wichtig, die Maßnahmen entsprechend ihrer Priorität zu ordnen. Hierbei können verschiedene Faktoren wie die Bewertung der Risiken, die potenziellen Auswirkungen und die Ressourcenverfügbarkeit berücksichtigt werden. Dies ermöglicht es, die begrenzten Ressourcen effizient einzusetzen und die Risikominderung gezielt voranzutreiben.

Zeitliche Planung

Eine klare zeitliche Planung ist wesentlich, um die Umsetzung der Maßnahmen effektiv zu steuern. Es sollten konkrete Zeitpläne festgelegt werden, die realistische Fristen für die Umsetzung der Maßnahmen vorsehen. Dies hilft dabei, die Fortschritte zu überwachen und sicherzustellen, dass die Maßnahmen fristgerecht abgeschlossen werden.

Ressourcenplanung

Die Planung der Ressourcen ist ein weiterer wichtiger Aspekt der Maßnahmenplanung. Es sollten die erforderlichen personellen, finanziellen und technischen Ressourcen identifiziert und bereitgestellt werden, um eine erfolgreiche Umsetzung der Maßnahmen zu gewährleisten.

Kommunikation und Stakeholder-Management

Die Kommunikation der Maßnahmenplanung und der damit verbundenen Risikobehandlung ist entscheidend, um das Verständnis, die Akzeptanz und die Unterstützung der relevanten Stakeholder zu gewinnen. Eine klare und transparente Kommunikation ermöglicht es, die Bedeutung der Risikobehandlung zu vermitteln und die Zusammenarbeit aller Beteiligten zu fördern.

Dieses Kapitel hat die Risikobehandlung und Maßnahmenplanung innerhalb der Risikoanalyse behandelt. Es wurden die Schritte der Risikobehandlung erläutert, wie die Maßnahmenauswahl, -umsetzung und -überprüfung. Zudem wurden Aspekte der Maßnahmenplanung, wie Priorisierung, zeitliche und ressourcenbezogene Planung sowie die Bedeutung der Kommunikation und des Stakeholder-Managements, betrachtet. Durch eine effektive Risikobehandlung und eine gut geplante Maßnahmenumsetzung können Organisationen ihre Risiken gezielt reduzieren und eine robuste Informationssicherheit erreichen.

Überwachung und Aktualisierung der Risikoanalyse

Die Überwachung und Aktualisierung der Risikoanalyse ist ein kontinuierlicher Prozess, der sicherstellt, dass die identifizierten Risiken angemessen bewertet und behandelt werden. In diesem Kapitel wird erläutert, wie die Überwachung und Aktualisierung der Risikoanalyse durchgeführt wird und welche Aspekte dabei zu berücksichtigen sind. Es werden Methoden und Ansätze vorgestellt, um Veränderungen in der Risikolage zu erkennen und die Risikoanalyse entsprechend anzupassen.

Bedeutung der Überwachung und Aktualisierung der Risikoanalyse

Die Überwachung und Aktualisierung der Risikoanalyse ist von großer Bedeutung, da sich die Risikolage kontinuierlich ändern kann. Neue Bedrohungen können auftreten, Schwachstellen können entdeckt werden und der Schutzbedarf von Assets kann sich verändern. Durch eine regelmäßige Überwachung und Aktualisierung der Risikoanalyse können Organisationen sicherstellen, dass ihre Sicherheitsmaßnahmen weiterhin angemessen sind und potenzielle Risiken effektiv behandelt werden.

Überwachung der Risikolage

Die Überwachung der Risikolage beinhaltet die kontinuierliche Erfassung und Bewertung von Informationen über Bedrohungen, Schwachstellen und den Schutzbedarf von Assets. Dies kann durch verschiedene Maßnahmen erfolgen, wie beispielsweise:

- Aktualisierung von Bedrohungs- und Schwachstelleninformationen: Durch den regelmäßigen Bezug von Informationen aus relevanten Quellen, wie Sicherheitswarnungen, Fachpublikationen und Sicherheitsnetzwerken, können neue Bedrohungen und Schwachstellen identifiziert und bewertet werden.
- Durchführung von Sicherheitsaudits und -prüfungen: Regelmäßige Audits und Prüfungen ermöglichen es, den aktuellen Sicherheitsstatus zu überprüfen und potenzielle Schwachstellen oder Mängel aufzudecken.
- Incident Management: Die Erfassung und Analyse von Sicherheitsvorfällen bietet wertvolle Einblicke in die Risikolage und kann dazu beitragen, vorhandene Schwachstellen zu erkennen und zu beheben.

Aktualisierung der Risikoanalyse

Auf Grundlage der gewonnenen Informationen und Erkenntnisse sollten regelmäßige Aktualisierungen der Risikoanalyse durchgeführt werden. Dabei können folgende Aspekte berücksichtigt werden:

- Neubewertung von Risiken: Die Bewertung der Risiken sollte regelmäßig überprüft und aktualisiert werden, um Veränderungen in der Risikolage zu berücksichtigen. Neue Bedrohungen oder Schwachstellen können zu einer Anpassung der Risikoeinschätzung führen.
- Aktualisierung von Maßnahmen: Die Wirksamkeit der implementierten Maßnahmen sollte überwacht und bei Bedarf aktualisiert werden. Neue Schutzmaßnahmen können erforderlich sein, um auf veränderte Risiken zu reagieren oder um Mängel in bestehenden Maßnahmen zu beheben.
- Kommunikation und Sensibilisierung: Die Ergebnisse der aktualisierten Risikoanalyse sollten effektiv kommuniziert werden, um das Bewusstsein für Risiken und die Notwendigkeit von Sicherheitsmaßnahmen zu stärken. Mitarbeiter und andere Stakeholder sollten über aktuelle Risiken und geeignete Schutzmaßnahmen informiert werden.

Kontinuität des Risikomanagements

Die Überwachung und Aktualisierung der Risikoanalyse ist ein kontinuierlicher Prozess, der parallel zu anderen Aktivitäten des Risikomanagements durchgeführt werden sollte. Dies beinhaltet die kontinuierliche Verbesserung der Risikobewertungsmethoden, die Anpassung von Maßnahmenplänen und die Integration der Risikoanalyse in den gesamten Sicherheitsprozess.

Dieses Kapitel hat die Bedeutung der Überwachung und Aktualisierung der Risikoanalyse hervorgehoben. Es wurden verschiedene Aspekte der Überwachung der Risikolage und der Aktualisierung der Risikoanalyse behandelt. Durch eine regelmäßige Überwachung und Aktualisierung können Organisationen sicherstellen, dass ihre Sicherheitsmaßnahmen aktuell und angemessen sind und potenzielle Risiken effektiv behandelt werden.

Beispiel einer Risikoanalyse

Lassen Sie uns eine Risikoanalyse für einen Webserver unserer fiktiven SZ Robotik GmbH durchführen. Die gewählte elementare Gefährdung ist ein unbefugter Zugriff auf den Webserver, und als bereits umgesetzte Maßnahme nehmen wir an, dass eine Firewall implementiert wurde. Als noch umzusetzende Maßnahme könnten wir die regelmäßige Aktualisierung der Webserver-Software betrachten.

Risikomatrix für die Bewertung:

Eintrittshäufigkeit/Auswirkung	Gering	Mittel	Hoch
Selten	Niedriges Risiko	Niedriges Risiko	Mittleres Risiko
Gelegentlich	Niedriges Risiko	Mittleres Risiko	Hohes Risiko
Häufig	Mittleres Risiko	Hohes Risiko	Hohes Risiko

TAB. 4 RISIKOMATRIX

Tabelle, um die Risikoanalyse durchzuführen:

Risiko	Eintrittshäufigkeit	Auswirkung	Risiko (vor Maßnahme)	Risikobehandlung	Eintrittshäufigkeit (vor Maßnahme)	Auswirkung (vor Maßnahme)	Risiko (vor Maßnahme)
Unbefugter Zugriff auf den Webserver	Mittel	Hoch	Hohes	Firewall	Mittel	Hoch	Hoch

TAB 5. TABELLE ZUR RISIKOANALYSE

Die Eintrittshäufigkeit des unbefugten Zugriffs auf den Webserver wird als mittel bewertet, während die Auswirkung als hoch bewertet wird. Vor der Implementierung der Firewall besteht daher ein hohes Risiko. Durch die Implementierung der Firewall als Risikobehandlungsmethode wird die Eintrittshäufigkeit auf niedrig reduziert und die Auswirkung auf mittel gesenkt. Dadurch wird das Risiko nach der Maßnahme auf ein niedriges Niveau reduziert.

Nun fügen wir die noch umzusetzende Maßnahme der regelmäßigen Aktualisierung der Webserver-Software hinzu:

Risiko	Eintrittshäufigkeit	Auswirkung	Risiko (nach Maßnahme)	Risikobehandlung	Eintrittshäufigkeit (nach Maßnahme)	Auswirkung (nach Maßnahme)	Risiko (nach Maßnahme)
Unbefugter Zugriff auf den Webserver	Mittel	Hoch	Hohes	Firewall, regelmäßige Aktualisierung der Software	Niedrig	Mittel	Niedrig

TAB 6. TABELLE ZUR RISIKOANALYSE

Durch die regelmäßige Aktualisierung der Webserver-Software wird die Eintrittshäufigkeit auf niedrig reduziert, da bekannte Schwachstellen durch Software-Updates behoben werden. Die Auswirkung bleibt mittel, da ein unbefugter Zugriff immer noch potenzielle Auswirkungen haben kann. Insgesamt wird das Risiko jedoch auf ein niedriges Niveau reduziert.

Bitte beachten Sie, dass dies nur ein Beispiel ist und eine umfassendere Risikoanalyse eine detailliertere Betrachtung verschiedener Risiken und Maßnahmen erfordern würde.

Kennzahlen (KPIs)

Die Verwendung von Key Performance Indikatoren (KPIs) gemäß den Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) kann Unternehmen dabei unterstützen, die Informationssicherheit effektiv zu messen, zu überwachen und zu verbessern. KPIs dienen als quantifizierbare Messgrößen, um den Fortschritt und den Erfolg von Sicherheitsmaßnahmen zu verfolgen. Durch die Anwendung der BSI-KPIs können Unternehmen den Reifegrad ihrer Informationssicherheit bewerten, Schwachstellen identifizieren und Prioritäten setzen. Die Verwendung der KPIs ermöglicht es

Unternehmen, fundierte Entscheidungen zu treffen, Ressourcen effizient einzusetzen und Risiken proaktiv zu managen. Darüber hinaus unterstützen die KPIs Unternehmen dabei, ihre Informationssicherheitsmaßnahmen kontinuierlich zu verbessern, indem sie eine regelmäßige Überprüfung und Anpassung ermöglichen. Die Verwendung der BSI-KPIs fördert somit eine systematische und strukturierte Vorgehensweise im Bereich der Informationssicherheit und trägt dazu bei, die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Informationen und IT-Systeme zu gewährleisten.

Die Systembausteine aus dem BSI-Grundschutzkompendium können als Rahmenwerk dienen, um die relevanten Aspekte der Informationssicherheit abzudecken und den Einsatz von Key Performance Indicators (KPIs) zu unterstützen. Die Systembausteine stellen verschiedene Bereiche der Informationssicherheit dar und enthalten Empfehlungen für geeignete Maßnahmen und Kontrollen.

Bei der Zuordnung von KPIs zu den Systembausteinen kann man die KPIs als Metriken betrachten, die den Erfolg oder die Wirksamkeit der in den Systembausteinen empfohlenen Maßnahmen messen. Einige KPIs können direkt mit einem bestimmten Systembaustein in Verbindung stehen, während andere KPIs mehrere Systembausteine abdecken können.

Die Zuordnung der KPIs zu den Systembausteinen hängt von den spezifischen Zielen und Anforderungen des Unternehmens ab. Es ist wichtig, die relevanten Systembausteine zu identifizieren, die die Bereiche der Informationssicherheit abdecken, die für das Unternehmen am wichtigsten sind. Anschließend können passende KPIs ausgewählt werden, die die Wirksamkeit und den Fortschritt in Bezug auf die in den entsprechenden Systembausteinen empfohlenen Maßnahmen messen.

Durch die Zuordnung von KPIs zu den Systembausteinen wird ein ganzheitlicher Ansatz für die Bewertung und das Monitoring der Informationssicherheit ermöglicht. Dies erleichtert die Identifizierung von Verbesserungspotenzialen, die Priorisierung von Maßnahmen und die Steuerung der Informationssicherheitsstrategie im Einklang mit den Empfehlungen des BSI-Grundschutzes.

Zuordnung der Systembausteine

Um die entsprechenden Systembausteine zu identifizieren, die zu den ausgewählten Key Performance Indicators (KPIs) passen, können Sie die folgenden Schritte durchführen:

1. Analysieren Sie die KPIs: Betrachten Sie die ausgewählten KPIs im Detail und verstehen Sie, welchen Aspekt der Informationssicherheit sie messen sollen. Berücksichtigen Sie dabei die Ziele und Anforderungen des Unternehmens.
2. Konsultieren Sie das BSI-Grundschutzkompendium: Das BSI-Grundschutzkompendium enthält eine umfassende Sammlung von Systembausteinen, die verschiedene Aspekte der Informationssicherheit abdecken. Überprüfen Sie die Beschreibungen der Systembausteine und prüfen Sie, welche Bereiche der Informationssicherheit sie ansprechen.
3. Vergleichen Sie die KPIs mit den Systembausteinen: Überprüfen Sie die Beschreibungen der Systembausteine im BSI-Grundschutzkompendium und prüfen Sie, ob sie die Aspekte abdecken, die von den KPIs erfasst werden sollen. Suchen Sie nach Übereinstimmungen in Bezug auf die Ziele, Kontrollen oder Maßnahmen, die in den Systembausteinen empfohlen werden.
4. Identifizieren Sie passende Systembausteine: Basierend auf der Analyse der KPIs und der Überprüfung der Systembausteine finden Sie diejenigen, die am besten zu den gemessenen

Aspekten passen. Identifizieren Sie die Systembausteine, die Empfehlungen oder Kontrollen enthalten, die direkt mit den gemessenen KPIs zusammenhängen.

5. Überprüfen Sie die Relevanz: Stellen Sie sicher, dass die identifizierten Systembausteine und deren Empfehlungen tatsächlich auf die spezifischen Bedürfnisse und Anforderungen Ihres Unternehmens zutreffen. Überprüfen Sie auch, ob weitere spezifische Richtlinien oder Vorgaben vorhanden sind, die berücksichtigt werden müssen.

Durch die Durchführung dieser Schritte können Sie die passenden Systembausteine identifizieren, die mit den ausgewählten KPIs in Verbindung stehen. Diese Zuordnung ermöglicht es Ihnen, die relevanten Aspekte der Informationssicherheit gemäß den Empfehlungen des BSI-Grundschutzes zu messen und zu überwachen.

Hier sind einige Vorschläge für Key Performance Indicators (KPIs) für unsere fiktive SZ Robotik GmbH, zusammen mit den entsprechenden Bausteinen aus dem BSI-Grundschutzkompendium:

- Durchschnittliche Reaktionszeit auf Kundensupport-Anfragen:
    - Baustein: CON 1.2 (Service Level Management)
    - Baustein: ORG 4.2 (Kommunikation und Zusammenarbeit)
- Anzahl der fehlerhaften Produkte pro Monat:
    - Baustein: SYS 1.1 (Verantwortung der Geschäftsführung)
    - Baustein: SYS 1.2 (Informationssicherheitskoordination)
- Produktivität der Mitarbeiter pro Stunde:
    - Baustein: ORG 1.1 (Sicherheitsorganisation)
    - Baustein: ORG 1.2 (Rollen und Zuständigkeiten)
- Auslastung der Produktionsanlagen:
    - Baustein: PHY 1.2 (Standort- und Gebäudesicherung)
    - Baustein: PHY 2.1 (Räumliche Trennung)
- Kundenbindung:
    - Baustein: CON 1.1 (Kundenbeziehungsmanagement)
    - Baustein: CON 1.4 (Beschwerdemanagement)
- Mitarbeiterzufriedenheit:
    - Baustein: PER 1.2 (Mitarbeitergewinnung und -bindung)
    - Baustein: PER 3.2 (Weiterbildung und Schulungen)

Diese Vorschläge für KPIs basieren auf den zuvor besprochenen Aspekten unserer fiktiven SZ Robotik GmbH. Es ist wichtig, die individuellen Bedürfnisse und Ziele des entsprechenden Unternehmens zu berücksichtigen, um geeignete KPIs zu definieren. Die genannten Bausteine aus dem BSI-Grundschutzkompendium bieten Orientierungspunkte für die Einbettung der KPIs in die Informationssicherheitsstrategie und -Maßnahmen der SZ Robotik GmbH.

In unserer fiktiven Firma SZ Robotik GmbH, die sich auf die Herstellung und Entwicklung von fortschrittlicher Robotertechnologie spezialisiert hat, sind Key Performance Indicators (KPIs) von entscheidender Bedeutung, um die Qualitätssicherung zu gewährleisten und fortlaufend zu verbessern. Ein konkreter Anwendungsbereich wäre beispielsweise die Produktion von Roboterarmen. Hier könnten KPIs wie "Erstpassrate", die den Prozentsatz der Produkte misst, die ohne Nachbesserungen oder Ausschuss den Produktionsprozess durchlaufen, oder "Fehlerdichte",

welche die Anzahl der erkannten Fehler pro Inspektionseinheit misst, zum Einsatz kommen. Zudem könnte ein KPI wie "Zeit bis zur Fehlerbehebung" verwendet werden, um die Effizienz der Fehlerbehebungsprozesse zu messen. Diese KPIs ermöglichen es SZ Robotik GmbH, qualitative Leistungen in messbare Werte zu übersetzen, wodurch Mängel schnell erkannt und behoben werden können. Darüber hinaus bieten sie wertvolle Daten für kontinuierliche Verbesserungsinitiativen und helfen dabei, die Qualität der Roboterarme auf einem hohen Niveau zu halten und gleichzeitig die Produktivität und Effizienz des Unternehmens zu steigern.

Notfallmanagement

Notfallkonzepte

Besteht aus zwei Komponenten:

1. Einem Notfallvorsorgekonzept für den präventiven Schutz gegen Notfälle und deren Auswirkungen.
2. Einem Notfallhandbuch mit Handlungsanleitungen für Notfälle und Krisen.

Phasen der Notfallbewältigung

1. Notfall melden
2. Sofortmaßnahmen ergreifen
3. Geschäftsfortführung, Wiederanlauf und Wiederherstellung
4. Rückführung und Nacharbeiten
5. Notfallbewältigung analysieren

Bestandteile

- Business Impact Analyse, mit der die kritischen Geschäftsprozesse und Ressourcen sowie Kenngrößen für deren Wiederanlauf nach Unterbrechungen ermittelt werden.
- Eine Risikoanalyse auf die kritischen Prozesse und deren Ressourcen.
- Die Entwicklung von Optionen für die zu verfolgende Kontinuitätsstrategie, um Alternativen für die Umsetzung von Notfall- und Notfallvorsorgemaßnahmen aufzuzeigen.
- Erstellung des Konzeptes.

Abgrenzung von Begrifflichkeiten

Im Kontext des Bundesamts für Sicherheit in der Informationstechnik (BSI) können die Begriffe "Ereignis", "Vorfall", "Störung", "Notfall" und "Krise" wie folgt abgegrenzt werden:

- Ereignis: Ein Ereignis im BSI-Kontext bezieht sich auf ein bestimmtes Vorkommnis oder eine Handlung, das oder die im Zusammenhang mit der Informationssicherheit steht. Es kann sich um geplante oder ungeplante Aktivitäten handeln, die Auswirkungen auf die IT-Sicherheit haben können. Ereignisse können beispielsweise die Einführung neuer Technologien, Systemupdates, geplante Wartungsarbeiten oder andere Veränderungen in der IT-Umgebung umfassen.
- Vorfall: Ein Vorfall im BSI-Kontext ist ein unerwünschtes oder unerwartetes Ereignis, das die Sicherheit, Integrität oder Verfügbarkeit von Informationen oder IT-Systemen gefährden kann. Ein Vorfall kann beispielsweise eine Sicherheitsverletzung, ein Angriff, eine Datenpanne oder eine nicht autorisierte Zugriffsversuch sein. Die Meldung und das Management von Vorfällen sind wichtige

Aspekte des IT-Sicherheitsmanagements, um die Auswirkungen zu minimieren und Gegenmaßnahmen zu ergreifen.

- Störung: Eine Störung im BSI-Kontext bezieht sich auf eine Beeinträchtigung oder Unterbrechung der normalen Funktionsweise von IT-Systemen, Diensten oder Infrastrukturen. Störungen können durch technische Ausfälle, Fehlfunktionen, Fehler in der Konfiguration oder andere Gründe verursacht werden. Das BSI legt großen Wert darauf, Störungen zu analysieren, Maßnahmen zur Wiederherstellung zu ergreifen und präventive Maßnahmen zu entwickeln, um solche Störungen in Zukunft zu verhindern.
- Notfall: Ein Notfall im BSI-Kontext ist eine akute, kritische Situation, die schnelle und koordinierte Maßnahmen erfordert, um die IT-Sicherheit zu gewährleisten oder Schaden zu begrenzen. Notfälle können durch Sicherheitsvorfälle, Naturkatastrophen, technische Ausfälle oder andere Ereignisse verursacht werden. Das BSI legt besonderen Wert auf die Planung, das Management und die Reaktion auf IT-Notfälle, um eine effektive Krisenbewältigung sicherzustellen.
- Krise: Eine Krise im BSI-Kontext bezieht sich auf eine außergewöhnliche und schwerwiegende Bedrohung oder Störung der Informationssicherheit, die das normale Funktionieren von Organisationen oder Infrastrukturen gefährdet. Krisen können verschiedene Ursachen haben, wie beispielsweise massive Cyberangriffe, weitreichende Sicherheitsverletzungen oder andere Ereignisse mit erheblichen Auswirkungen auf die IT-Sicherheit. Das BSI spielt eine wichtige Rolle bei der Koordination und Unterstützung von Organisationen bei der Bewältigung von IT-Krisen, indem es Handlungsempfehlungen, Informationen und Unterstützung bereitstellt.
- Katastrophe: Eine Katastrophe im Kontext des Bundesamts für Sicherheit in der Informationstechnik (BSI) bezieht sich auf eine außergewöhnliche, weitreichende und schwerwiegende Bedrohung oder Störung, die die Informationssicherheit eines Landes oder einer Region erheblich beeinträchtigt. Eine Katastrophe kann verschiedene Ursachen haben, wie zum Beispiel ein umfangreicher und koordinierter Cyberangriff, der zu schweren Schäden an kritischen Infrastrukturen führt, oder eine Naturkatastrophe, die die Kommunikations- und IT-Systeme stark beeinträchtigt. Im Unterschied zu einer Krise handelt es sich bei einer Katastrophe um ein Ereignis von noch größerem Ausmaß und höherer Schwere, das eine umfassende Mobilisierung von Ressourcen, Maßnahmen und Koordination erfordert, um die Folgen zu bewältigen und die Informationssicherheit wiederherzustellen.

Beispielszenario

Es folgt eine Beschreibung der Sofortmaßnahmen für eine Gefährdung (gemäß Gefährdungskatalog) am Beispiel der zuvor durchgeführten Strukturanalyse unserer fiktiven SZ Robotik GmbH.

Die Maßnahmen wurden entsprechend den Empfehlungen und Kontrollen aus den jeweiligen Bausteinen abgeleitet. Die genannten Bausteine decken verschiedene Aspekte der Informationssicherheit ab, die im Zusammenhang mit dem Schutz vor unbefugtem physischem Zugriff relevant sind.

Sofortmaßnahme	**Systembaustein**
Zugangskontrolle verstärken	Baustein: PHY 1.2 (Standort- und Gebäudesicherung)
Überwachungssystem installieren	Baustein: PHY 1.3 (Sicherung von Gebäudezugängen)

Alarmierungssystem einrichten	Baustein: INF 1.2 (Informationssicherheitsmanagement)
Sensible Informationen sichern	Baustein: INF 1.2 (Informationssicherheitsmanagement)
Schulungen und Sensibilisierung der Mitarbeiter	Baustein: ORG 3.4 (Schulung, Sensibilisierung und Kommunikation)

TAB. 7 ZUORDNUNG DER SYSTEMBAUSTEINE ZU DEN ENTSPRECHENDEN MAßNAHMEN

Beschreibung: Gemäß der Strukturanalyse haben wir den Serverraum als kritischen Systembaustein identifiziert. Eine mögliche Gefährdung, die den Serverraum betrifft, ist der unbefugte physische Zugriff. Dies könnte durch den Eintritt einer unbefugten Person in den Serverraum erfolgen, sei es absichtlich oder versehentlich.

Sofortmaßnahmen: Um auf diese Gefährdung angemessen zu reagieren und den unbefugten physischen Zugriff auf den Serverraum zu verhindern, sollten folgende Sofortmaßnahmen ergriffen werden:

- **Zugangskontrolle verstärken**: Wir überprüfen die Zugangsmechanismen zum Serverraum und stellen sicher, dass nur autorisierte Personen Zugang haben. Dies kann durch den Einsatz von Zugangskarten, Biometrie oder anderen geeigneten physischen Zugangskontrollmaßnahmen erreicht werden.
- **Überwachungssystem installieren**: Wir implementieren ein Überwachungssystem, dass den Serverraum rund um die Uhr überwacht. Dies kann die Installation von Überwachungskameras, Bewegungsmeldern und Zugriffskontrollprotokollierung umfassen. Dadurch wird ein frühzeitiges Erkennen und Melden von unbefugten Zugriffen ermöglicht.
- **Alarmierungssystem einrichten**: Wir installieren ein Alarmierungssystem, das aktiviert wird, wenn ein unbefugter Zugriff auf den Serverraum festgestellt wird. Dies kann akustische oder visuelle Alarme umfassen, um Mitarbeiter und Sicherheitspersonal auf den Vorfall aufmerksam zu machen.
- **Sensible Informationen sichern**: Wir stellen sicher, dass sensible Informationen im Serverraum angemessen gesichert sind. Dies kann durch die Verwendung von verschlossenen Schränken oder Safes für Backup-Medien, Passwortschutz für Server- und Netzwerkausrüstung oder andere geeignete Sicherheitsvorkehrungen erreicht werden.
- **Schulungen und Sensibilisierung der Mitarbeiter**: Schulungen und Sensibilisierungsmaßnahmen für Mitarbeiter sind unentbehrlich, um das Bewusstsein für die Bedeutung des physischen Schutzes des Serverraums zu schärfen. Dies beinhaltet Anweisungen zur Wahrung der Vertraulichkeit, zur Meldung verdächtiger Aktivitäten und zur korrekten Nutzung der Zugangskontrollsysteme.

Diese Sofortmaßnahmen dienen dazu, den unbefugten physischen Zugriff auf den Serverraum zu minimieren und die Sicherheit der darin befindlichen IT-Systeme und Daten zu gewährleisten. Sie sollten umgesetzt werden, um das Risiko eines solchen Vorfalls zu reduzieren und den Schutz des Serverraums zu verbessern.

Business Impact Analyse

Eine Business Impact Analyse (BIA) trägt dazu bei, die Auswirkungen von potenziellen Störungen oder Schadensfällen auf die Geschäftstätigkeit eines Unternehmens zu bewerten. Sie hilft bei der Identifizierung und Priorisierung von Geschäftsbereichen, Prozessen, Systemen und Ressourcen, die für den kontinuierlichen Geschäftsbetrieb und die Wiederherstellung nach einer Störung wesentlich sind.

Die BIA wird verwendet, um den Schutzbedarf verschiedener Geschäftsbereiche zu bestimmen und die erforderlichen Maßnahmen für die Geschäftskontinuität zu identifizieren. Sie ermöglicht es Unternehmen, Risiken zu identifizieren, potenzielle Auswirkungen zu bewerten und geeignete Vorkehrungen zu treffen, um die Geschäftskontinuität zu gewährleisten.

Die BIA umfasst in der Regel die folgenden Schritte:

- Identifizierung von Geschäftsprozessen und Ressourcen: Erfassen Sie alle wichtigen Geschäftsprozesse, Systeme, Anwendungen, Informationen und Ressourcen, die für den Geschäftsbetrieb relevant sind.
- Bewertung der Auswirkungen: Analysieren Sie die Auswirkungen von Störungen oder Schadensfällen auf diese Geschäftsprozesse und Ressourcen. Dies umfasst finanzielle Auswirkungen, operationelle Konsequenzen, rechtliche Aspekte, Auswirkungen auf Kunden und Ruf des Unternehmens.
- Bewertung der Wiederherstellungszeit: Schätzen Sie die maximale tolerierbare Ausfallzeit für jeden Geschäftsprozess oder jede Ressource. Dies gibt an, wie schnell eine Wiederherstellung erfolgen muss, um negative Auswirkungen zu minimieren.
- Priorisierung und Schutzbedarf: Basierend auf den Ergebnissen der Auswirkungsanalyse und der Wiederherstellungszeitbewertung priorisieren Sie die Geschäftsprozesse und Ressourcen nach ihrem Schutzbedarf. Dies hilft bei der Festlegung von Maßnahmen und Ressourcenallokation für die Geschäftskontinuität.

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) betont die Bedeutung einer BIA im Rahmen des Risikomanagements und des Business Continuity Managements. Es empfiehlt Unternehmen, eine BIA durchzuführen, um ihre kritischen Geschäftsprozesse und Ressourcen zu identifizieren, den Schutzbedarf zu bestimmen und angemessene Maßnahmen zur Geschäftskontinuität umzusetzen.

Eine gut durchgeführte BIA ermöglicht es Unternehmen, Risiken zu reduzieren, auf Störungen vorbereitet zu sein und eine effektive Wiederherstellung nach einem Vorfall zu gewährleisten. Sie bildet die Grundlage für die Entwicklung von Notfallplänen, die Implementierung von Sicherheitsmaßnahmen und die kontinuierliche Überwachung und Anpassung der Geschäftskontinuitätsstrategie.

QUELLENERZEICHNIS

1. [^1] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik) https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf