OPITZ CONSULTING
SOFTWARE

SICHERE SOFTWARE ENTWICKELN

IT-Security entlang der PRINCE2-Methodik

How-to Guide

WARUM DIESER HOW-TO GUIDE?

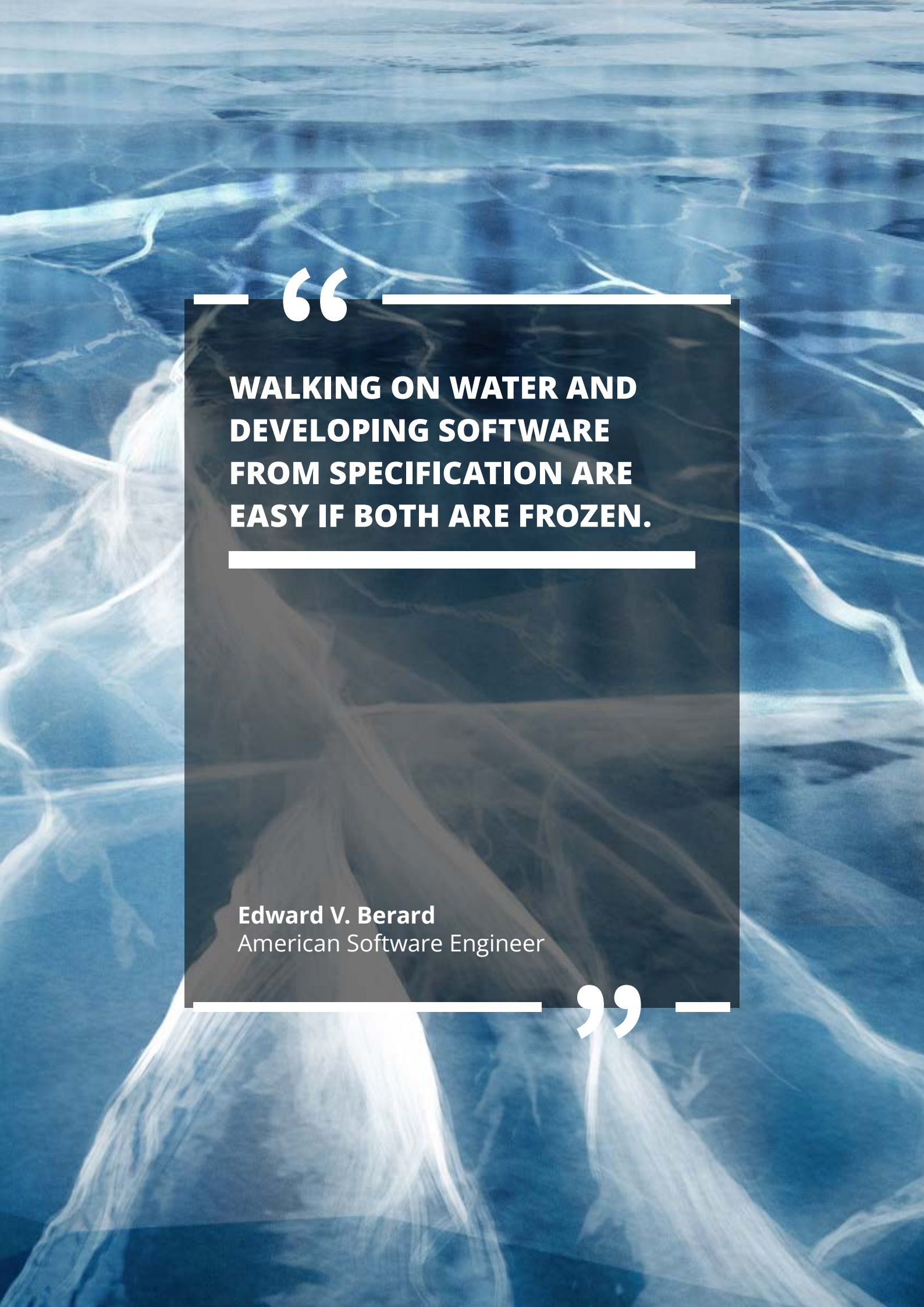
Der aktuelle Bericht des BSI zur Lage der Informationssicherheit in Deutschland zeichnet nach wie vor ein düsteres Bild und macht auf die vielfältige Bedrohungslage aufmerksam. Resiliente Systeme sind gefragt, um die Werte eines Unternehmens zu schützen. Das betrifft insbesondere die Softwareentwicklung.

Dieser How-to Guide zeigt, wie Sicherheit in IT-Projekten pragmatisch und dennoch wirkungsvoll umgesetzt werden kann.

ÜBER DEN AUTOR

Andreas Becht begann seine Karriere vor über 20 Jahren als Entwickler und Berater. Später übernahm er Projektleitungsrollen und leitet heute den Bereich Software Consulting. Seine Leidenschaft liegt in der Umsetzung ganzheitlicher Digitalisierungsprojekte und der Entwicklung maßgeschneiderter IT-Lösungen. Andreas legt besonderen Wert auf den Faktor Mensch in Digitalisierungsprojekten und begleitet Teams in ihren Veränderungsprozessen.

#INHALTSVERZEICHNIS



WALKING ON WATER AND DEVELOPING SOFTWARE FROM SPECIFICATION ARE EASY IF BOTH ARE FROZEN.

Edward V. Berard
American Software Engineer

LAGE: ANGESPANNT BIS KRITISCH

LAGE: RESILIENZ ALS GEMEINSAME AUFGABE

Im Lagebericht zur IT-Sicherheit in Deutschland von 2024 stellt das Bundesamt für Sicherheit in der Informationstechnik (BSI) fest: „Die vier Dimensionen Bedrohungen, Angriffsflächen, Gefährdungen und Schadwirkungen zeigen eine immense negative Wirkung." Die entscheidende Dimension, um dem entgegenzutreten, sei Resilienz. „Resilienz lässt sich jedoch nicht allein und über Nacht umsetzen. Alle Beteiligten sind gefordert, zur Stärkung der Resilienz gegen Cyberkriminalität und IT-Sicherheitsvorfälle beizutragen." (BSI, 2025, https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html, abgerufen am 11.02.2025)

Dieser How-to-Guide beschäftigt sich mit der Frage, wie IT-Sicherheit bei der Erstellung von individuellen IT-Produkten im Projektkontext gewährleistet werden kann. Dafür nehmen wir die Perspektive eines externen IT-Dienstleisters in der Rolle des Projektpartners ein.

Wo liegt der Knackpunkt?

Das Projektgeschäfts ist schnelllebig, die Herausforderung an IT-Dienstleister hoch, das wirtschaftlichste Angebot abzugeben, um einen Projektauftrag zu gewinnen. Dazu kommt der Termindruck. Diese Lage erleichtert nicht gerade das Streben nach einem guten Niveau an IT-Sicherheit.

Sichere IT-Lösungen werden zwar als Liefergegenstand vorausgesetzt, dennoch lässt sich der damit verbundene Aufwand im Projekt oft schwer argumentieren.

Was können wir tun?

Wie das Lagebild des BSI zeigt, ist es dringend notwendig, sichere IT-Produkte herzustellen. Als IT-Dienstleister sind wir dazu in der Lage. Um Projekte erfolgreich durchzuführen, nutzen wir strukturierte und methodische Projektmanagementansätze. Diese gelten als Qualitätsmerkmal für eine erfolgreiche Projektdurchführung, Auch bei der IT-Sicherheit hilft ein strukturiertes Vorgehen, ein hohes Sicherheitsniveau zu erreichen.

Sichere IT-Lösungen werden vorausgesetzt, der damit verbundene Aufwand lässt sich aber oft schwer argumentieren.

Erprobte Standards und Methoden für IT-Sicherheit stehen bereit, müssen aber Schritt für Schritt mit dem Projektmanagementansatz zusammengeführt werden.

Ab Seite 12 gehen wir die Prozesse von PRINCE2 anhand einer Projektskizze durch, und zeigen, wie wir individuelle IT-Produkte sicher erstellen können.

WANN IST EIN IT-PRODUKT SICHER?

WANN IST EIN IT-PRODUKT SICHER?

„IT-Sicherheit hat die Aufgabe, Unternehmen und deren Werte [...] zu schützen und wirtschaftliche Schäden, die durch Vertraulichkeitsverletzungen, Manipulationen oder auch Störungen der Verfügbarkeit von Diensten des Unternehmens entstehen können, zu verhindern“

IT-Sicherheit hat die Aufgabe, Unternehmen und deren Werte zu schützen.

(Eckert, 2023, S. 1).

Unter **Informationssicherheit** wird auch die Sicherheit von Informationen vor unbefugtem Zugriff, Manipulation, Verwertung oder Zerstörung verstanden. Enger gefasste Begriffe sind **Datensicherheit**, die den Schutz personenbezogener Daten adressiert und **Datenschutz** in seiner juristischen Dimension, der die Grundlage für gelebte Datensicherheit bildet. Informationssicherheit, Datensicherheit und Datenschutz sind dabei losgelöst von IT-gestützter Datenverarbeitung zu verstehen und damit auch in der analogen Welt gültig und anwendbar. (Vgl. Kipker, 2023, S. 2-3)

Allgemeine Schutzziele

Der Informationssicherheit liegen allgemeine Schutzziele zugrunde. Klassische Schutzziele der Informationssicherheit:

- **Vertraulichkeit**: Informationen dürfen nur von autorisierten Personen eingesehen werden bzw. zugreifbar sein.
- **Integrität**: Informationen müssen vor unautorisierten Veränderungen geschützt werden.
- **Verfügbarkeit**: IT-Systeme müssen ihre Dienste verlässlich anbieten, damit Informationen funktionssicher verarbeitet werden können.
- **Datenschutz**: Personenbezogene Daten müssen geschützt, das Recht auf informationelle Selbstbestimmung gewahrt werden.
- **Authentizität**: Informationen müssen echt und bzgl. ihrer Urheberschaft nachvollziehbar sein.
- **Zurechenbarkeit/Nicht-Abstreitbarkeit**: Der Zugriff auf Informationen muss nachvollziehbar sein. Diesbezügliche Handlungen müssen verbindlich nachweisbar sein.

(vgl. Kipker, 2023, S. 6-8)

IT-Sicherheit zielt auf die Sicherheit und den Schutz von IT-Systemen ab, die Daten und die darin enthaltenen Informationen verarbeiten. Ein etwas weiter gefasster Begriff ist Cyber-Sicherheit. Cyber-Sicherheit umfasst IT-Sicherheit, Informationssicherheit und Datensicherheit von IT-Systemen in einem vernetzten digitalen Raum (Cyber-Raum) und kann als genereller Oberbegriff verstanden werden. (Vgl. Kipker, 2023, S. 2-3)

Um IT-Sicherheit wirkungsvoll umzusetzen, müssen wir den Wert der Assets ermitteln.

Der How-to Guide beschäftigt sich mit der Frage, wie sich IT-Sicherheit im Kontext individuell erstellter IT-Produkte hinreichend gewährleisten lässt. Gemeint sind hier Informations- und Datensicherheit.

Die Struktur von sicher

Aus der allgemeinen Definition von Informationssicherheit und IT-Sicherheit lässt sich eine **Struktur von sicher** bei der Entwicklung von IT-Produkten ableiten:

Ausgangspunkt der Informationssicherheit sind die Werte, die es in einer Organisation zu schützen gilt. Diese Werte werden auch als Assets bezeichnet.

Dabei handelt es ich um

- **Geschäftsprozesse und -funktionen,** also Wissen über Abläufe und Geschäftsmodell, Innovation oder Intellectual Property
- oder **Geschäftsdaten,** also alle Informationen in den Daten.

Im Falle von individuellen IT-Produkten, die Geschäftsprozesse digital abbilden, und Geschäftsdaten verarbeiten, sprechen wir von IT-Assets.

Dazu gehören:

- **IT-Produkt** bestehend aus Hosting, (z. B. Rechenzentrum, Hardware, physisches Netzwerk), **Infrastrukturkomponenten** (z. B. Betriebssysteme, Datenbanken, Container-Plattform) und **Softwarekomponenten** (z. B. Fachapplikation)
- **Betriebsumgebungen** für das IT-Produkt (z. B. Entwicklungsplattform, DevOps-Pipeline)
- **IT-Prozesse** für Konstruktion, Erstellung, Betrieb und Management des IT-Produkts
- **Organisation** mit Personen, Gruppen, und Rollen

Um IT-Sicherheit in individuellen IT-Produkten wirkungsvoll umzusetzen, müssen wir den Wert der Assets ermitteln.

IT-Assets müssen den Schutzbedarf der Assets, die sie digitalisieren, erfüllen. Das zu erreichende Sicherheitsniveau des IT-Produkts wird dabei als **Schutzbedarf des IT-Assets** bezeichnet.

Das Schutzbedarfe werden durch wirkungsvolle Schutzmaßnahmen umgesetzt. Dies sind Maßnahmen, die IT-Assets vor Bedrohungenschützen, und Schwachstellen absichern. Was wirkungsvoll und angemessen ist, muss unter Risikoabwägungen bewertet und entschieden werden.

Was wirkungsvoll und angemessen ist, muss unter Risikoabwägungen entschieden werden.

Die Compliance-Sicht

IT-Assets bestehen nicht nur aus schützenswerten technischen Komponenten eines IT-Produkts. Sie umfassen auch die Räumlichkeiten, in denen ein IT-Produkt entwickelt, betrieben und gesteuert wird. Ebenso die Prozesse, die bei Konstruktion, Bau und Betrieb des IT-Produkts zum Einsatz kommen.

Auch die beteiligten Personen und die Organisation als Ganzes sind IT-Assets.

Das auftraggebende Unternehmen unterliegt in aller Regel Compliance-Vorgaben, die sich aus der rechtlichen Einordnung der Organisation oder auch aus innerbetrieblichen Vorgaben ableiten. Ob diese Vorgaben relevant für das zu erstellende IT-Produkt sind, bleibt zu überprüfen.

Ein wichtiger Aspekt aus Compliance-Perspektive sind geltende Industrie- und Branchenstandards, Verordnungen oder Richtlinien, die Einfluss haben auf das Erreichung der Sicherheitsziele beim IT-Produkt und beim Vorgehen im Projekt. Beispiele für solche Compliance-Vorgaben sind das NIS2-Gesetz oder die DORA-Verordnung

Sicherheitsstandards

Im Bereich der Informationssicherheit gibt es zahlreiche nationale wie internationale Standards und Normen. Auf dem deutschen IT-Markt sind z. B. diese beiden häufig zu erfüllen:

- Zertifizierung nach **ISO/IEC 27001**
- Vorgehen nach **BSI IT-Grundschutz**

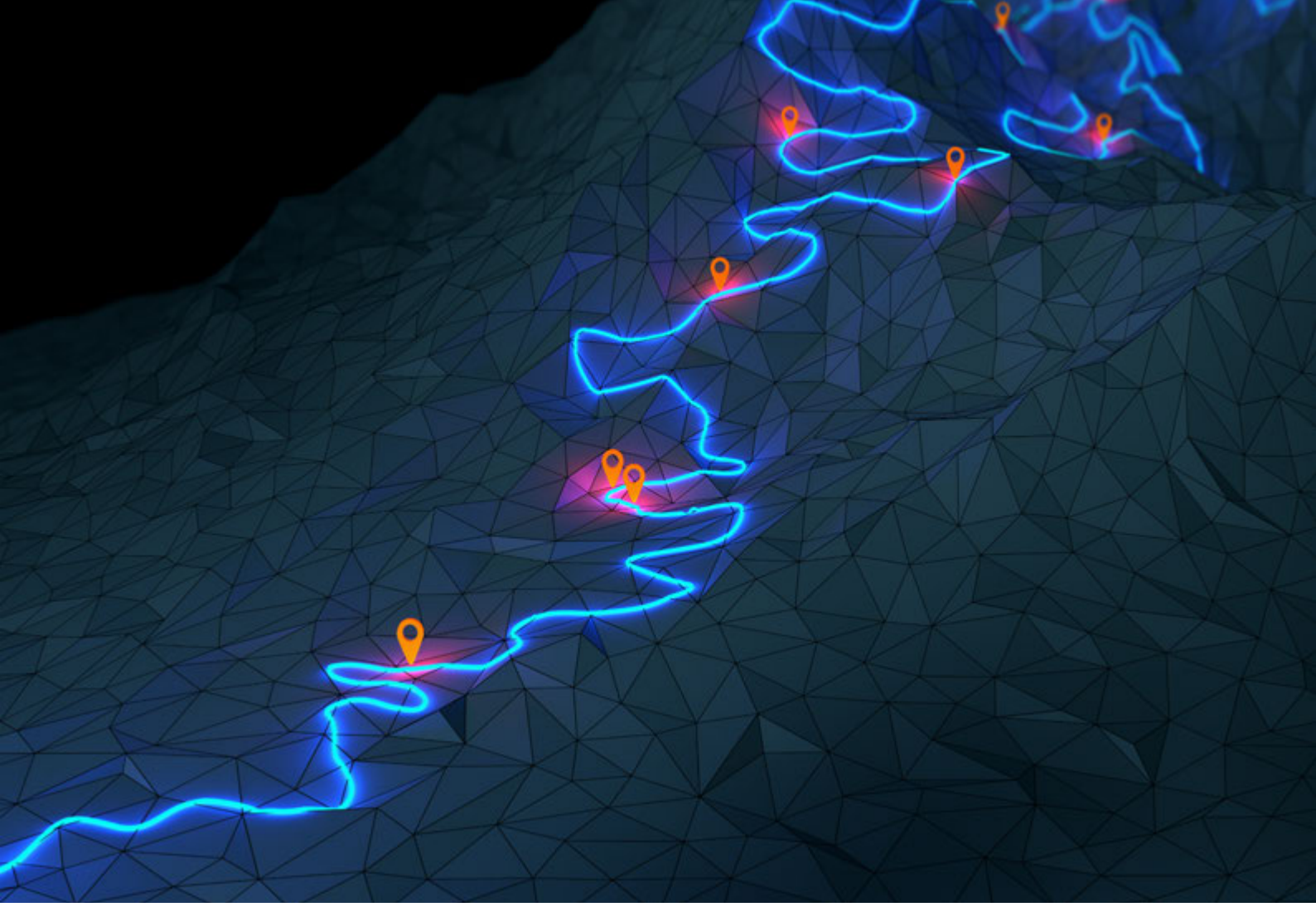
Die ISO/IEC 27000-Familie ist eine internationale Normenreihe und beinhaltet verschiedene Standards zur Informationssicherheit. So definiert die Norm **ISO/IEC 27001** die konkreten Anforderungen an ein Informationssicherheits-Managementsystem (ISMS) und gilt als De-facto-Standard für die Etablierung eines Informationssicherheitsmanagements in Organisationen. (Vgl. Kipker, 2023, S. 159)

Normen, Standards und ein Koffer voller Methoden.

Der IT-Grundschutz des BSI mit seinen Hauptwerken **BSI-Standards** und **IT-Grundschutz-Kompendium** stellt einen Koffer zur Verfügung mit konkreten Methoden für die Umsetzung von IT-Sicherheit in Organisationen sowie vordefinierte Bausteine für jeden Anwendungsbereich. Die Bausteine leiten aus typischen Bedrohungen und Risken für den jeweiligen Anwendungsbereich Anforderungen für ein angemessenes Sicherheitsniveau ab. (Vgl. Karg, 2022, S. 12-13)

ISO/IEC 27001 und IT-Grundschutz lassen sich kombinieren. Das heißt, beim Aufbau und der Weiterentwicklung eines ISMS berücksichtigen wir die ISO/IEC 27001 Norm und für konkrete Bedrohungs- und Risikoanalysen nutzen wir die Bausteine aus dem IT-Grundschutz. (Vgl. Karg, 2022, S. 12-13)

6 SCHRITTE ZUM SICHEREN IT-PRODUKT



6 SCHRITTE ENTLANG PRINCE2

PRINCE2 (Projects IN Controlled Environments) ist eine prozessorientierte Projektmanagementmethode, die weltweit verwendet wird. Sie segmentiert Projekte in kontrollierbare Phasen und definiert klare Rollen und Verantwortlichkeiten. Die Methode besteht aus bestimmten Prinzipien, Themen und Prozessen, die eine strukturierte Planung, Überwachung und Steuerung von Projekten ermöglichen. Dabei ist PRINCE2 sehr flexibel und kann an verschiedene Projektgrößen und -arten angepasst werden.

Für die Erzeugung von sicheren IT-Produkten gehen wir **6 Schritte** entlang von PRINCE2:

1. **Projekt vorbereiten**
2. **Projekt lenken**
3. **Projekt initiieren**
4. **Phasenübergang managen**
5. **Managen von Projektphase und Produktlieferung**
6. **Projekt abschließen**

1. PROJEKT VORBEREITEN

In der Projektvorbereitung werden das geplante Vorhaben begründet und die Strukturen für das Projekt geklärt. Aus Perspektive der IT-Sicherheit sind im ersten Schritt diese Dinge wichtig:

Strukturen und die verschiedenen Rollen im Projekt müssen geklärt werden.

- Rollenverständnis klären bezüglich Asset Owner, Product Supplier oder Service Provider in der Auftraggeber-/Auftragnehmer-Konstellation.
- Beauftragte für Informationssicherheit und Datenschutz (ISB und DSO) in die Projektorganisation integrieren.
- Assets und Schutzziele bestimmen.
- Interne oder externe Compliance-Vorgaben identifizieren.
- Security-Awareness-Maßnahmen einplanen.
- Unterstützung des Top-Managements einholen.

Rollen klären

Aus der Perspektive des Projektmanagements: Hier wird zwischen drei Interessensgruppen unterschieden: Auftraggebern, Nutzern und Lieferanten.

Im Projektmanagement ist es üblich, dass Vertreter dieser Interessensgruppen das Lenkungsgremium bilden. Wenn es um die Entwicklung individueller IT-Produkte geht, ist in der Praxis meist die IT die Auftraggeberin und verantwortet daher auch die externe Vergabe von Leistungen an die Lieferanten. Die Interessen der Benutzer vertreten meist Personen aus den betroffenen Fachbereichen.

Aus Perspektive der IT-Sicherheit: Hier ist das Rollenverständnis beim Auftraggeber teilweise anders gelagert. Er ist bemüht, Kompromisse zu finden zwischen Sicherheitsniveau und Funktion des Produkts auf der einen Seite und Risikobewusstsein, Kosten und Nutzen des IT-Produkts auf der anderen Seite. Entscheidungen zur IT-Sicherheit brauchen eine Instanz, die am Ende verantwortlich ist. Diese Instanz vertritt die Sicht des Eigentümers und Betreibers des IT-Produkts, bezieht aber auch die Sicht der Benutzer mit ein. Diese Rolle wird als **Asset Owner** bezeichnet. (Vgl. Kipker, 2023, S. 189)

Aus Sicht der Lieferanten: Hier geht es vor allem darum, Klarheit über die Rolle von Hersteller (Product Supplier) und Dienstleister (Service Provider) herzustellen.

Als Service Provider unterstützt der Dienstleister den Asset Owner, die IT-Sicherheit des beauftragten IT-Produkts zu gewährleisten. Der Dienstleister handelt in diesem Fall als beratender und ausführender Experte. Die Verantwortung für die IT-Sicherheit des Produkts trägt der Eigentümer. Als Product Supplier ist der Dienstleister hingegen vollumfänglich für die Qualität und die IT-Sicherheit des zu liefernden Produktes verantwortlich. (vgl. Kipker, 2023, S. 189)

Die Rollenausprägungen und die damit verbundenen Verantwortlichkeiten und Erwartungshaltungen bei den Beteiligten vorab zu klären, ist wichtig für die Sicherheit des zu entwickelnden IT-Produkts.

ISB und DSB einbinden

Auch die Einbindung von **Informationssicherheitsbeauftragten (ISB)** und **Datenschutzbeauftragten (DSB)** in die Projektorganisation ist in dieser frühen Phase essenziell.

Die Rolle ISB wird im IT-Grundschutz beschrieben. Damit hat sie eine wichtige Funktion für das Informationssicherheitsmanagementsystem des Auftraggebers. (Vgl. BSI, 2023a, S. 30)

Im Kontext eines IT-Projekts unterstützen ISB bei:

- Ausgestaltung der Sicherheitsanforderungen
- Bestimmung des notwendigen Sicherheitsniveaus
- Bewertung des erreichten Sicherheitsniveaus
- Definition des Geltungsbereiches von IT-Sicherheit für das konkrete Projektvorhaben

In der Projektvorbereitung ist die Einbindung von Datenschutzbeauftragten (DSB) essenziell.

Auch die Rolle der DSB ist wichtig. Sie ist Teil der Datenschutzgrundverordnung (vgl. Europäisches Parlament, 2016, Abschnitt 4). Ihre Einbindung ist insbesondere von Bedeutung bei:

- Analyse und Bewertung von Schutzmaßnahmen zur Datensicherheit
- Identifikation von Anforderungen aus Compliance-Regelungen
- Risikobewertung und Folgenabschätzung zum Datenschutz

Ohne die Einbindung von ISB und DSB gelingt weder die nachfolgende Sicherheitskonzeption für das IT-Produkt noch die Einbindung des IT-Produkts in das Informationssicherheitsmanagementsystems der Gesamtorganisation.

Bestimmung von Asset und Schutzbedarf

Teil der Projektvorbereitung nach PRINCE2 ist die Beschreibung des Projektgegenstands, in unserem Fall des IT-Produkts sowie der Entwurf eines ersten Business Cases. Auch für ein gutes Sicherheitskonzept ist die frühzeitige Bestimmung von Asset und Schutzbedarf enorm wichtig.

Es geht um die Frage, welchen Wert die Prozesse und die Informationen, die damit bearbeitet werden, für das Unternehmen besitzen.

Welche Geschäftsprozesse werden durch das Projektvorhaben digital abgebildet? Welche Geschäftsdaten werden mit dem IT-Produkt verarbeitet?

Dabei geht es immer um die Frage, welchen Wert die Geschäftsprozesse und die damit bearbeiteten Informationen für das Unternehmen besitzen.

Laut IT-Grundschutz teilt sich der Schutzbedarf in die Kategorien „Normal“, „Hoch“ und „Sehr hoch“. (Vgl. BSI, 2023b, S. 72-73)

Die Kategorisierung orientiert sich an den allgemeinen Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit. (Details in Anhang 1)

Da die Bestimmung des Assets und seines Werts eine wichtige Grundlage für die Sicherheitskonzeption darstellt, sollte sie auch in den Projektmanagement-Artefakten als Kernbestandteil der Produktbeschreibung und des Business Cases enthalten sein.

Compliance-Vorgaben

Zu den Aufgaben der Projektvorbereitung zählt auch die Analyse von Compliance-Anforderungen mit Relevanz für den Projektgegenstand. Die Compliance-Anforderungen sind für die Sicherheitskonzeption in späteren Projektphasen relevant. Sie helfen in diesem ersten Schritt aber auch, den Wert des Assets zu bestimmen, in dem sie Hinweise geben auf schützenswerte Informationen und Prozesse im Unternehmen.

Maßnahmen für Security Awareness

Informationssicherheit benötigt Standards und Normen. Vor allem aber braucht sie Menschen, die in der Organisation nach diesen agieren. Da das Bewusstsein für Informations- und IT-Sicherheit nicht bei allen Beteiligten vorausgesetzt werden kann, ist es wichtig, schon in der Projektvorbereitung unterstützende Maßnahmen einzuplanen.

Hier wird die initiale Projektorganisation definiert. Auch in allen folgenden Schritten sind Informations- und IT-Sicherheit Teil der Aufgabenstellung der Projektbeteiligten. Es empfiehlt sich daher, schon im Planungsentwurf die Stärkung des Sicherheitsbewusstseins durch geeignete Schulungsmaßnahmen als Aufgabenpaket zu berücksichtigen.

Unterstützung durch das Top-Management

Zuletzt gilt es in der Vorbereitungsphase, das Top-Management bzw. die Management-Hierarchiestufe, die der beauftragenden Organisationeinheit vorgesetzt ist, mit an den Tisch zu holen.

Denn: Bei Entscheidungen zur IT-Sicherheit sind vielfach organisatorische oder prozessuale Aspekte betroffen, die Auswirkung über die Projektgrenzen hinaus haben. Des Weiteren sind Risiken zu bewerten, Folgen abzuschätzen, und es ist über den Umgang mit Restrisiken zu entscheiden.

Das Bewusstsein des Top-Managements ist ein weiterer Erfolgsfaktor.

3 Faktoren für den Erfolg:

- Der Kommunikationskanal zum Top-Management funktioniert.
- Das Top-Management ist sich der Wichtigkeit von IT-Sicherheit bewusst.
- Entscheidungen und Aufwand für IT-Sicherheit werden unterstützt.

Diese Unterstützung sicherzustellen, ist Aufgabe des Lenkungsgremiums, das nach PRINCE2 die Aufgabe verantwortet, einen Kommunikationskanal zum Top-Management zu halten. (Vgl. Kaiser und Simschek, 2000, S. 89-90)

2. PROJEKT LENKEN

Für die Lenkung des Projektverlaufs ist, wie der Name schon sagt, das Lenkungsgremium verantwortlich. Dieses hat keine spezifischen Aufgaben im Kontext der IT-Sicherheit zu erbringen. Jedoch sollte das Lenkungsgremium die Sicherheit des IT-Produkts strategisch unterstützen.

2

Das strategische Lenken soll im Kontext der IT-Sicherheit **vier Aufgaben** erfüllen:

- **Berichtswesen sicher machen:** Das im Kommunikationsmanagement des Projektes vereinbarte Berichtswesen muss die Aspekte der IT-Sicherheit ausreichend berücksichtigen. Im Rahmen regelmäßiger Projektberichte und bei Phasenübergängen müssen die vereinbarten Maßnahmen zur IT-Sicherheit sowie Veränderungen an IT-Assets und daraus resultierende Veränderungen bei der Risikobewertung dargestellt, betrachtet und ggf. neu bewertet werden.
- **Sicht von Eigentümer und Nutzern gleichermaßen einbeziehen:** Die Rolle des Asset Owners muss durch Personen des Lenkungsgremiums ausgefüllt werden. Um Fragestellungen und Entscheidungen im Kontext der IT-Sicherheit gerecht zu werden, muss eine kombinierte Sicht aus Eigentümer/Betreiber und Benutzer des Projektgegenstands eingenommen werden.
- **Kosten und Nutzen im Business Case berücksichtigen:** Bei der Sicherstellung und Überprüfung der Wirtschaftlichkeit des Projekts muss darauf geachtet werden, dass sowohl Kosten als auch Nutzen von IT-Sicherheit angemessen im Business Case berücksichtigt werden.
- **Einbindung des Top-Managements:** Die Aspekte der IT-Sicherheit müssen gegenüber dem Top-Management vertreten werden. Die Einbindung des Top-Managements bzw. einer Management-Hierarchiestufe, die der beauftragenden Organisationeinheit vorgesetzt ist, ist zu gewährleisten. Dies gilt insbesondere bei Fragestellungen und Entscheidungen zur Risikobewertung und dessen Folgeabschätzung.

Das Lenkungsgremium sollte die IT-Sicherheit für das IT-Produkt strategisch unterstützen.

3. PROJEKT INITIIEREN

3

In der Phase der Projektinitiierung steht generell die Sicherheitskonzeption für das IT-Produkt im Fokus. Methodisch orientiert sich das Vorgehen an den Vorgaben aus dem BSI-Standard 200-2 für die Kern-Absicherung.

(Details siehe Anhang 2)

Besondere Aufmerksamkeit gilt bei der Projektinitialisierung dem IT-Produkt, das im Projekt erstellt werden soll, sowie den Prozessen und der Organisation für das Projektvorhaben. Das BSI konzentriert sich hingegen auf die allgemeine Informationssicherheit einer Organisation und der bereits bestehenden IT-Landschaft. Das Vorgehen muss also entsprechend adaptiert werden. Für eine vollständige Abdeckung werden weitere Methoden ergänzt.

Das Sicherheitskonzept erfolgt in diesen Teilschritten:

a. Validierung des Assets und seines Schutzbedarfs

b. Geltungsbereich der Sicherheitskonzeption festlegen

c. Strukturanalyse für die Bestimmung der IT-Assets

d. Schutzbedarf der IT-Assets ermitteln

e. Schwachstellen- und Bedrohungsanalysen nach BSI Methodik

f. Erweiterte Bedrohungsanalyse und Thread Modelling

g. Risikoanalyse und Risikobewertung

h. Bestimmung von Maßnahmen

i. Verankerung in den Projektmanagement-Artefakten

Die Ergebnisse münden in Artefakte oder ergänzen die Artefakte, die in dieser Phase für das Projektmanagement erstellt und verfeinert werden.

Der Fokus der Initiierungsphase liegt auf dem konkreten IT-Produkt, Prozessen und der Organisation des Vorhabens.

Validierung des Assets und seines Schutzbedarfs

Das Asset und dessen Schutzbedarf wurden in der Vorbereitungsphase bestimmt. Des Weiteren wurden relevante externe und interne Compliance-Vorgaben für das Projekt ermittelt, als Handlungsrahmen für Schutzmaßnahmen.

Mit dem Initiierungsauftrag für das Projekt werden das Asset und die ermittelte Schutzbedarfskategorie noch einmal validiert und als Basis für die spätere Strukturanalyse bestätigt.

Geltungsbereich der Sicherheitskonzeption festlegen

Analog zur Definition des Projekt-Scopes muss für die Sicherheitskonzeption ein Geltungsbereich bestimmt werden. Welche Dinge gehören in das Sicherheitskonzept? Welche Aspekte existieren bereits im Informationssicherheitsmanagementsystem des Auftraggebers? Welche kommen neu hinzu?

Des Weiteren ist zu definieren, für welche Dinge der Dienstleister zuständig ist und welche Verantwortlichkeiten beim Auftraggeber verbleiben. Die Klärung dieser Verantwortlichkeiten hängt sehr stark mit der Rollenausprägung Service Provider versus Product Supplier zusammen, die in der Vorbereitungsphase zu klären war. Insgesamt ist darauf zu achten, dass sich das Sicherheitskonzept in das Informationssicherheitsmanagementsystem einfügt und es vollständig ist. Für die Bestimmung des Geltungsbereichs ist die Einbindung von ISB und DSB notwendig.

Strukturanalyse für die Bestimmung der IT-Assets

Die Bestimmung des IT-Assets erfolgt über eine Strukturanalyse auf Basis des definierten Assets. Die Strukturanalyse gliedert sich in zwei Teile:

- **Produktbeschreibung** (z. B. die Beschreibung der Systemstruktur des Produkts)
- **Projektlösungsansatz** (Prozesse, Vorgehen) sowie **Projektorganisation**

Dies ist zu tun:

a. Zunächst werden die beteiligten Organisationsbereiche und Personengruppen identifiziert, auf die sich etwaige Maßnahmen zur Erreichung des notwendigen Sicherheitsniveaus beziehen.

b. Des Weiteren werden die Prozesse erfasst, die zur Erstellung des IT-Produkts notwendig sind. Hierbei ist insbesondere der Geltungsbereich der Sicherheitskonzeption zu berücksichtigen.

b. Der größte Teil der Strukturanalyse besteht aus der Segmentierung des IT-Produkts in seine einzelnen Komponenten. Diese erfolgt über die Beschreibung der Systemarchitektur. Dafür muss die Architektur in dieser Phase mindestens die Komponenten der Lösung sowie die Kommunikationsflüsse zwischen den Komponenten beinhalten.

Gleichartige Komponenten unterliegen in der Regel gleichartigen Bedrohungen.

c. Die Komponenten der Struktur werden gelistet und dabei Gruppen von gleichartigen Komponenten gebildet. Auf dieser Basis setzt die nachfolgende Schwachstellen- und Bedrohungsanalyse auf. Gleichartige Komponenten unterliegen in der Regel gleichartigen Bedrohungen. Sie haben die gleichen Schwachstellen und sind damit den gleichen Gefahren ausgesetzt. Daher lassen sich Komponenten einer Gruppe zur Erreichung der Schutzziele mit den gleichen Maßnahmen absichern.

Schutzbedarf der IT-Assets ermitteln

Nachdem die IT-Assets analysiert wurden, gilt es, ihren Schutzbedarf zu ermitteln. Der Schutzbedarf der Assets, die dem Projektvorhaben zugrundeliegen, wurde bereits definiert. Diesen können wir als Benchmark für alle IT-Assets nutzen. Tatsächlich können wir in der Regel davon ausgehen, dass der Schutzbedarf eines Assets an die IT-Assets vererbt wird. Haben wir also einen hohen Schutzbedarf bei einem Geschäftsprozess und der Geschäftsinformation festgestellt, setzen wir auch den Schutzbedarf des IT-Produkts und dessen Komponenten entsprechend hoch an. Eine detaillierte Bewertung des Schutzbedarfs jedes einzelnen Assets hängt aber natürlich immer vom Projektvorhaben ab.

In der Regel wird der Schutzbedarf eines Assets an die IT-Assets vererbt.

Außerdem ist es möglich, dass im Projekt IT-Assets erzeugt werden, die sich über das Projekt hinaus auswirken oder Verwendung finden. Dies kann zum Anlass genommen werden, den Schutzbedarf höher einzuschätzen und dies als Sicherheitsanforderung im Projekt zu berücksichtigen.

Schwachstellen- und Bedrohungsanalyse

Nach Strukturanalyse und Schutzbedarfsfeststellung erfolgt die Bedrohungsmodellierung gemäß IT-Grundschutz-Kompendium. (Erläuterungen und Überblick siehe Anhang 3)

Für jedes Element der IT-Assets, also für Systemteile, Organisation und Prozesse, werden ein oder mehrere passende Bausteine aus dem IT-Grundschutz-Kompendium gemappt. Das heißt, die zu erstellende IT-Lösung wird mit diesen Bausteinen modelliert.

In den Bausteinen enthalten sind

- Gefährdungen
- Anforderungen an Maßnahmen.
- Teilweise Umsetzungshinweise

Bei normalem Schutzbedarf sind Basis- und Standard-Anforderungen umzusetzen. Bei hohem Schutzbedarf ist eine ergänzende Risikoanalyse durchzuführen.

Erweiterte Bedrohungs-analyse

Eine einfache Bedrohungsanalyse reicht oft nicht aus. Zum Beispiel, wenn

- sie nicht vollständig mit den Bausteinen des IT-Grundschutz-Kompendiums modelliert und beschrieben werden kann.
- ein sehr hoher Schutzbedarf besteht oder es sehr spezifische Sicherheitsziele gibt.
- die Bedrohungsanalyse in einzelnen Aspekten noch konkretisiert wird und suksessive geeignete Maßnahmen vorgeschlagen werden.

In diesen Fällen können wir die Bedrohungsanalyse mit Methoden des **Thread Modellings** erweitern.

Eine seit Jahren bewährte Methode aus diesem Bereich ist die **STRIDE-Methode** von Microsoft. Die Abkürzung STRIDE steht für gängige Kategorien von Sicherheitsrisiken:

S = Spoofing (Identitätsverschleierung)
T = Tampering (Manipulation),
R = Repudiation (Nichtanerkennung)
I = Information Disclosure (Datenpanne)
D = Denial of Service (Service-Verweigerung)
E = Privilege Escalation (Erhöhung von Rechten)

Die Analyse und Modellierung der Bedrohungen kann in Workshops erfolgen. Hier werden die einzelnen ElementederIT-AssetshinsichtlichBedrohungs-szenarien analysiert. (vgl. Kipker, 2023, S. 1079-1080)

In Workshops. werden die Elemente der IT-Assets hinsichtlich Bedrohungsszenarien analysiert.

Das BSI berücksichtigt diese Bedrohung in den Bausteinen zur Software-Entwicklung (CON.10 Eintwicklung von Webanwendungen, CON.8 Software-Entwicklung).

Bei den OWASP Top 10 handelt es sich um die zehn kritischsten Sicherheitsrisiken für Webapplikationen. (Ein Beispiel zu den OWASP Top 10 siehe Anhang 4)

Neben der Liste der Schwachstellen liefert die OWASP auch wertvolle Hinweise für den Softwareentwicklungsprozess. Hier gibt es Tipps für die Minimierung und die Vermeidung von Bedrohungen, die in Anforderungen oder Testkriterien einfließen können.

Risikoanalyse und Risikobewertung

IT-Dienstleister sind auf den Umgang mit Projektrisiken spezialisiert.

Auf Basis von Bedrohungs- und Schwachstellenanalysen wurde das Gefährdungspotential des IT-Produkts beschrieben, einschließlich organisatorischer und prozessualer Aspekte.

Das Ergebnis ist eine Liste an Gefährdungen. Hierzu werden daraufhin die Risiken eingeschätzt und es wird über geeignete Maßnahmen entschieden.

Bei Bedrohungen und Schwachstellen, die auf Basis der BSI-Standards ermittelt wurden, liegt bereits eine implizite Risikobewertung zugrunde. Die Standards empfehlen Maßnahmen differenziert je nach Sicherheitsniveau. Bei darüber hinausgehenden analysierten oder modellierten Schwachstellen und Bedrohungen müssen das Gefährdungspotential und die daraus resultierenden Risiken explizit bewertet werden.

Bei der Risikobewertung geht es darum, zu entscheiden, welche Maßnahmen zur Abwehr von Gefahren im Projektvorgehen ergriffen werden, welche Maßnahmen zum Schutz des IT-Produkts notwendig und adäquat sind, und welches Restrisiko verbleibt. Beim Restrisiko gilt es zu bewerten, ob die Folgen, die beim Eintritt einer Gefahr zu erwarten sind, toleriert werden können.

Der jeweilige Business Case, Kosten und Nutzen des Produkts als Teil der Projektmanagement-Artefakte sowie der Wert und der Schutzbedarf des Assets, der sich aus der Sicherheitskonzeption ergibt, sind ebenfalls wichtige Parameter für die Festlegung der Behandlungsoptionen für identifizierte und bewertete Risiken.

Insbesondere die Option der Auslagerung von Risiken hat bei der Projektzusammenarbeit mit externen IT-Dienstleistern eine besondere Bedeutung.

IT-Dienstleister sind auf den Umgang mit Projektrisiken spezialisiert. Das bedeutet, sie können mit professionellen Methoden, Werkzeugen und Kompetenzen Sicherheitsrisiken übernehmen und diese mittels etablierter Schutzmaßnahmen minimieren.

Für die Risikoanalyse und -bewertung stellt das BSI mit dem BSI-Standard 200-3 geeignete Hilfsmittel bereit.

Der BSI-Standard 200-3 baut auf dem Vorgehen nach IT-Grundschutz auf und beschreibt ein System, mit dem eine Gefährdungsübersicht erstellt und Risiken sowie der Behandlungsoptionen für Risiken eingestuft werden können. Ein Überblick zur Risikoanalyse auf Basis des IT-Grundschutzes befindet sich in Anhang 5.

Ein ergänzender Ansatz spezifisch für Softwareentwicklungsvorhaben ist die DREAD-Methode von Microsoft. Auch sie bezieht das Schadenspotentials mit ein. Aber anstelle der Eintrittswahrscheinlichkeit gibt es genauere Bewertungskriterien wie Reproduzierbarkeit der Gefahr, Ausnutzbarkeit von Angriffen, Auswirkung auf betroffene Benutzer und Auffindbarkeit der Sicherheitslücke. (Vgl. Kipker, 2023, S. 1080-1082)

Für die Risikobewertung und die Festlegung von Maßnahmen für das angestrebte Sicherheitsniveau ist es wie erwähnt wichtig, das Top-Management einzubeziehen. Risikobereitschaft, Sicherheitsanforderungen und Kosten müssen in Einklang gebracht werden. Insbesondere auch im Zusammenspiel mit Dienstleistern ist der Grad der Risikoverlagerung und Risikoübernahme auszubalancieren.

Maßnahmen im Sicherheitskonzept festlegen

Das Sicherheitskonzept umfasst das IT-Produkt mit seinen Komponenten sowie Prozesse und Organisation. Die Maßnahmen, die sich aus Analysen und Risikobewertung ergeben, sind hier final festzulegen. Sie werden folgendermaßen in die nächsten Projektphasen überführt:

- Sicherheitsanforderungen und Maßnahmen als funktionale Anforderungen für die IT-Lösung
- Sicherheitsanforderungen und Maßnahmen als Anforderungen an Werkzeuge zur automatisierten Unterstützung von Prozessen
- Sicherheitsanforderungen als Qualitätssicherungs- und Abnahme-Kriterien um zu verifizieren, ob Maßnahmen umgesetzt wurden
- Sicherheitsanforderungen und Maßnahmen als Handlungsanweisungen für beteiligte Personengruppen im Projekt
- Sicherheitsanforderungen und Maßnahmen als Prozessschritte in relevanten Prozessen
- Sicherheitsanforderungen als Ausbildungs- und Awareness-Maßnahmen für beteiligte Personengruppen im Projekt

Die Ergebnisse des Sicherheitskonzepts werden in den Artefakten des Projektmanagements verankert. Sie sind verpflichtend für die weiteren Projektphasen.

4. ÜBERGANG MANAGEN

Im Übergang zwischen den einzelnen Schritten geht es vor allem darum, das Sicherheitskonzept zu prüfen: Ist es auf dem aktuellen Stand? Wird es erfüllt?

Aktualität

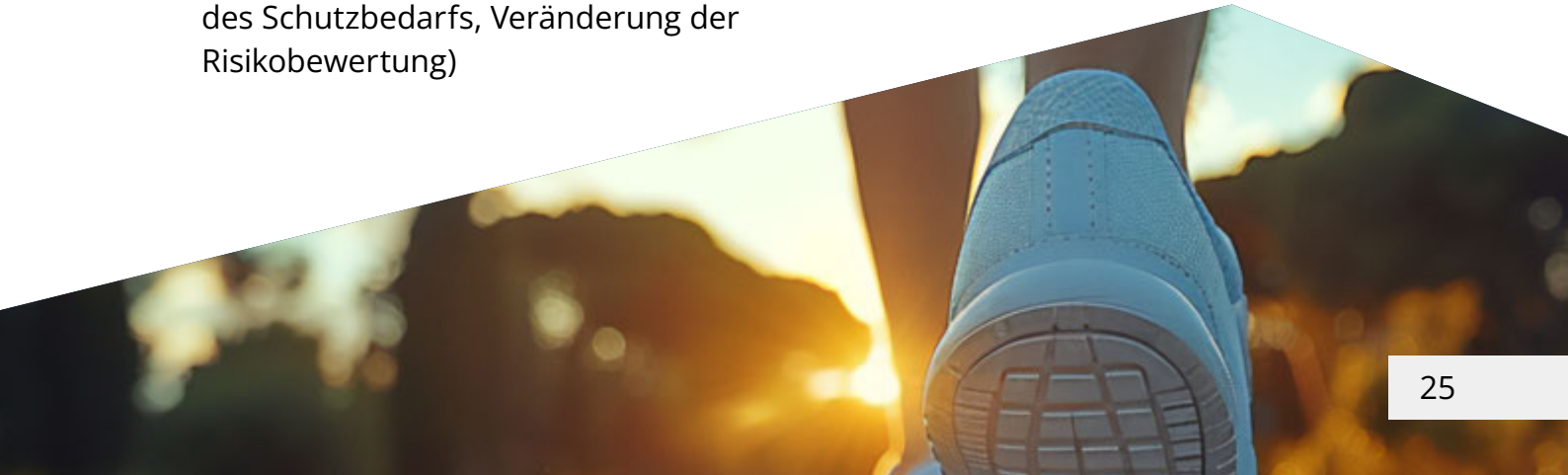
Im Projektverlauf kann es Änderungen und Anpassungen geben, die immer wieder die Überprüfung und Aktualisierung des Sicherheitskonzepts erforden. Dazu gehören:

- Veränderungen der Systemarchitektur im Projektverlauf (IT-Assets werden verändert)
- Austausch von Komponenten durch andere Technologien (IT-Assets werden verändert)
- Neue Erkenntnisse zu Bedrohungen und Schwachstellen (Es gibt neue bzw. veränderte Gefährdungen)
- Die Risikobereitschaft verändert sich, z. B. durch externe Einflüsse wie Sicherheitsvorfälle bei Wettbewerbern, Häufung von Angriffen, Neue Angriffsvektoren (die Risikobewertung ist nicht mehr adäquat)
- Veränderungen in gesetzlichen Vorgaben, Verordnungen oder Compliance-Anforderungen (Veränderung des Schutzbedarfs, Veränderung der Risikobewertung)

Wenn wichtige Änderungen im Projektverlauf entstanden sind, muss die Sicherheitskonzeption gemäß des Schritts „Projekt initiieren“ angepasst werden. Es werden dabei gezielt nur die betroffenen Bereiche überarbeitet. Dies ist in der Projektplanung für den nächsten Schritt zu berücksichtigen und für das Lenkungsgremium transparent aufzubereiten.

4

Wenn wichtige Änderungen entstanden sind, muss die Sicherheitskonzeption angepasst werden.



Umsetzung und Erfolg

Weitere Aspekte, die zu überprüfen sind, sind der Grad der Umsetzung von Sicherheitsmaßnahmen und die Ergebnisse:

- Wurden funktionale Sicherheitsanforderungen umgesetzt und strukturiert überprüft oder getestet?
- Werden Handlungsanweisungen verstanden, akzeptiert und angewandt?
- Wurden prozessuale Maßnahmen umgesetzt und funktionieren sie in der Praxis?
- Wurden automatisierbare Maßnahmen entsprechend der Anforderungen umgesetzt? (z. B. Checks in der DevOps-Pipeline)
- Wurden Security-Awareness-Maßnahmen erfolgreich umgesetzt?

Zu überprüfen sind Umsetzbarkeit und Akzeptanz von Sicherheitsmaßnehmen.

Wenn es zu Problemen oder Widerständen bei der Umsetzung bzw. bei der Akzeptanz von Maßnahmen im Projektverlauf kommt, ist zu prüfen, wie Umsetzung und Anwendbarkeit verbessert werden können. Ggf. kann über Projektsteuerung und konsequentere Führung die Umsetzung erreicht werden.

5. MANAGEN VON PROJEKTPHASE UND PRODUKTLIEFERUNG

In den Prozessen „Steuern einer Phase“ und „Managen der Produktlieferung“ ist hinsichtlich der IT-Sicherheit dafür zu sorgen, dass Maßnahmen und Anforderungen zur IT-Sicherheit bei der Erstellung des IT-Produkts umgesetzt werden.

Dies beinhaltet:

- Umsetzung funktionaler Anforderungen zur IT-Sicherheit
- Umsetzung von Automatismen in Werkzeugen
- Einhaltung von Prozessen
- Befolgung von Handlungsanweisungen

5

Bewährt hat sich hierfür die Etablierung eines „Secure-Development-Prozesses“. Dieser Begriff entstand in Anlehnung an den Security Development Lifecycle (SDL) von Microsoft, einem Ergebnis der Sicherheitsinitiative des Herstellers in den 2000er Jahren. (Vgl. Microsoft, 2024)

Ein Security-Development-Prozess hilft den Verantwortlichen, in einem Projektszenario mit einem für das Vorhaben zusammengestellte Entwicklungs- und IT-Spezialisten-Team ein ähnliches Verständnis für „sichere Entwicklung“ zu fördern.

Im Team der Entwicklungs- und IT-Spezialist:innen muss ein ähnliches Verständnis zu „sicherer Entwicklung“ etabliert werden.

Fünf Aspekte sind dafür wichtig und sollten etabliert werden:

- Enablement & Awareness für sichere IT-Produkte
- Security by Design
- Secure Coding
- Testing und Verifikation
- Review, Learning & Improvement

(Vgl. Kipker, 2023, S. 1078-1079)

Enablement und Awareness für sichere IT-Lösungen

Dreh- und Angelpunkt für ein sicheres IT-Produkt sind am Ende die Menschen, die an der Erstellung der Lösung mitwirken. Neben einer Grundkompetenz für ihre Aufgaben müssen sie in das Vorhaben und seine Ziele gut eingeführt werden.

Im Engineering Handbook werden Handlungsanweisungen und Regeln dokumentiert.

Dazu gehört das Enablement für das Sicherheitskonzept und dessen Inhalte. Darüber hinaus werden Handlungsanweisungen und Regeln in einem gut zugänglichen Handbuch als wichtiger Teil der Projekt-Artefakte „Richtlinien und Management-Praktiken“ dokumentiert: dem **Engineering Handbook**.

Denn – und man kann es nicht oft genug sagen: Ein gleiches Verständnis für die Sicherheitsziele und die dafür notwendigen Maßnahmen und Verhaltensweisen kann nicht vorausgesetzt, sondern muss im Projekt aktiv und nachhaltig gefördert werden.

Security by Design

Der Security-by-Design-Ansatz setzt auf die frühe Berücksichtigung von Sicherheitsanforderungen an ein IT-Produkt in der Phase des Lösungsdesigns.

Deshalb ist es so wichtig, bereits in der Phase der Projektinitiierung die Sicherheitskonzeption strukturiert und methodisch zu entwickeln. Diese dient neben den funktionalen Anforderungen als Basis für die Architektur und das technische Design.

Insbesondere Transparenz zu Bedrohungen und Risiken aber auch das Verständnis über schützenswerte Eigenschaften und den Wert des IT-Produkts gibt bei der Konstruktion ein gutes Verständnis dafür, was in Bezug auf Sicherheit bei Architektur und technischem Design zu berücksichtigen ist – und warum.

Secure Coding

Beim Secure Coding geht es darum, die Maßnahmen und Anforderungen der IT-Sicherheit praktisch umzusetzen. Dies gelingt, wenn Entwickungsteams und IT-Fachleute für die besondere Projektumgebung sowie ein solides Lösungsdesign gut enabled und IT-Sicherheitsaspekte von Grund auf berücksichtigt wurden.

Des Weiteren müssen die Entwicklungswerkzeuge Automatismen zur Verfügung stellen, die Umsetzung und Verifikation von IT-Sicherheitsanforderungen unterstützen.

Testing und Verifikation

Wenn es um die Qualität der IT-Lösung geht, gilt es, neben der funktionalen Sicherheit auch die IT-Sicherheitsanforderungen strukturiert und wo möglich automatisiert zu testen und deren Erfüllung zu verifizieren.

Zum einen kann dies durch eine Reihe von Automatismen in Entwicklungsumgebungen erreicht werden, insbesondere in den Werkzeugen für eine automatisierte Build- und Deployment-Pipeline.

Zum zweiten kann ein Penetration Test eingesetzt werden, um systematisch Schwachstellen auszunutzen, die in der Bedrohungsanalyse identifiziert wurden. So lässt sich herausfinden, ob die Sicherheitsmaßnahmen wirken.

Review, Learning und Improvement

Zuletzt gilt es, den Prozess von Konstruktion und Bau des IT-Produkts immer wieder neu zu beleuchten. Beobachtet werden sollten:

- Werkzeuge
- Wissen und die gelebte Praxis der Projektteilnehmenden?
- Rahmenbedingungen

Agile Arbeitsweisen und ein agiles Mindset in IT-Projekten helfen dabei, Verbesserungen regelmäßig durchzuführen.

Die Möglichkeit für regelmäßige Verbesserungen und Anpassungen geht einher mit agilen Arbeitsweisen.

Agilität gilt daher als Grundvoraussetzung, um die nötige Akzeptanz zu erreichen, Sicherheitsanforderungen nachhaltig zu verfolgen und entsprechende Prozesse anzuwenden und Handlungsanweisungen zu befolgen.

6. PROJEKT ABSCHLIESSEN

In der Abschlussphase eines Projekts bzw. bei der Vorbereitung der Projektabnahme gilt es aus Perspektive der IT-Sicherheit die Sicherheitsziele und das angesetzte Sicherheitsniveau nachzuweisen.

Ob Sie Ihre Sicherheitsziele erreicht haben, können Sie in strukturierten Security Checks feststellen. Darin werden alle in der Sicherheitskonzeption definierten Sicherheitsanforderungen noch einmal abschließend geprüft und verifiziert.

Ob Sie Ihre Sicherheitsziele erreicht haben, können Sie in strukturierten Security Checks feststellen.

Dies **Abnahme** ist der Startpunkt für die Überführung des IT-Produkts in den Betrieb. Daraufhin erfolgt also die Übergabe des IT-Produkts an die zuständige Betriebsorganisation. Teil der Abschlussarbeiten können dementsprechend auch Maßnahmen sein wie ein abschließendes Härten von Systemkomponenten durch das Anpassen der Konfiguration für den Produktivbetrieb oder Ähnliches.

Ein weitere Maßnahme wäre die **externe Verifikation**. Hierzu eignet sich ein unabhängiges, externes Security-Audit, das auf Grundlage der Sicherheitskonzeption durchführt wird. Es geht also darum, dass eine externe und neutrale Instanz die Erreichung der gesetzten Schutzziele bestätigt.

6

Auch **Penetration Tests** durch einen externen Dienstleister wären eine Möglichkeit, das Sicherheitsniveau des IT-Produkts unabhängig zu überprüfen.

SUMMARY

SUMMARY

Der aktuelle Bericht des BSI zur Lage der Informationssicherheit in Deutschland zeichnet macht auf die weiterhinangespannte Bedrohungslage aufmerksam. (Vgl. Bundesamt für Sicherheit in der Informationstechnik (2024)) Ein hohes Maß an IT-Sicherheit in Unternehmen ist also notwendiger denn je, um die Werte der Organisation zu schützen.

Der Schlüssel liegt in der Verknüpfung des Projektmanagements mit den Methoden zur Erreichung von IT-Sicherheit.

In diesem How-to-Guide wird ein Weg beschrieben, der dabei helfen kann, individuelle IT-Produkte mit einem hohen Maß an Sicherheit für die Organisation bereitzustellen.

Ein großer Vorteil ist, dass sich dieser Weg eng an der Praxis eines IT-Projekts orientiert. Das hilft dabei, die notwendigen Schritte wirkungsvoll umzusetzen.

Synergien von Projektmanagement und IT-Sicherheit nutzen

Für die praktische Umsetzbarkeit lag es nahe, Methoden des Projektmanagements mit Methoden und Standards für IT-Sicherheit zu verknüpfen. Da die Projektmanagementmethoden schon etabliert und integraler Bestandteil eines jeden projektierten IT-Vorhabens sind, geht es ohne viel Aufhebens an die Umsetzung.

Ein weiterer Vorteil: Die Artefakte für das Lenken, Steuern und Managen einer Produktlieferung überschneiden sich an vielen Punkten mit den Methoden für IT-Sicherheit. Diese Synergien nutzen wir.

Früher Blick lohnt sich

Es lohnt sich, früh auf die Anforderungen zu schauen, die ein sicheres Produkt erfüllen muss. Denn schon bei der Vorbereitung und Initiierung des IT-Projekts werden die Weichen für ein angemessenes Schutzniveau gelegt. Damit IT-Sicherheit gelingt, braucht es:

- Hohe Priorität der Sicherheitsaspekte im Lösungsdesign
- Befähigung der Projektbeteiligten
- Bewusstsein für Informationssicherheit und Datenschutz

Strukturiert handeln

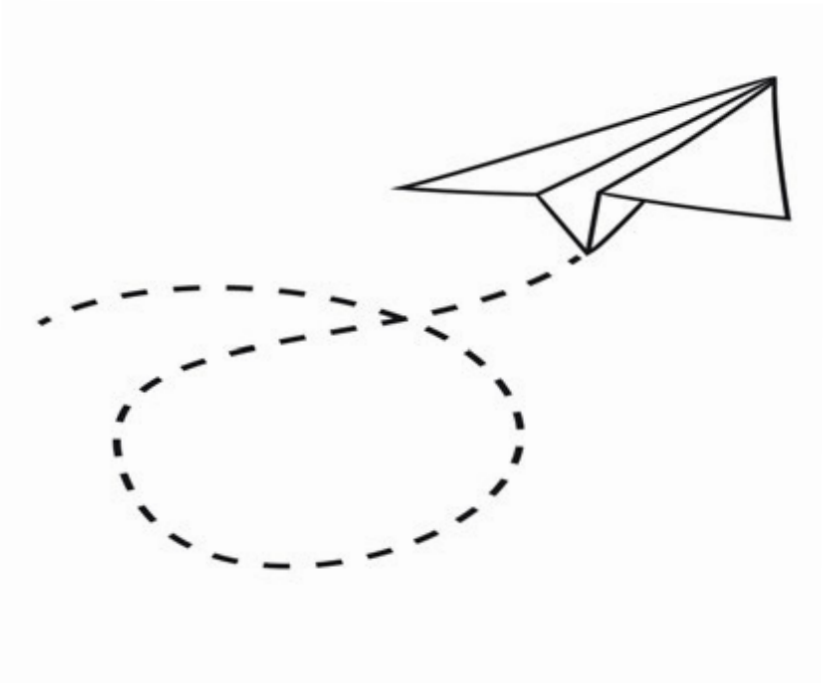
Angemessene IT-Sicherheit braucht strukturiertes und methodisches Handeln.

Mit dem IT-Grundschutz steht ein erprobter Baukasten mit Methoden und Komponenten zur Verfügung, die helfen, den Schutzbedarf eines IT-Produkts zu ermitteln und Maßnahmen zur Abwehr und Vermeidung von Gefährdungen abzuleiten.

Angemessene IT-Sicherheit ist durch strukturiertes und methodisches Handeln herstellbar.

Diese frei verfügbare Vorgehensweise setzt mit den BSI Standards und dem IT-Grundschutz-Kompendium einen Standard für IT-Sicherheit in Institutionen und lässt sich auf einzelne IT-Produkte und das Projektumfeld adaptieren.

Sicherheit braucht methodisches, strukturiertes Handeln!



TAKE AWAY

Strukturiertes, methodisches Vorgehen in der IT-Sicherheit ist für die Softwareentwicklung entscheidend. Dieses Vorgehen hilft uns, Bedrohungen frühzeitig zu erkennen, Schwachstellen zu schließen und Sicherheitsvorfälle effizient zu bewältigen. So schützen wir unsere Software zuverlässig vor Angriffen und minimieren Risiken.

LITERATUR & ANHANG

LITERATUR

Bundesamt für Sicherheit in der Informationstechnik (2024) Regelungsdokument für das Informationssicherheitsmanagementsystem in der IT-Konsolidierung Bund [Online]. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_ISMS_ITKB_V1_0.html (Abgerufen am 11.02.2025).

Bundesamt für Sicherheit in der Informationstechnik (2023) BSI-Standard 200-2: IT-Grundschutz-Methodik [Online]. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.html (Abgerufen am 11.02.2025).

Bundesamt für Sicherheit in der Informationstechnik (2023) BSI-Standard 200-3: Risikomanagement [Online]. Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf (Abgerufen am 11.02.2025).

Bundesamt für Sicherheit in der Informationstechnik (2023) IT-Grundschutz-Kompendium – Werkzeuge für Informationssicherheit [Online]. Verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutzKompendium.html (Abgerufen am 11.02.2025).

Bundesamt für Sicherheit in der Informationstechnik (2023) IT-Grundschutz-Bausteine [Online]. Verfügbar unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html (Abgerufen am 18.12.2023)

Bundesamt für Sicherheit in der Informationstechnik (2024) Die Lage der IT-Sicherheit in Deutschland 2024 [Online]. Verfügbar unter https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html (Abgerufen am 11.02.2025).

Eckert, Claudia (2023) IT-Sicherheit [Online], 11. Auflage, Berlin/Bosten, Walter de Gruyter GmbH. Verfügbar unter https://doi.org/10.1515/9783110985115-201 (Abgerufen am 11.02.2025).

Europäisches Parlament (2016) Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (BMWK).

Kaiser, Fabian und Simschek, Roman (2020) PRINCE2 Die Erfolgsmethode einfach erklärt: Version 2017/6 [Online], 3. Auflage, München, UVK Verlag. Verfügbar unter https://elibrary.narr.digital/book/99.0000/9783739880587 (Abgerufen am 11.02.2025).

Karg, Stefan (Bundesamt für Sicherheit in der Informationstechnik) (2022) IT-Grundschutz Arbeitshandbuch: DIN ISO/IEC 27001, DIN ISO/IEC 27002, BSI-Standards 200-1/2/3, 3. Auflage, Köln, Reguvis Fachmedien GmbH.

Kipker, Dennis-Kenji (2023) Cybersecurity, 2. Auflage, München, Verlag C. H. Beck oHG.

Microsoft (© 2024) Security Engineering: About Microsoft SDL [Online]. Verfügbar unter https://www.microsoft.com/en-us/securityengineering/sdl/about (Abgerufen am 11.02.2025).

Open Web Application Security Project (© 2024) OWASP Top Ten [Online]. Verfügbar unter https://owasp.org/www-project-top-ten/ (Abgerufen am 11.02.2025).

ANHANG 1

Der BSI-Standard 200-2 stellt beispielhaft Kriterien zur Bestimmung eines angemessenen Sicherheitsniveaus für Geschäftsprozesse oder Organisationsbereiche in Bezug auf die Grundwerte der Informationssicherheit zur Verfügung. (vgl. BSI, 2023b, S. 24-25)

„Anhand derjenigen Aussagen, die am ehesten zutreffen, lässt sich das Sicherheitsniveau (normal, hoch oder sehr hoch) einzelner Geschäftsprozesse bzw. Bereiche bestimmen“ (BSI, 2023b, S. 24-25).

Schutzbedarf: Sehr hoch

- **Allgemein:** Ausfall der Geschäftsprozesse, unberechtigter Zugriff oder Manipulation von kritischen Informationen führen zum Zusammenbruch der Organisation oder haben schwerwiegende Folgen
- **Vertraulichkeit:** Der Schutz vertraulicher Informationen muss unbedingt gewährleistet sein; sicherheitskritische Bereiche; es gelten strenge Vertraulichkeitsanforderungen, Offenlegung vertraulicher Informationen kann schwere Folgen haben, Fortbestand der Organisation ist gefährdet
- **Integrität:** Informationen müssen im höchsten Maße korrekt sein
- **Verfügbarkeit:** Zentrale Aufgaben der Organisation, ohne IT-Einsatz nicht leistbar, ständige Präsenz der aktuellen Informationen notwendig, Ausfallzeiten inakzeptabel
- **Datenschutz:** Gefahr für Leib und Leben oder für die persönliche Freiheit des Betroffenen. Schutz persönlicher Daten muss unbedingt gewährleistet sein

Schutzbedarf: Hoch

- **Allgemein:** Organisation ist in zentralen Bereichen handlungsunfähig im Schadensfall. Erhebliche Beeinträchtigungen der Organisation oder weiterer Betroffener im Schadensfall
- **Vertraulichkeit:** Es bestehen hohe Anforderungen für den Schutz vertraulicher Informationen; Schutz von Informationen muss in sicherheitskritischen Bereichen stärker ausgeprägt werden
- **Integrität:** Informationen müssen korrekt sein, Fehler müssen erkannt werden und vermeidbar sein
- **Verfügbarkeit:** es handelt sich um zeitkritische Prozesse; Vorgänge nur mit IT-Einsatz leistbar, kurze Ausfallzeiten sind tolerierbar
- **Datenschutz:** Hohe Anforderungen an personenbezogene Daten, Gefahr der erheblichen Beeinträchtigung von betroffenen Personen im Schadensfall

Schutzbedarf: Normal

- **Allgemein:** Im Schadensfall ist die Organisation beeinträchtigt
- **Vertraulichkeit:** Informationen sollen korrekt sein, Fehler können im kleinen Umfang toleriert werden; Fehler müssen erkennbar und vermeidbar sein
- **Verfügbarkeit:** längere Ausfallzeiten sind tolerierbar
- **Datenschutz:** personenbezogene Daten müssen geschützt werden; Gefahr der Beeinträchtigung von betroffenen Personen im Schadensfall

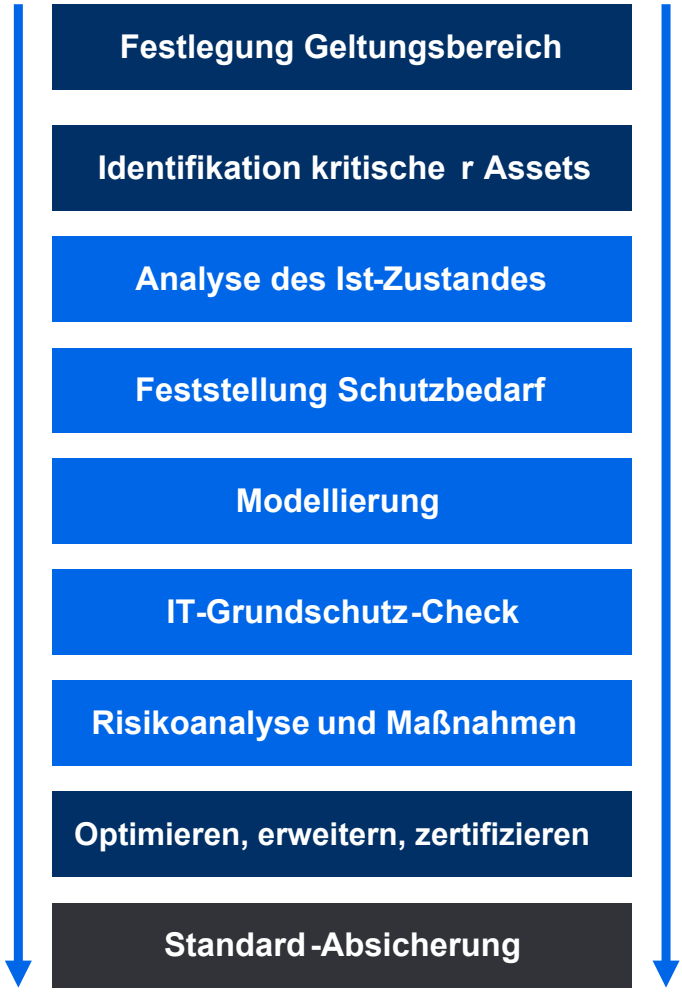
(Vgl. BSI, 2023b, S. 24-25)

ANHANG 2

Der BSI-Standard 200-2 als Teil der BSI-Methodik stellt Prozesse für die Erstellung einer Sicherheitskonzeption bereit. Die Vorgehensweisen der Prozesse unterscheiden sich nach der angestrebten Absicherung, die zu erreichen ist.

- Sicherheitskonzeption nach Vorgehensweise Basis-Absicherung
- Sicherheitskonzeption nach Vorgehensweise Kern-Absicherung
- Sicherheitskonzeption nach Vorgehensweise Standard-Absicherung

Im Folgenden wird die Erstellung einer Sicherheitskonzeption nach dem Vorgehen der Kern-Absicherung skizziert. Dieser Prozess bildet die Grundlage für die in dieser Studienarbeit adaptierten Vorgehensweise bei Erstellung einer Sicherheitskonzeption im Kontext von IT-Projekten. Die Abbildung rechts zeigt den schematischen Ablauf der Kern-Absicherung nach BSI-Standard 200-2. (Vgl. BSI, 2023b, S. 68)



ANHANG 3

Die Bausteine im IT-Grundschutz sind in thematische Bereiche gegliedert und umfassen das Sicherheitsmanagement, die Organisation als auch technische Komponenten.

In den Texten der Bausteine sind sowohl Gefährdungen beschrieben als auch Anforderungen, die zur Erreichung eines definierten Sicherheitsniveaus erfüllt sein müssen. Die Bausteine implizieren bereits eine Risikobewertung. Diese ist ausgelegt auf den normalen Schutzbedarf. (Vgl. BSI, 2023d). Hier ein Auszug (vgl. BSI, 2023e):

ISMS: SICHERHEITSMANAGEMENT
ISMS.1 Sicherheitsmanagement

ORP: ORGANISATION & PERSONAL
ORP.3 Sensibilisierung und Schulung
ORP.4 Identitäts - und Rechtemanagement
…

CON: KONZEPT & VORGEHEN
CON.1 Kryptokonzept
CON.2 Datenschutz
CON.6 Löschen und Vernichten
…

OPS: BETRIEB
OPS.1.1.1 Allgemeiner IT-Betrieb
OPS.1.1.3 Patch- und Changemanagement
OPS.1.1.5 Protokollierung
…

IND: INDUSTRIELLE IT
IND.1 Prozessleit- und Automatisierungstechnik
IND.2.2 Speicherprogrammierte Steuerung
IND.2.3 Sensoren und Aktoren
IND.2.4 Maschine
…

DER: DETEKTION & REAKTION
DER.2.1 Behandlung Sicherheitsvorfälle
DER.2.2 Vorsorge für IT-Forensik
DER.3.1 Audits und Revision
DER.4 Notfallmanagement
…

APP: ANWENDUNGEN
APP.1.2 Webbrowser
APP.1.4 Mobile Anwendungen (Apps)
APP.2.3 OpenLDAP
APP.3.2 Webserver
APP.4.3 Relationale Datenbanksysteme
APP.4.4 Kubernetes
APP.7 Entwicklung Individualsoftware
…

SYS: IT-SYSTEME
SYS.1.1 Allgemeiner Server
SYS.1.5 Virtualisierung
SYS.1.6 Containerisierung
…

NET: NETZE & KOMMUNIKATION
NET.1.1 Netzarchitektur und -design
NET.2.1 WLAN-Betrieb
NET.3.2 Firewall
NET 3.3 VPN
NET.4.1 TK-Anlagen
…

INF: INFRASTRUKTUR
INF.1 Allgemeine Gebäude
INF.2 Rechenzentrum sowie Serverraum
INF.7 Büroarbeitsplatz
INF.14 Gebäudeautomation
…

ANHANG 4

Das Open Web Application Security Project (OWASP) ist eine Non-Profit-Organisation, die sich dem Ziel verschrieben hat, die IT-Sicherheit im Web zu verbessern.

In den OWASP Top 10 beschreibt die OWASP die zehn kritischsten Sicherheitsrisiken für Webapplikationen.

Die Liste der Top 10 wird im Abstand von drei bis vier Jahren aktualisiert und veröffentlicht. Die aktuelle Version stammt aus dem Jahre 2021.

Im grauen Kasten finden Sie als Beispiel die OWASP Top 10 von 2021.

(Vgl. Open Web Application Security Project, 2023)

A01:2021 – BROKEN ACCESS CONTROL
A02:2021 – CRYPTOGRAPHIC FAILURES
A03:2021 – INJECTION
A04:2021 – INSECURE DESIGN
A05:2021 – SECURITY MISCONFIGURATION
A06:2021 – VULNERABLE AND OUTDATED COMPONENTS
A07:2021 – IDENTIFICATION AND AUTHENTICATION FAILURES
A08:2021 – SOFTWARE AND DATA INTEGRITY FAILURES
A09:2021 – SECURITY LOGGING AND MONITORING FAILURES
A10:2021 – SERVER SIDE REQUEST FORGERY

ANHANG 5

Der BSI-Standard 200-3 als Teil der BSI-Methodik stellt eine Vorgehensweise zur Risikoanalyse und -bewertung zur Verfügung mit dem Ziel, die Risiken der Informationssicherheit angemessen zu steuern. Die Risikoanalyse nach der BSI-Methodik läuft in vier Phasen ab:

- Erstellung Gefährdungsübersicht
- Einstufung von Risiken: Einschätzung und Bewertung von Risiken
- Behandlung von Risiken: Umgang mit identifizierten und bewerteten Risiken
- Konsolidierung der Sicherheitskonzeption: Integration der Analyse

Das Vorgehen der Risikoanalyse fügt sich in den BSI-Standard 200-2 als Methodik für die Erstellung einer Sicherheitskonzeption ein. (vgl. BSI, 2023c, S. 5-8)

Die Einschätzung von Risiken nach BSI-Methodik sieht zwei Kategorien vor. Zum einen die Eintrittshäufigkeit, sowie die Schadensauswirkung, die dem Risiko unterstellt wird.

In den beiden Tabellen unten werden die Kategorien mit vorgeschlagenen Wertebereichen dargestellt. (vgl. BSI, 2023c, S. 26-27)

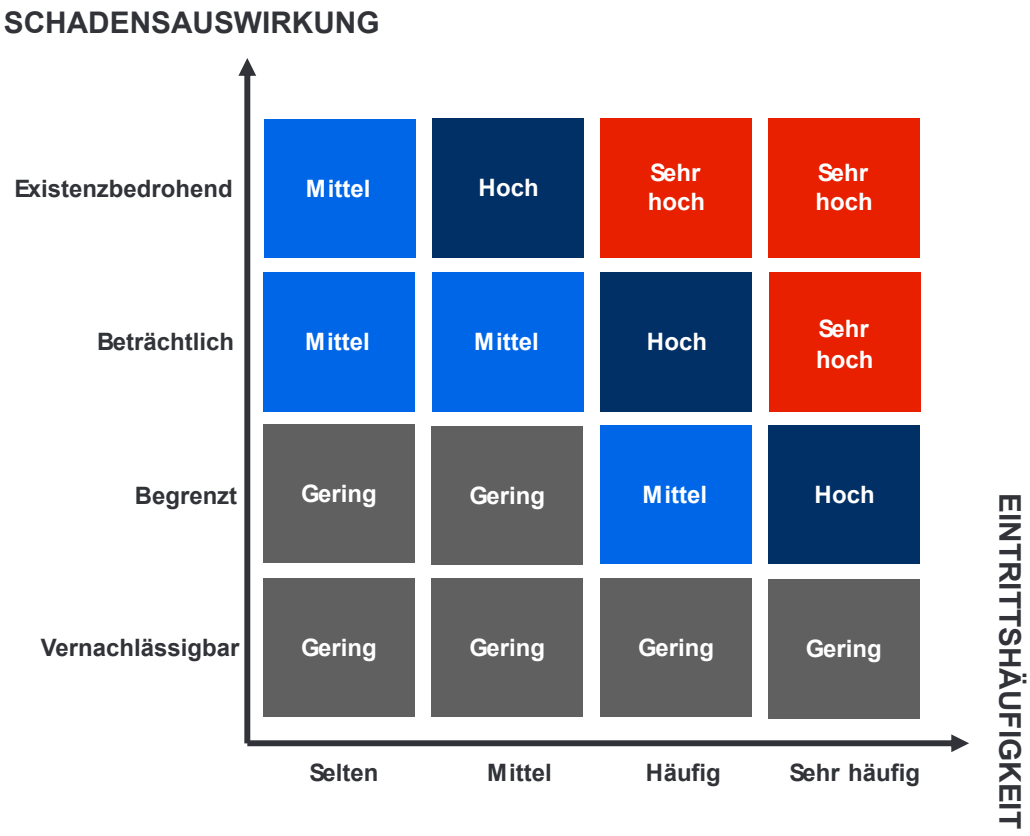
Eintrittshäufigkeit – Kategorisierung	
Selten	Ereignis höchstens alle 5 Jahre (nach heutigem Kenntnisstand)
Mittel	Ereignis: 1x in 5 Jahren bis 1x pro Jahr
Häufig	Ereignis: 1x im Jahr bis 1x pro Monat
Sehr häufig	Ereignis: mehrfach pro Monat

Schadensauswirkung – Kategorisierung	
Vernachlässigbar	Geringe bis vernachlässigbare Auswirkung
Begrenzt	Begrenzte bis überschaubare Auswirkung
Beträchtlich	Beträchtliche Auswirkung
Existenzbedrohend	Existenzielle Bedrohung, katastrophale Auswirkung

Auf Basis der Kategorisierung von Eintrittshäufigkeit und Schadensauswirkung werden die eingeschätzten Risiken in einer Risikomatrix abgebildet.

Die in der Matrix abgebildeten Risikokategorien sind je nach Bedarf der Organisation individuell festzulegen.

Diese Abbildung zeigt eine Risikomatrix nach BSI:



Die Tabelle zeigt beispielhaft die Kategorisierung zur gezeigten Risikomatrix (vgl. BSI, 2023c, S. 27-28):

Risiko – Kategorisierung	
Gering	Umgesetzte oder vorgesehene Sicherheitsmaßnahmen bieten ausreichenden Schutz. Geringe Risiken sind zu akzeptieren aber Gefährdungen dennoch zu beobachten.
Mittel	Umgesetzte oder vorgesehene Sicherheitsmaßnahmen reichen möglicherweise nicht aus.
Hoch	Umgesetzte oder vorgesehene Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der Gefährdung.
Sehr hoch	Umgesetzte oder vorgesehenen Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der Gefährdung. Risiken sind in der Regel nicht zu akzeptieren.

Auf Basis der identifizierten und bewerteten Risiken erfolgt die Festlegung der Behandlungsstrategien für die Risiken. Folgende Optionen der Risikobehandlung können gewählt werden:

- Risiken vermeiden
- Risiken reduzieren
- Risiken transferieren / auslagern
- Risiken akzeptieren

Die Optionen Risikovermeidung, Risikoreduktion und Risikotransfer sind Behandlungsoptionen, die mit der Festlegung und Umsetzung von Sicherheitsmaßnahmen operationalisiert werden. (Vgl. BSI, 2023c, S. 33-34)

KONTAKT

Warum stehen Sie morgens auf? Um Ihr Unternehmen besser zu machen? Die richtigen Entscheidungen auf Basis der aktuellen Daten und Vorhersagen zu treffen? Sie wollen Prozesse verschlanken und automatisieren? Sich auf Ihr Geschäft konzentrieren und nicht auf Ihre IT? Wir stehen morgens auf, um Sie dabei zu unterstützen! Wir wissen, es braucht gute IT-Lösungen und mehr!

Mehr als 500 Fachleute an 9 Standorten treten bei uns jeden Tag an, um Ihre Herausforderungen zu meistern und Sie in Ihrem Geschäft besser zu machen! Wir befähigen Menschen und bauen für sie passende digitale Lösungen! 2/3 der DAX-Unternehmen vertrauen uns. Wir sind die Digitale Service Manufaktur.

Wie können wir Sie besser machen?
Kontaktieren Sie mich!

andreas.becht@opitz-consulting.com

OPITZ CONSULTING