

Referenzprofil

IT Security Coordinator

Irmhild Rogalla

Dieses Referenzprofil wurde im Rahmen des bmb+f geförderten Projekts „Arbeitsprozess-orientierte Weiterbildung in der IT-Branche“ erarbeitet von:



Fraunhofer ISST



Bildungspartner



TENOVIS
Business Communications.

Unternehmenspartner

Danksagung

Diese Profilbeschreibung entstand auf Basis eines Praxisprojekts der Firma *Tenovis*, deren zuständigem Sicherheitsbeauftragten Herrn Volker Ahrend wir herzlich für seine fachkundige und umfassende Hilfe danken. Fachlich beratend mitgewirkt haben Bernd Kaiser sowie Volker Müller, *NT+C Network Training and Consulting*. Ohne ihre Hilfe hätte dieses Dokument nicht entstehen können.

Inhalt

1	EINFÜHRUNG: REFERENZPROZESSE ALS CURRICULA.....	4
1.1	EREIGNIS-PROZESS-KETTEN: SYMBOLIK.....	4
1.2	REFERENZPROZESS UND TEILPROZESSE	6
2	DAS PROFIL: IT SECURITY COORDINATOR (IT-SICHERHEITSKOORDINATOR/IN)	9
2.1	TÄTIGKEITSBESCHREIBUNG	9
2.2	PROFILTYPISCHE ARBEITSPROZESSE	9
2.3	PROFILPRÄGENDE KOMPETENZFELDER	10
2.4	QUALIFIKATIONSERFORDERNISSE	11
2.5	EINORDNUNG INS SYSTEM UND KARRIEREPFADE.....	11
3	REFERENZPROZESS	13
3.1	IT-SICHERHEITSKOORDINATION	13
3.1.1	Referenzprozess IT-Sicherheitskoordination	14
3.1.2	Das Beispielprojekt: Anbindung von Außenstellen über VPN	17
3.1.3	Prozesskompass IT-Sicherheitskoordination.....	18
3.1.3.1	Aufrechterhalten der IT-Sicherheit.....	19
3.1.3.2	Mitwirken bei der Vertragsgestaltung im IT-Bereich.....	22
3.1.3.3	Vertreten des Unternehmens in Sicherheitsfragen nach außen.....	24
3.1.3.4	Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit.....	25
3.1.3.5	Unterstützen der Partner bei sicherheitstechnischen Maßnahmen.....	27
3.1.3.6	Gegenseitiges Informieren der Partner über sicherheitsrelevante Änderungen	30
3.1.3.7	Beraten bei der Anpassung und Konkretisierung der Sicherheitsziele	31
3.1.3.8	Entwerfen der Sicherheitsleitlinien.....	34
3.1.3.9	Durchführen von IT-Strukturanalysen.....	36
3.1.3.10	Feststellen des Schutzbedarfs der Fachabteilungen.....	39
3.1.3.11	Aufstellen des Grundschutzmodells	42
3.1.3.12	Vergleichen von Ist- und Soll-Zustand in den Fachabteilungen	46
3.1.3.13	Spezifizieren des Maßnahmenplans.....	49
3.1.3.14	Präsentieren der Vorschläge bei den Entscheidern	52
3.1.3.15	Planen der Umsetzung	54
3.1.3.16	Begleiten der Umsetzung.....	56
3.1.3.17	Schulen der Mitarbeiterinnen und Mitarbeiter.....	58
3.1.3.18	Durchführen von Funktionsprüfungen	61
3.1.3.19	Dokumentieren des gesamten IT-Sicherheitsprozesses	63

1 Einführung: Referenzprozesse als Curricula

Das Referenzprojekt des IT Security Coordinators (IT-Sicherheitskoordinator/in) verdeutlicht paradigmatisch die diesem Tätigkeitsfeld zugrunde liegenden Arbeitsprozesse, die mit ihnen verbundenen Ansprüche sowie die daraus resultierenden Anforderungen an Inhalt und Durchführung einer qualitativ hochwertigen Weiterbildung.

Das Referenzprojekt erfüllt mehrere Funktionen:

Aus der Praxis für die Praxis

Als Abstraktion tatsächlich stattgefundener Projekte und Prozesse bieten die Referenzprozesse eine realistische und leicht nachvollziehbare Abbildung dessen, was die Tätigkeiten eines IT Security Coordinators sind.

Prozessorientierung als innovatives „Curriculum“

Als vollständige Darstellung aller wichtigen Arbeitsprozesse sowie der dazugehörigen Qualifikationen, Tätigkeiten und Werkzeuge bieten die Referenzprozesse die Grundlage für die Weiterbildung zum IT Security Coordinator. Alle diese Prozesse müssen – entsprechend den Vorgaben – einmal oder mehrfach durchlaufen werden und ermöglichen dadurch den Weiterzubildenden den arbeitsplatznahen, integrativen Erwerb von relevanten Kompetenzen. Durch den Verbleib im Arbeitsprozess wird nicht nur für die Weiterzubildenden eine hohe Motivation (Arbeit an echten Projekten/Aufgaben) und Nachhaltigkeit erreicht, sondern auch – aus Sicht des Unternehmens – die Kontinuität und Qualität der laufenden Arbeiten gesichert (keine Ausfallzeit durch Seminartage, kein mühsamer Transfer).

Qualitätsstandard für die Weiterbildung

Als Referenz bieten insbesondere die Teilprozesse und die mit ihnen verbundenen Tätigkeits- und Qualifikationsziele einen Qualitätsmaßstab für die arbeitsprozessorientierte Weiterbildung und die resultierenden Abschlüsse. Vollständige Transparenz und klare Zielvorgaben ermöglichen die qualitativ hochwertige Absicherung auch komplexer Kompetenzen sowie den systematischen Erwerb des notwendigen Erfahrungswissens.

Transferprozesse

Die Generalisierung des Referenzprojekts aus der Praxis und seine didaktische Anreicherung ermöglichen eine leichte Auswahl angemessener Transferprozesse, deren Bearbeitung die Grundlage der Weiterbildung ist. Transferprozesse sind reale Prozesse, die Referenzprojekte in einer lernförderlichen Umgebung abbilden. Abgeschlossene Transferprozesse auf Basis der hier dargestellten Anforderungen und Qualitätsmaßstäbe sind nicht nur Qualifikationsnachweis des Einzelnen, sondern bilden auch die Basis eines angemessenen und zielgerichteteren Umgangs mit Geschäfts- und Arbeitsprozessen im Unternehmen.

1.1 Ereignis-Prozess-Ketten: Symbolik

Die Darstellung der Referenzprozesse in Form von Ereignis-Prozess-Ketten¹ ermöglicht einen schnellen Überblick. Vollständigkeit kann leicht überprüft werden, Anpassungen und

¹ Vgl. A.-W. Scheer, *Wirtschaftsinformatik*, Springer 1998.

Modifikationen in Hinblick auf das eigene Unternehmen sind problemlos möglich und Anknüpfungspunkte an andere Prozesse, aber auch zu weiterführenden Informationen ergeben sich automatisch.

Die bei der Darstellung der Referenz- und Teilprozesse verwendete Modellierungssprache stellt eine Anpassung und Weiterentwicklung der klassischen EPK-Modellierung dar:

- Referenz- wie Teilprozesse sind aus der Sicht des jeweiligen Spezialisten, also als Arbeitsprozesse einer Person dargestellt.
- Referenz- wie Teilprozesse stellen in der Regel keinen Geschäftsprozess dar.

Die EPK-Symbole werden hier wie folgt verwendet:

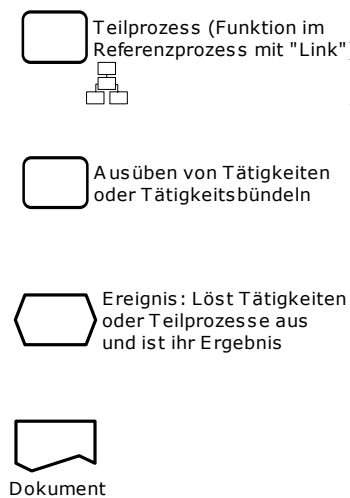



Abbildung 1: Grundlegende Symbole der Referenz- und Teilprozessmodelle.


Die wichtigsten Symbole sind:

- die Tätigkeiten bzw. Tätigkeitsbündel oder Teilprozesse, die mit dem Funktionssymbol dargestellt werden
- die Ereignisse, die Tätigkeiten bzw. Teilprozesse auslösen und Ergebnisse von Teilprozessen sind

Grundsätzlich gilt: Auf ein Ereignis folgt immer ein Teilprozess bzw. eine Tätigkeit.

Ergebnisse von Tätigkeiten sind sehr oft Dokumente, diese werden dann zusätzlich durch das Dokumentsymbol dargestellt.

 UND-Verknüpfung

 XOR-Verknüpfung

 ODER-Verknüpfung

Abbildung 2: Konnektoren.

Wenn Alternativmöglichkeiten bestehen, werden Ereignisse und Teilprozesse/Tätigkeiten über Konnektoren (AND, OR, XOR) verbunden. Dabei steht AND für ein verbindendes „Und“, OR für ein „Oder“, das alle Möglichkeiten offen lässt, und XOR für ein „ausschließendes Oder“, welches nur einen der angegebenen Pfade ermöglicht.

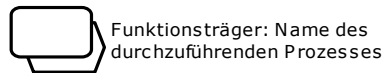


Abbildung 3: Schnittstelle.

Da die Prozesse aus der Sicht des jeweiligen Spezialisten formuliert werden, sind Schnittstellen zu Prozessen anderer Spezialisten oder zu Entscheidungsprozessen auf höherer Ebene notwendig. Dazu wird das Schnittstellensymbol verwendet. Es steht für Prozesse, die der Spezialist nicht selber durchführt, auf deren Durchführung er aber angewiesen ist. Parallel zu jeder Schnittstelle wird die Tätigkeit dargestellt, die der Spezialist selbst in diesem Zusammenhang ausübt, wie „Beraten bei ...“, „Unterstützen bei ...“ oder „Informieren des ...“.

Alle Prozesse werden durch die Verwendung dieser Symbole klar und einfach strukturiert dargestellt und sind offen für die Übertragung in konkrete Transferprozesse.

1.2 Referenzprozess und Teilprozesse

Der hier vorgestellte Referenzprozess und seine Teilprozesse stellen das Curriculum des Spezialistenprofils IT Security Coordinator dar.

Der Referenzprozess erhebt nicht den Anspruch eines Vorgehensmodells, sondern bildet beispielhaft den möglichen Arbeitsprozess und Verlauf eines Projekts auf Spezialistenebene ab.

Er bildet die Grundlage für Weiterbildungen und damit einen Qualitäts-, Niveau- und Komplexitätsmaßstab. Die zugehörigen Teilprozesse sind hier beispielhaft modelliert und stellen eine Möglichkeit der Durchführung dar. Einzelheiten zu den unverzichtbaren Prozessen und Kompetenzfeldern sind hier im Referenzprojekt festgelegt. Die Reihenfolge und die Inhalte der Teilprozesse sind abhängig vom jeweils auszuwählenden Transferprojekt und werden in diesem Zusammenhang festgelegt.

Die Darstellung der Prozesse erfolgt systematisch:

Jeder Prozess wird mithilfe von Ereignis-Prozess-Ketten dargestellt. Einem auslösenden Ereignis folgt eine Funktion, die wiederum ein oder mehrere Ereignisse als Ergebnis hat. Ereignisse und Funktionen können mit AND, OR oder XOR, den Konnektoren, verbunden sein.

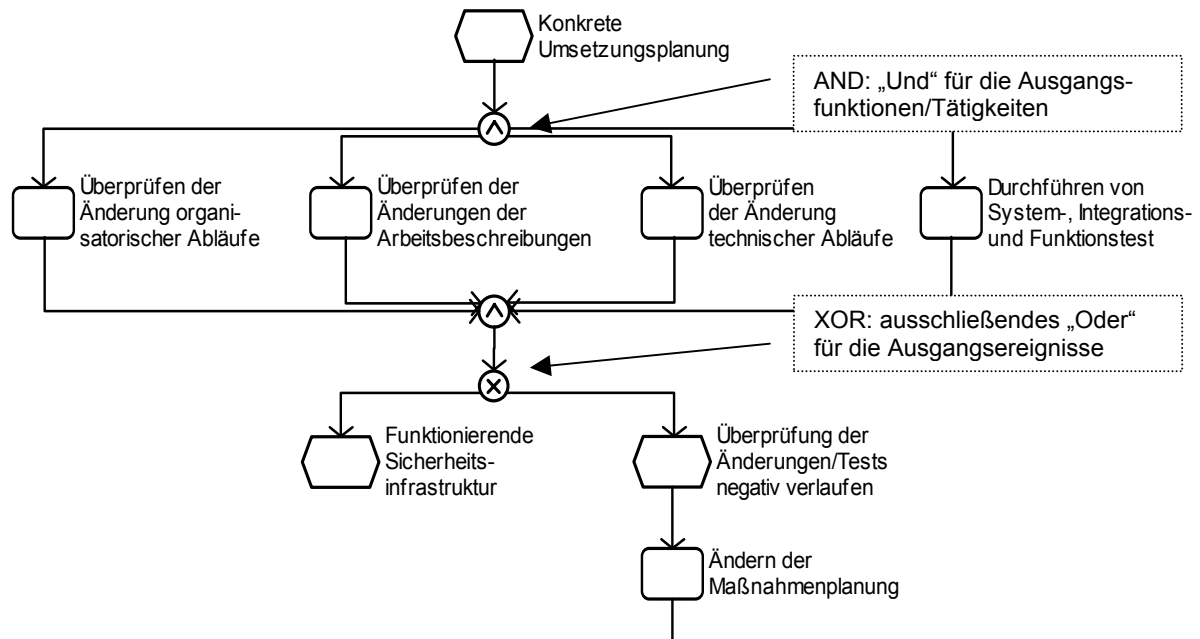


Abbildung 4: Beispielprozess mit unterschiedlicher Verwendung von Konnektoren.

Die Verbindung von Referenzprozess und Teilprozessen erfolgt über die Funktionen des Referenzprozesses:

Jede Funktion im Referenzprozess steht für einen Teilprozess.

Ereignisse, die dem jeweiligen Teilprozess direkt vor- oder nachgeordnet sind, sind Anfangs- und Endereignisse der jeweiligen Teilprozesse. Damit stellen die Teilprozesse die Funktionen des Referenzprozesses ausführlich dar, und ein Hin- und Herbewegen zwischen Referenz- und Teilprozessen ist jederzeit problemlos möglich.

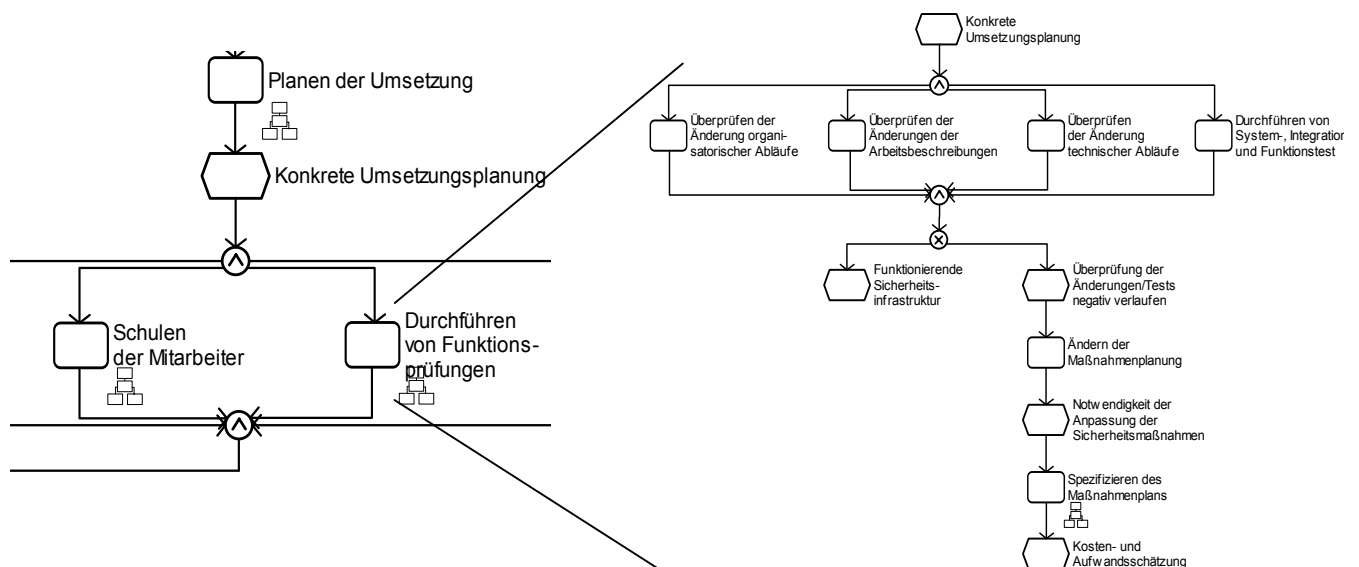


Abbildung 5: Ausschnitt aus dem Referenzprozess (links) und Zoom in den dazugehörigen Teilprozess „Durchführen von Funktionsprüfungen“ (rechts).

Die Teilprozesse stellen so die wesentlichen Teile eines Projekts dar und lassen sich entsprechend auf Transferprojekte übertragen. Den Teilprozessen sind die jeweils wesentlichen Tätigkeiten und Kompetenzfelder zugeordnet.

2 Das Profil: IT Security Coordinator (IT-Sicherheitskoordinator/in)

IT Security Coordinator² konzipieren angemessene IT-Sicherheitslösungen entsprechend den geltenden technischen Standards, Gesetzen und Vorschriften, begleiten deren Umsetzung und passen sie laufend den aktuellen Gegebenheiten an.

2.1 Tätigkeitsbeschreibung

IT Security Coordinator beraten und unterstützen Unternehmensleitung, Partner und Kunden bezüglich IT-Sicherheit. Sie konzipieren angemessene Sicherheitslösungen entsprechend den geltenden technischen Standards, Gesetzen und anderen Vorschriften und betreuen ihre Realisierung. Sie erarbeiten mit den Fachkräften der verschiedenen Bereiche und Ebenen gemeinsam Lösungen (Organisation, Personal, Infrastruktur, Hard- und Softwaremanagement), beraten bei der Umsetzung und protokollieren die Realisierung.

IT Security Coordinator analysieren Netzwerk- und arbeitsplatzspezifische Risiken und Schwachstellen, erstellen organisatorische und technische Sicherheitskonzepte gemeinsam mit den zuständigen Fachkräften und erarbeiten Richtlinien und Vorschriften zur Informationssicherheit. Sie realisieren IT-Sicherheitsmaßnahmen und entwickeln unter Berücksichtigung neuer Produkte sowie der wirtschaftlichen Gegebenheiten risikomindernde Maßnahmen und innovative Sicherheitsverfahren und führen sie ein. Sie schulen und sensibilisieren Nutzer.

2.2 Profiltypische Arbeitsprozesse

Die im Folgenden beschriebenen Teilprozesse dokumentieren den gesamten profiltypischen Arbeitsprozess des IT Security Coordinators. Die Beherrschung dieses Arbeitsprozesses in Verbindung mit den Kompetenzen in den jeweiligen Kompetenzfeldern und der Berufserfahrung bildet die Grundlage für die berufliche Handlungskompetenz.

1. Beraten bei der Konkretisierung von Sicherheitszielen und dem Entwurf von Sicherheitsleitlinien. Mitwirken bei der Vertragsgestaltung im IT-Umfeld
2. Durchführen der IT-Strukturanalysen, um eine aktuelle Bestandsaufnahme der IT und vorhandener Sicherheitsvorkehrungen zu erhalten
3. Beraten der Fachabteilungen (und ggf. der Partner) bei der Feststellung des Schutzbedarfs bezüglich Vertraulichkeit, Integrität und Verfügbarkeit der Systeme, Kommunikationsverbindungen, Anwendungen und Daten. Festlegen eindeutiger Verantwortlichkeiten
4. Aufstellen des Grundschutzmodells als Prüf- oder Entwicklungsplan
5. Unterstützen der Fachabteilungen (und ggf. der Partner) bei der Durchführung von Soll-Ist-Vergleichen, bei besonderen Schutzbedürfnissen einschließlich ergänzender Sicherheitsanalysen für besonders gefährdete und schutzbedürftiger Bereiche; Erstellen von Maßnahmenplänen

² Kapitel 2: „Das Profil: IT Security Coordinator (IT-Sicherheitskoordinator/in)“ gibt den offiziellen Text der „Vereinbarung über die Spezialistenprofile im Rahmen des Verfahrens zur Ordnung der IT-Weiterbildung“ vom 25.05.2002 (Bundesanzeiger 105, ausgegeben am 12.06.2002) wieder.

6. Überprüfen und Detaillieren der Maßnahmenpläne hinsichtlich Notwendigkeit, Anpassungsbedarf und Durchsetzungsmöglichkeiten
7. Schätzen der Kosten und des Aufwands; falls notwendig: Analysieren, Bewerten und Auswählen von am Markt angebotenen Sicherheitsprodukten
8. Präsentieren der entwickelten Vorschläge bei Entscheidern
9. Planen der Umsetzung von Maßnahmen bezüglich Reihenfolge und Verantwortlichkeiten
10. Begleiten der Umsetzung der festgelegten Maßnahmen (organisatorische oder technische Lösungen, Einsatz von Hard- oder Software) in den verschiedenen Aufgabefeldern (Infrastruktur, Organisation, Datensicherheit, Datenschutz, Virenschutz, Kryptokonzept, Hard- und Softwaremanagement)
11. Durchführen und Dokumentieren von Funktionsprüfungen
12. Unterstützen der Partner bei der Realisierung sicherheitstechnischer Maßnahmen und ggf. bei der Anbindung und Synchronisation der Systeme
13. Erstellen von Konzepten zur Schulung und Sensibilisierung der Nutzer, Durchführen von Schulungen
14. Durchführen von Revisionen und Aktualitätsprüfungen der durchgeführten Sicherheitsmaßnahmen; Ändern und Anpassen der Sicherheitsmaßnahmen, erneutes Modellieren von Schutzmodellen und Prüfplänen
15. Vertreten des Unternehmens nach außen (Partner, Kunden, Verbände) in Sicherheitsfragen

2.3 Profilprägende Kompetenzfelder

Die Beherrschung der profiltypischen Arbeitsprozesse setzt Kompetenzen unterschiedlicher Reichweite in den nachstehend aufgeführten beruflichen Kompetenzfeldern³ voraus. Den Kompetenzfeldern sind Wissen und Fähigkeiten sowie typische Methoden und Werkzeuge unterschiedlicher Breite und Tiefe zugeordnet.

Grundlegend zu beherrschende, gemeinsame Kompetenzfelder⁴:

- Unternehmensziele und Kundeninteressen
- Problemanalyse, -lösung
- Kommunikation, Präsentation
- Konflikterkennung, -lösung
- fremdsprachliche Kommunikation (englisch)
- Projektorganisation, -kooperation
- Zeitmanagement, Aufgabenplanung und -priorisierung
- wirtschaftliches Handeln
- Selbstlernen, Lernorganisation
- Innovationspotenziale
- Datenschutz, -sicherheit
- Dokumentation, -standards
- Qualitätssicherung

³ Die Kompetenzfelder werden in der nachfolgenden Auflistung jeweils durch ein zusammenfassendes Stichwort benannt. Da die Weiterbildung zum Spezialisten auf die erfolgreiche Bewältigung zunehmend offener beruflicher Handlungssituationen sowie ganzheitlichen Kompetenzerwerb abzielt, bildet der Kompetenzerwerb einen integralen Bestandteil der Arbeits- und Weiterbildungsprozesse und lässt sich nur im Zusammenhang mit diesen operationalisieren (vgl. dazu die Abschnitte „Kompetenzfelder“ in den Kapiteln 3.1.3ff)

⁴ Jeder Spezialist muss in den in diesem Abschnitt genannten „weichen“ Kompetenzfeldern wie „Kommunikation, Präsentation“, „Konflikterkennung, -lösung“ usw. ein Niveau erreichen, das über dem einer Fachkraft liegt. Das heißt, er muss auch in diesen Feldern zu eigenständigem Handeln in der Lage sein und zum Erreichen des Ziels in dem jeweiligen Feld ggf. über den Rahmen bekannter Verfahren und Lösungen hinausgehen können.

Fundiert zu beherrschende, gruppenspezifische Kompetenzfelder:

- Systemanalyse, -modellierung, -entwicklung, -integration
- Entwicklungsstandards (Leistungsfähigkeit, Sicherheit, Verfügbarkeit, Innovation)
- Engineering-Prozesse
- Analysemethoden, -strategien, -muster
- Design-Methoden
- Qualitätsstandards
- vernetztes Denken
- Wirtschaftlichkeitsanalysen
- Marktüberblick
- nutzerorientierte Problemanalyse, -lösung
- Projektplanung und -management
- Moderation

Routiniert zu beherrschende, profilspezifische Kompetenzfelder:

- Informationstechnologie: Netzwerke, Protokolle, Betriebssysteme, Anwendungen
- System- und Netzmodellierung
- Sicherheitsanforderungen und -lösungen
- Sicherheitsüberwachung, Schutzstrategien und -methoden
- rechtliche Grundlagen
- Datenschutz
- Verschlüsselung
- Wirtschaftlichkeitsanalysen
- Projektspezifikation, -überwachung
- Risikomanagement

2.4 Qualifikationserfordernisse

Im Regelfall wird ein hinreichendes Qualifikationsniveau auf der Basis einschlägiger Berufsausbildung oder Berufserfahrung vorausgesetzt.

2.5 Einordnung ins System und Karrierepfade

Das neue IT-Weiterbildungssystem gibt auf Basis der vier neuen IT-Ausbildungsberufe drei Ebenen für die Weiterqualifizierung vor: Spezialisten, wie auch der IT Security Coordinator einer ist, operative und strategische Professionals. Auf der Ebene der Spezialisten existieren eine Reihe verwandter Profile, und selbstverständlich kann sich auch der IT Security Coordinator zu einem Professional weiterqualifizieren.

Verwandte Profile

Der IT Security Coordinator weist eine Reihe verwandter Profile auf. Da der IT Security Coordinator für die Sicherheit von IT-Systemen und Netzen verantwortlich ist, überschneiden sich seine Aufgabengebiete mit denen der Administratoren, insbesondere denen des IT Systems Administrator, des Network Administrator und des Web Administrator.

Eine enge Verbindung besteht aufgrund der gemeinsamen Thematik auch zum Security Technician: Schwerpunkt beider Profile ist die Sicherheit. Allerdings kümmert sich der Security Technician speziell um Zugangskontrollen und andere Sicherungssysteme; er hat seinen Schwerpunkt also im Bereich technischer Komponenten und weniger – wie der IT Security Coordinator – in den Bereichen Software und Kommunikation/Koordination.

Strukturelle Ähnlichkeiten haben die Aufgaben des IT Security Coordinators mit denen des IT Quality Management Coordinator: Beider Tätigkeit ist geprägt von dem Erreichen und Aufrechterhalten von Standards, von einer Mischung aus ständig durchzuführenden Arbeiten, auch Kontrollen und eher seltenen Projekten.

Aufstiegsqualifizierung

Das Tätigkeitsfeld des IT Security Coordinators ist eine ideale Grundlage für Aufstiegsqualifizierungen insbesondere zum IT Business Consultant mit dem Schwerpunkt IT-Sicherheit und zum IT Business Manager mit den Schwerpunkten Koordinieren, Steuern und Unterstützen von Projekten und Prozessen, die die Unternehmenssicherheit betreffen.

3 Referenzprozess

Der Referenzprozess des IT Security Coordinators ist geprägt durch zwei große, unterschiedliche Abschnitte:

1. Koordinieren und Aufrechterhalten der IT-Sicherheit im täglichen Geschäft
2. Konzipieren und Umsetzen sicherheits- oder datenschutzrelevanter Projekte

3.1 IT-Sicherheitskoordination

Der Referenzprozess des IT Security Coordinators besteht – kurz zusammengefasst – aus folgenden ineinander greifenden Teilen:

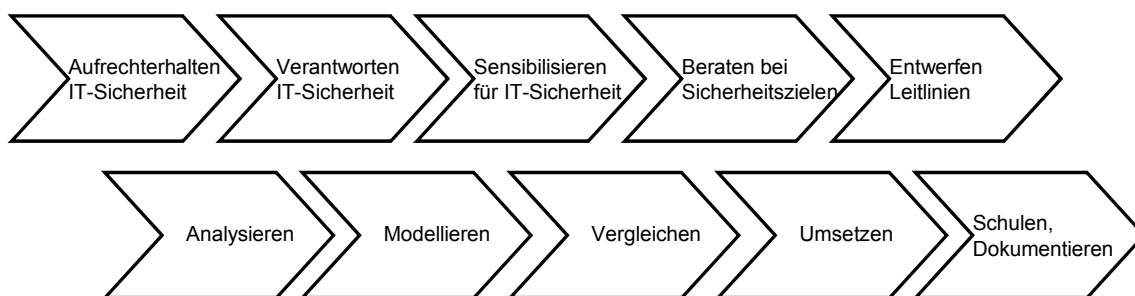


Abbildung 6: Zusammenfassung des Referenzprozesses „IT-Sicherheitskoordination“.

Diese Prozesse werden im Folgenden ausführlich dargestellt:

Der Referenzprozess gibt die Tätigkeiten des IT Security Coordinators auf hohem Abstraktionsniveau wieder und ermöglicht so einen Überblick.

Mit den Teilprozessen wird in den Referenzprozess hineingezoomt. Die Teilprozesse entsprechen damit in etwa der Abbildung von Arbeitsprozessen; sie stellen einen konkreten Tätigkeitsverlauf, einschließlich auslösendem Ereignis und Ergebnis, dar.

Die zur Durchführung der Teilprozesse notwendigen Tätigkeiten und Kompetenzfelder werden jeweils in einem separaten Abschnitt aufgelistet.

Das Praxisprojekt dient als Beispiel zur Konkretisierung und Veranschaulichung. Es ist ein echtes, bereits durchgeführtes Projekt, auf dessen Grundlage die hier dargestellten Referenz- und Teilprozesse entwickelt wurden.

3.1.1 Referenzprozess IT-Sicherheitskoordination

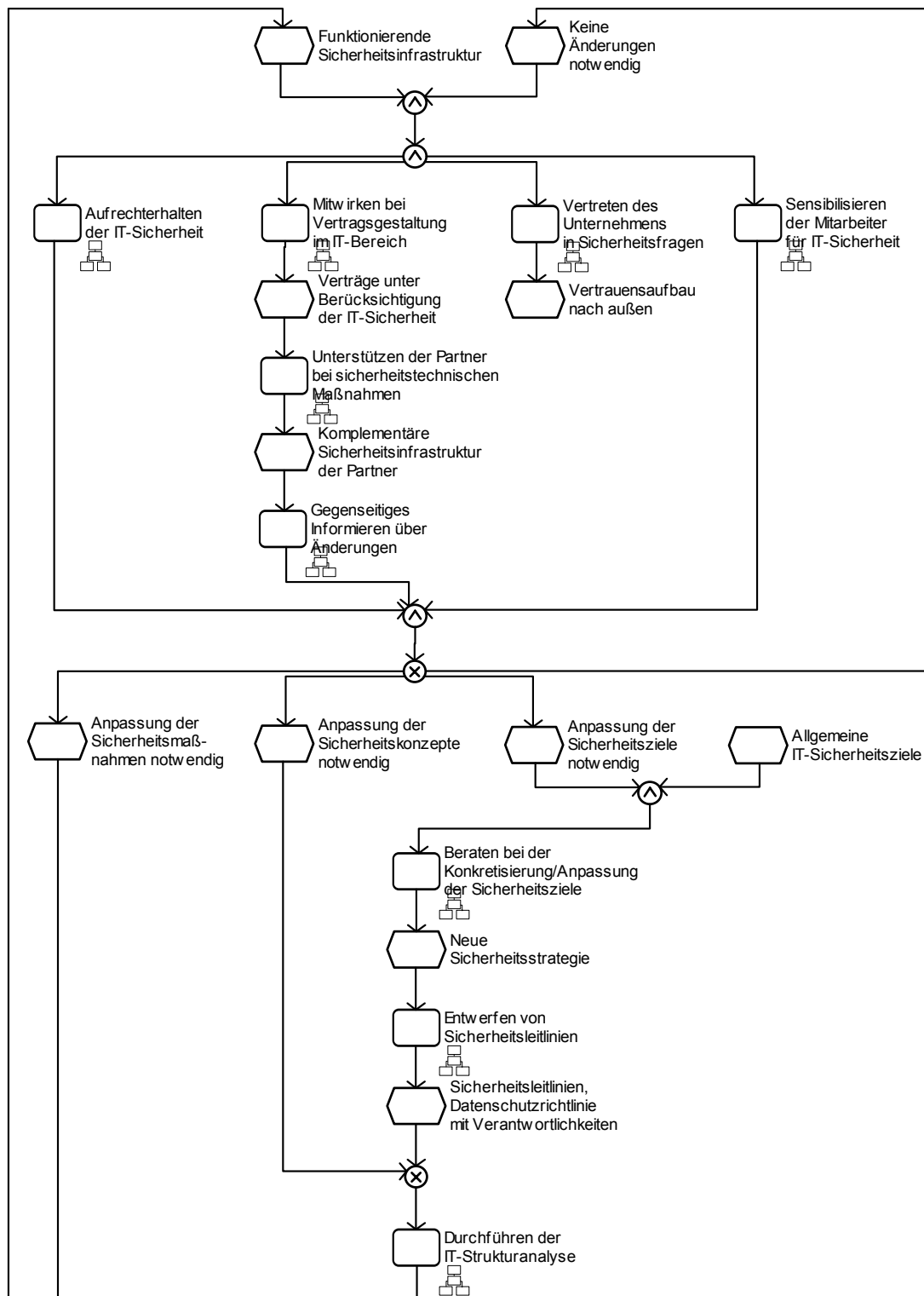


Abbildung 7: Referenzprozess IT Security Coordinator, Teil 1.

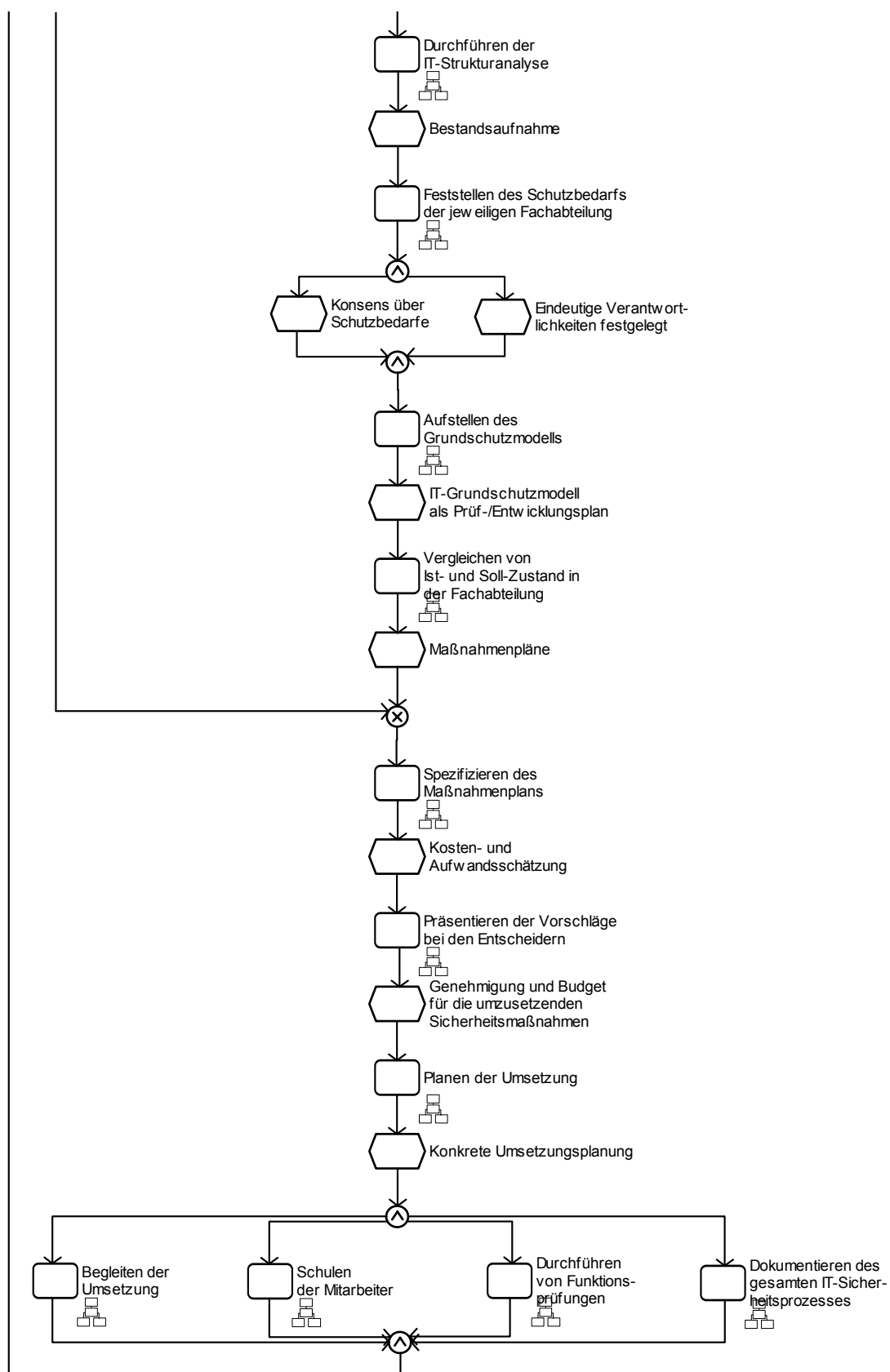


Abbildung 8: Referenzprozess IT Security Coordinator, Teil 2.

Der Prozess „Koordinieren der IT-Sicherheit“ basiert auf zwei sehr wesentlichen Annahmen:

1. Das Unternehmen, in dem der IT Security Coordinator tätig ist, hat bereits Sicherheitsziele festgelegt und einen Sicherheitsprozess - zumindest in Ansätzen - eingerichtet.
2. Die Verantwortung für die IT-Sicherheit liegt bei der Unternehmensleitung bzw. dem Management. In den Begriffen des IT-Weiterbildungssystems ausgedrückt bedeutet dies, dass die strategischen Leitaussagen zur IT-Sicherheit von den strategischen Professionals getroffen, die konzeptionellen Vorgaben und organisatorischen Rahmenbedingungen von einem operativen Professional geschaffen werden. Aufgrund seiner fachlichen Kompetenz kann der IT Security Coordinator bei diesen Aufgaben beratend hinzugezogen werden.

Der Referenzprozess des IT Security Coordinators ist also typisch für einen Lösungsentwickler auf Spezialistenebene, der in einem Unternehmen angesiedelt ist:

1. Der IT Security Coordinator hält die IT-Sicherheit aufrecht, ist Ansprechpartner für IT-bezogene Vertragsgestaltung insbesondere mit Partnern oder Auftragnehmern, unterstützt die Partner und kommuniziert mit ihnen über Änderungen. Wichtige Teile seiner täglichen Aufgaben sind auch die Vertretung des Unternehmens in Sicherheitsfragen nach außen und nach innen, also das Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für Sicherheitsfragen. In dieser Funktion ist der IT Security Coordinator auch Ansprechpartner für alle (potenziell) sicherheitsrelevanten Fragen und Hinweise.
2. Stehen sicherheits- oder datenschutzrelevante Änderungen ins Haus, unterstützt und berät der IT Security Coordinator beim Aufstellen der Sicherheitsziele und -strategien, entwickelt Sicherheitsleitlinien, analysiert die Gegebenheiten im Unternehmen, gleicht – in enger Zusammenarbeit mit den betroffenen Mitarbeiterinnen und Mitarbeitern sowie Abteilungen – Soll- und Ist-Zustand ab und leitet daraus Maßnahmen ab. Die Umsetzung dieser Maßnahmen wird von ihm – nach der Freigabe – geplant und überwacht. Der Schwerpunkt liegt aber auch hier wieder auf der Kommunikation und Kooperation mit den Mitarbeiterinnen und Mitarbeitern, die von den Maßnahmen betroffen sind. Auch die in einem solchen Change Management durchgeführten Änderungen werden Bestandteil der täglichen Arbeit des IT Security Coordinators und müssen im Rahmen der Aufrechterhaltung der IT-Sicherheit überprüft und gesichert werden.

Dieser Prozess läuft in kleinen wie in großen Unternehmen ab, die die Funktion „IT-Sicherheitskoordination“ definiert haben. Relevante Änderungen ergeben sich, wenn ein Experte für IT-Sicherheit von außen in das Unternehmen kommt. Dann wird mit dem zweiten Teil des Prozesses begonnen und in diesem Rahmen sicherlich die Funktion „interne, ständige Sicherheitskoordination“ errichtet.

Nicht in jedem Unternehmen und jedem Projekt wird jeder Teilprozess den gleichen Umfang und die gleiche Komplexität haben. Der Referenzprozess umfasst aber alle relevanten Funktionen, die ein IT Security Coordinator beherrschen muss.

Integraler Bestandteil der Tätigkeiten und Prozesse eines IT Security Coordinators ist die Beachtung und Aufrechterhaltung des Datenschutzes im Unternehmen. Genauso wie er für die Sicherheit verantwortlich ist, ist er auch für den Schutz personenbezogener Daten zuständig. Da die zur Aufrechterhaltung von Datensicherheit und Datenschutz notwendigen Maßnahmen eng verwandt, teilweise identisch sind, werden sie in diesem einen Profil zusammengefasst.

Für den zweiten Teil des Referenzprozesses gibt das „BSI-Grundschutzhandbuch“ einen Leitfaden für die Vorgehensweisen und Methoden bei der Erstellung eines unternehmensweiten IT-Sicherheitsprozesses vor. In Deutschland gilt das BSI-Grundschutzhandbuch als Quasi-Standard und wird bei Behörden und Institutionen regelmäßig angewandt. Es ist kostenlos beim Bundesamt für Sicherheit in der Informationstechnik (BSI) erhältlich und steht auch online zur Verfügung (www.bsi.de/gshb). Daher wird in den Teilprozessen regelmäßig auf die relevanten Abschnitte im BSI-Grundschutzhandbuch verwiesen.

Das IT-Grundschutzhandbuch beschreibt detailliert Standard-Sicherheitsmaßnahmen, die praktisch für jedes IT-System zu beachten sind. Es umfasst:

- Standardsicherheitsmaßnahmen für typische IT-Systeme mit „normalem“ Schutzbedarf
- eine Darstellung der pauschal angenommenen Gefährdungslage
- ausführliche Maßnahmenbeschreibungen als Umsetzungshilfe
- eine Beschreibung des Prozesses zum Erreichen und Aufrechterhalten eines angemessenen IT-Sicherheitsniveaus
- eine einfache Verfahrensweise zur Ermittlung des erreichten IT-Sicherheitsniveaus in Form eines Soll-Ist-Vergleichs

Arbeitet ein Unternehmen international, so kann als weiterer Standard der British Standard 7799 bzw. ISO 17799 in Betracht kommen.

BS 7799 befasst sich hauptsächlich mit dem Aufbau eines IT-Sicherheitsmanagements und seiner Verankerung in der Organisation. Anders als im IT-Grundschutzhandbuch finden sich hier keine detaillierten Umsetzungshinweise, sondern übergreifende Anforderungen.

3.1.2 Das Beispielprojekt: Anbindung von Außenstellen über VPN

Eine Firma plant, mehrere Außenstellen über VPN (Virtual Private Network) an das Unternehmensnetz der Hauptstelle anzubinden.

Einige Außenstellen werden bei Bedarf eingerichtet und sollen, wie die festen Außenstellen auch, auf bestimmte Daten, die in der Hauptstelle zur Verfügung gestellt werden, sicher zugreifen können.

Die Idee besteht darin, Geschäftsprozesse im eigenen Haus zu vereinfachen und den Außenstellen schnelleren, gesicherten Zugriff auf die Daten und Ressourcen über das Internet zu ermöglichen.

Da es sich bei einigen der Außenstellen um eigenständige Kompetenzzentren handelt, müssen diese vom Aufwand solch einer Maßnahme überzeugt und zur Unterstützung der Durchführung gewonnen werden.

Der Kunde hat sich bereits mit der IT-Sicherheit beschäftigt und möchte sein bisheriges Sicherheitskonzept überarbeiten und an die neuen Gegebenheiten anpassen.

Da dieses Beispielprojekt nicht alle Teilprozesse des IT Security Coordinators abdeckt, wird es teilweise durch andere Beispiele ergänzt. Auch in der Umsetzung, also in den Qualifizierungsprojekten potenzieller IT Security Coordinator können die Teilprozesse auf mehrere Qualifizierungsprojekte aufgeteilt werden.

3.1.3 Prozesskompass IT-Sicherheitskoordination

1. Aufrechterhalten der IT-Sicherheit
2. Mitwirken bei der Vertragsgestaltung im IT-Bereich
3. Vertreten des Unternehmens in Sicherheitsfragen nach außen
4. Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit
5. Unterstützen der Partner bei sicherheitstechnischen Maßnahmen
6. gegenseitiges Informieren der Partner über sicherheitsrelevante Änderungen
7. Beraten bei der Anpassung und Konkretisierung der Sicherheitsziele
8. Entwerfen der Sicherheitsleitlinien
9. Durchführen von IT-Strukturanalysen
10. Feststellen des Schutzbedarfs der Fachabteilungen
11. Aufstellen des Grundschutzmodells
12. Vergleichen von Ist- und Soll-Zustand in den Fachabteilungen
13. Spezifizieren des Maßnahmenplans
14. Präsentieren der Vorschläge bei den Entscheidern
15. Planen der Umsetzung
16. Begleiten der Umsetzung
17. Schulen der Mitarbeiterinnen und Mitarbeiter
18. Durchführen von Funktionsprüfungen
19. Dokumentieren des gesamten IT-Sicherheitsprozesses

Die genannten Teilprozesse geben den Prozess IT-Sicherheitskoordination ausführlich und detailliert wieder. Sie entsprechen den realen Gegebenheiten und dem Projekt, welche als Grundlage für den Referenz- und die Teilprozesse gedient haben und als Beispiel zur Veranschaulichung beschrieben werden.

3.1.3.1 Aufrechterhalten der IT-Sicherheit

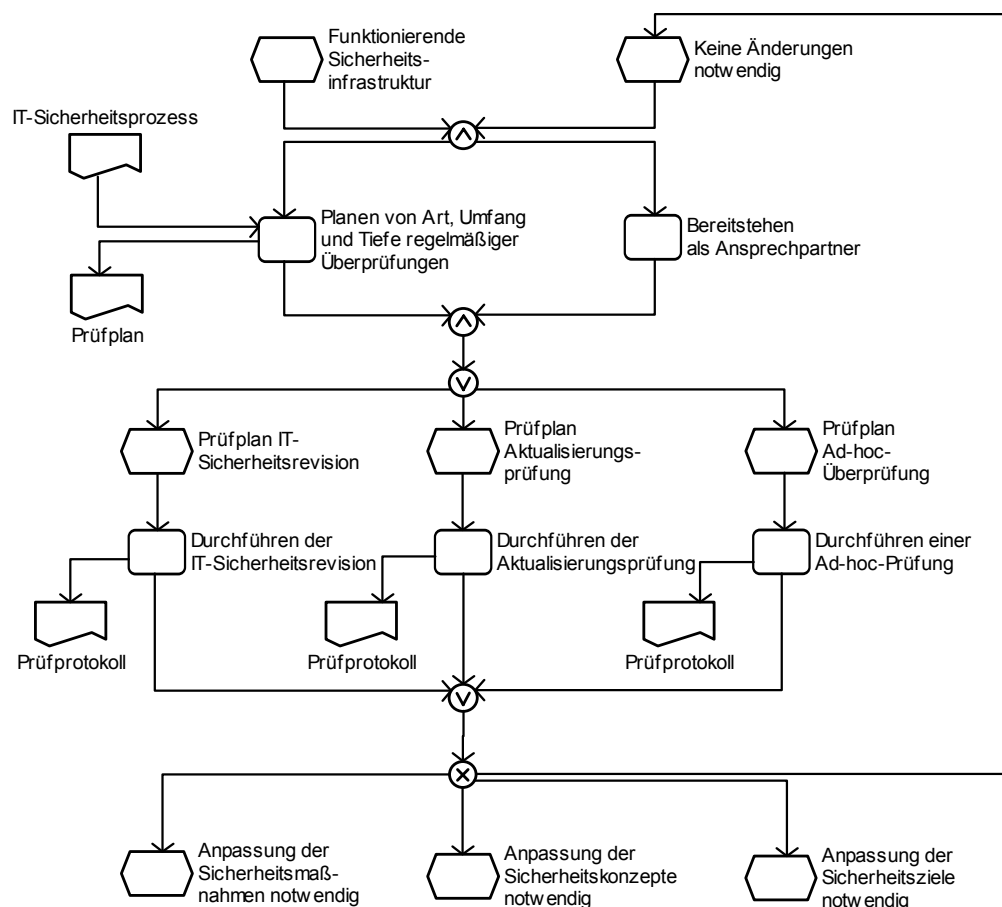


Abbildung 9: Aufrechterhalten der IT-Sicherheit.

In diesem Teilprozess wird nur die (technische) Überprüfung der IT-Sicherheit beschrieben. Zur vollständigen Aufrechterhaltung der IT-Sicherheit gehören alle Teilprozesse des ersten Abschnitts des Gesamtprozesses, also auch die Mitarbeit bei der Vertragsgestaltung, das Sensibilisieren der Mitarbeiterinnen und Mitarbeiter sowie die Kooperation mit Partnern, soweit sie für die IT-Sicherheit relevant ist.

Speziell für die Aufrechterhaltung der IT-Sicherheit sind die Hinweise des BSI-Grundschutzhandbuchs M 2.199 relevant.

3.1.3.1.1 Tätigkeiten: Aufrechterhalten der IT-Sicherheit

- Planen von Art, Umfang und Tiefe regelmäßiger Überprüfungen der vorhandenen IT-Sicherheitsinfrastruktur;
- Bereitstehen als ständiger Ansprechpartner/in für sicherheitsrelevante Fragen und Hinweise
- Durchführen von IT-Sicherheitsrevisionen
- Durchführen von Aktualisierungsprüfungen
- Durchführen von Ad-hoc-Prüfungen bei (potenziell) sicherheitsrelevanten Hinweisen oder Vorkommnissen

3.1.3.1.2 Kompetenzfelder: Aufrechterhalten der IT-Sicherheit

Fähigkeiten/Fertigkeiten

- Sicherheits-, Datenschutz-, Erfolgs-, Misserfolgskriterien sowie entsprechende Vorgaben in prüfbare Kriterien und messbare Kenngrößen übersetzen können
- Beurteilungskriterien ableiten können
- spezielle Risiken kennen und erkennen („erahnen“) können
- gesetzliche Grundlagen und Regeln bzgl. IT-Sicherheit und Datenschutz anwenden können
- Prüfpläne (Zeit, Prüfgegenstände, Meilensteine etc.) für die unterschiedlichen Bereiche und Aufgaben erstellen können
- Einzelpläne sinnvoll zu einem Gesamtplan zusammenführen/synchronisieren können
- automatische Überwachungstools auswählen und mit diesen umgehen können
- mit unterschiedlichen Mitarbeiterinnen und Mitarbeitern des Unternehmens angemessen (Ansprache, Kommunikationsmedien, Verhalten) kommunizieren können
- von Mitarbeiterinnen und Mitarbeitern mitgeteilte sicherheitsrelevante Vorkommnisse in ihrer Relevanz einschätzen können
- informelle Gespräche mit Mitarbeiterinnen und Mitarbeitern führen können, dabei Vertrauensverhältnisse aufbauen und pflegen
- offene (ggf. auch anonyme) Kommunikationsmöglichkeiten einrichten und betreuen können, z. B. Sicherheitssprechstunden, Web-Forum im Unternehmens-Intranet o. Ä.
- Logfiles und Meldungen von Überwachungstools auswerten und angemessene Maßnahmen einleiten können
- Sicherheitsrevisionen und Aktualisierungsprüfungen durchführen können, ggf. gemeinsam mit den Zuständigen (z. B. Administratoren)
- Sicherheitsrevisionen und Aktualisierungsprüfungen sowie Ad-hoc-Prüfungen dokumentieren und protokollieren können
- Ergebnisse der Prüfungen auswerten und auf Relevanz für Sicherheitsmaßnahmen beurteilen können

Wissen

- konkrete Anwendung sicherheits- und datenschutzrelevanter Gesetze, Standards und Normen im Unternehmen
- Sicherheitsniveau, -maßnahmen und -infrastruktur des Unternehmens
- informationstechnische Sicherheits- und Schutzmaßnahmen, ihre Funktionsweise, Aufgaben und Risiken
- Datenschutzmaßnahmen und ihre Funktionsweise, Aufgaben und Risiken
- Informationsmöglichkeiten über aktuelle sicherheitsrelevante Vorkommnisse (Mailing-Listen, Security Advisories, Bugreports etc.) und Schutzmaßnahmen
- Risiken in und für informationstechnische Systeme
- Kommunikationsmodelle
- Elemente und Regeln verbaler und nonverbaler Kommunikation
- typische Kommunikationsmuster und Umgang mit diesen
- typische Konflikte, deren Ursachen und Symptome
- Prüfpläne und ihre Gestaltung
- Prüf- und Überwachungsmöglichkeiten für Systeme und Risiken

Werkzeuge/Methoden

- Monitoring Tools
- Ablauf- und Terminmanagement

3.1.3.1.3 Beispiel: Aufrechterhalten der IT-Sicherheit

Die Überprüfung zur Aufrechterhaltung der IT-Sicherheit erfolgt im Live-Betrieb in gewissen Zeitabständen, nach System- und Netzwerkupgrades, nach der Migration zu neuen Technologien, nach dem Anschluss an neue Netzwerke, nach dem erstmaligen Internet-, Intranet-, Extranet-Anschluss oder nach der Installation neuer Basissoftware.

Im konkreten Fall wurde dazu ein automatisiertes Managed Vulnerability Assessment Tool eingesetzt, das periodisch die Sicherheit der öffentlich zugänglichen Systeme, aber auch von bestimmten internen Systemen prüft.

Der IT Security Coordinator erhält mithilfe dieses Tools Auswertungen und detaillierte Hinweise, wo Schwachstellen zu finden sind und wie diese behoben werden können.

3.1.3.2 Mitwirken bei der Vertragsgestaltung im IT-Bereich

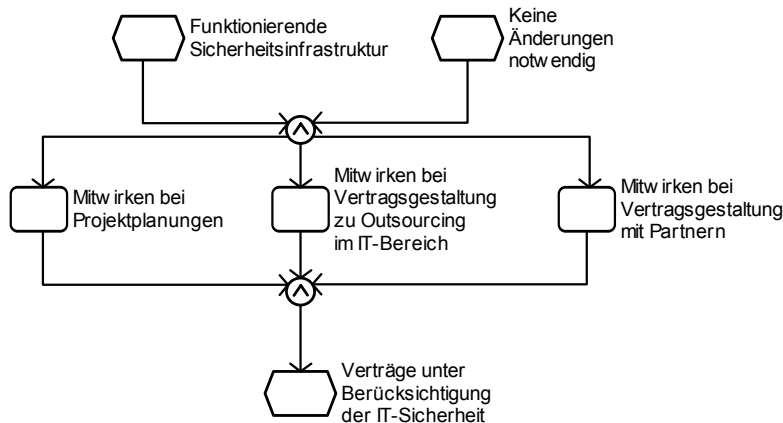


Abbildung 10: Mitwirken bei der Vertragsgestaltung im IT-Bereich.

3.1.3.2.1 Tätigkeiten: Mitwirken bei der Vertragsgestaltung im IT-Bereich

- Mitwirken bei Projektplanungen
- Mitwirken bei der Vertragsgestaltung beim Outsourcing von Aufgaben und Funktionen im IT-Bereich
- Mitwirken bei Vertragsgestaltung mit Partnern, soweit sie für IT relevant sind, beispielsweise bei der gemeinsamen Nutzung von Netzen, Plattformen o. Ä.

Das Ziel dieser Tätigkeiten des IT Security Coordinators ist es, so frühzeitig wie eben möglich sicherheits- und datenschutzrelevante Belange in Projekte und Verträge einbringen zu können. Die konkrete Ausgestaltung dieser Tätigkeiten ist vom Umfeld, vom Unternehmen und von jedem Einzelfall abhängig. Da IT-Sicherheit wie Datenschutz nicht selbstverständlich berücksichtigt werden, muss der IT Security Coordinator als Lobbyist für Sicherheit und Datenschutz wirken.

3.1.3.2.2 Kompetenzfelder: Mitwirken bei der Vertragsgestaltung im IT-Bereich

Fähigkeiten/Fertigkeiten

- in Projektplänen sicherheits- und datenschutzrelevante Vorhaben und Aspekte erkennen können
- bei Vorhaben und Vertragsverhandlungen sicherheits- und datenschutzrelevante Vorhaben und Aspekte erkennen können
- kostenintensive Risiken in und für Sicherheitsinfrastrukturen einschätzen und ggf. notwendige Änderungen in der Vertragsgestaltung vorschlagen können
- sinnvolle, inhaltlich, technisch und kostenmäßig angemessene Vorschläge für Maßnahmen zur Einhaltung von Vorschriften in Projekten und Vorhaben machen können

Wissen

- sicherheitsrelevante Gesetze, Standards und Normen und ihre konkrete Anwendung im Unternehmen
- datenschutzrelevante Gesetze und Normen (Bundesgesetz über den Datenschutz DSG vom 19. Juni 1992, Verordnung zum Bundesgesetz über den Datenschutz VDSG vom 14. Juni 1993; Grundgesetz, Bürgerliches Gesetzbuch, Strafgesetzbuch, Datenschutzgesetze der Länder, Sozialgesetzbuch, Handelsgesetzbuch,

Personalvertretungsgesetz, Betriebsverfassungsgesetz, Urheberrechtsgesetz, Patentgesetz, Informations- und Kommunikationsdienstegesetz IuKDG, Gesetz zur Kontrolle und Transparenz im Unternehmen KonTraG) und ihre Anwendung im Unternehmen

- Vertragsgestaltung
- IT-Infrastrukturen und ihre Gestaltungs- und Anbindungsmöglichkeiten
- Sicherheitssysteme und ihre Möglichkeiten

3.1.3.2.3 Beispiel: Mitwirken bei der Vertragsgestaltung im IT-Bereich

Ein typisches, aber fiktives Beispiel für die Missachtung datenschutzrelevanter Probleme ist die Einführung eines Customer-Relationship-Management-Systems (CRM) in einem Unternehmen. Kundendaten, die weit über das für den üblichen Geschäftsverkehr Notwendige hinausgehen (z. B. Geburts- oder Hochzeitsdaten der Ansprechpartner) werden gesammelt, gespeichert, ausgewertet, sind einer Vielzahl von Mitarbeitern zugänglich und werden schlimmstenfalls sogar weiterverkauft. Oftmals geschieht dies ohne Beachtung des Datenschutzes und ohne Rechtsgrundlage. Hier kann der IT Security Coordinator beratend tätig werden.

Ein weiteres, ebenfalls fiktives Beispiel: Ein Unternehmen will einen Teil der Administration seiner IT-Infrastruktur extern vergeben. Dafür wird einem entsprechenden Dienstleister ein Zugriff für die Fernwartung des Netzes eingerichtet. Bei den Vertragsverhandlungen mit dem Dienstleister wird der IT Security Coordinator u. a. auf die Rechtsverwaltung und die Absicherung des Zugriffs achten. Eine weitere wichtige Aufgabe des IT Security Coordinators ist die Ausgestaltung des Sicherheitsparagraphen in den Service Level Agreements (SLAs).

3.1.3.3 Vertreten des Unternehmens in Sicherheitsfragen nach außen

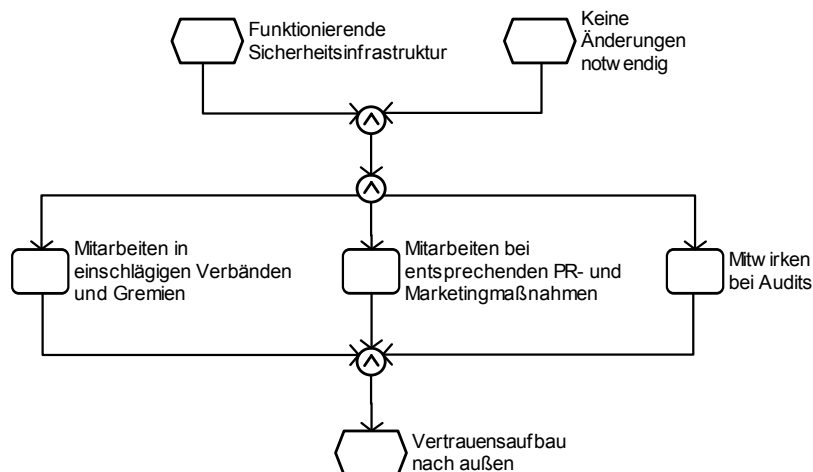


Abbildung 11: Vertreten des Unternehmens in Sicherheitsfragen nach außen.

3.1.3.3.1 Tätigkeiten: Vertreten des Unternehmens in Sicherheitsfragen nach außen

- Mitarbeiten in einschlägigen Verbänden und Gremien
- Mitwirken bei die IT-Sicherheit oder den Datenschutz betreffenden PR- oder Marketing-Maßnahmen
- Mitwirken bei sicherheitsrelevanten Audits

Diese Tätigkeiten dienen alle dem Ziel des Vertrauensaufbaus nach außen. Auch hier hängt die konkrete Ausgestaltung vom Einzelfall ab.

3.1.3.3.2 Kompetenzfelder: Vertreten des Unternehmens in Sicherheitsfragen nach außen

Fähigkeiten/Fertigkeiten

- Relevanz der Mitarbeit in Verbänden und Gremien (regional und überregional) für den Vertrauensaufbau nach außen einschätzen können
- Sicherheitsprobleme und ihre Lösungen in geeigneter Weise nach außen kommunizieren können
- Sicherheitsprobleme anderer auf ihre Relevanz für das eigene Unternehmen einschätzen können
- Präsentationen und Themen aufbereiten und vortragen können
- relevante Themen für PR und Marketing auswählen, beurteilen und bei der angemessenen Aufbereitung mitwirken können
- Überprüfungen (Reviews, Audits, Revisionen) vorbereiten können

Wissen

- für IT-Sicherheit relevante Verbände, Institutionen, Gremien und Mitwirkungsmöglichkeiten
- Fachzeitschriften und Kommunikationsforen im Internet
- Grundkenntnisse der Unternehmenskommunikation und des Marketings
- aktuelle Sicherheitsthemen

Werkzeuge/Methoden

- Reviews, Audits, Revisionen
- Präsentationstechnik

3.1.3.4 Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit

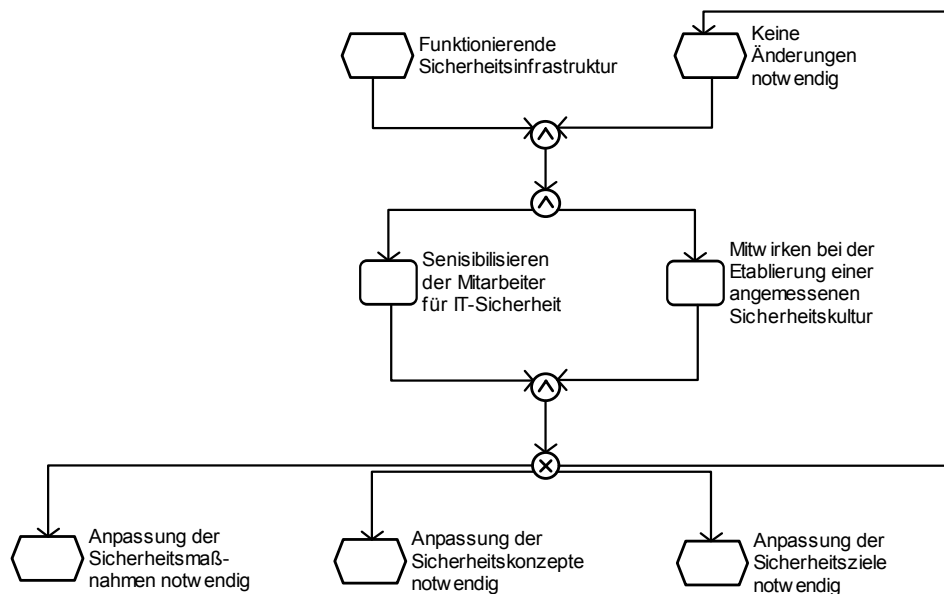


Abbildung 12: Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit.

3.1.3.4.1 Tätigkeiten: Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit

- Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit; vgl. hierzu BSI-Grundschutzhandbuch: M 2.198
- Mitwirken bei der Etablierung einer angemessenen Sicherheitskultur im Unternehmen

3.1.3.4.2 Kompetenzfelder: Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit

Fähigkeiten/Fertigkeiten

- sicherheitsrelevante Themen für das Unternehmen bzw. bestimmte Mitarbeitergruppen erkennen, sie angemessen aufbereiten und glaubwürdig vermitteln können
- Workshops zu sicherheitsrelevanten Themen für Mitarbeiterinnen und Mitarbeiter unterschiedlicher Unternehmensbereiche vorbereiten, durchführen und evaluieren können
- Informationsbereiche im firmeneigenen Intranet aufbauen sowie aktualisieren und pflegen können
- mit unterschiedlichen Mitarbeiterinnen und Mitarbeitern des Unternehmens angemessen (Ansprache, Kommunikationsmedien, Verhalten) kommunizieren können, dabei regelmäßiges Feedback einholen
- informelle Gespräche führen können, dabei Vertrauensverhältnisse aufbauen und pflegen
- offene (ggf. auch anonyme) Kommunikationsmöglichkeiten einrichten und betreuen können, z. B. Sicherheitssprechstunden, Web-Forum im Unternehmens-Intranet o. Ä.
- sinnvoll Wege für die Verteilung von Sicherheitsinformationen (schwarzes Brett, Newsletter usw.) erkennen und nutzen können
- durchgängige und einheitliche Kommunikation (Stellenwert der Sicherheit) auf allen Unternehmensebenen sicherstellen können

Wissen

- didaktische Grundlagen und Modelle
- Motivation; Motivationstypen
- Lernprozesse (Gestaltung, Medien, Wege der Wissensvermittlung)
- Kommunikation und Kommunikationsmodelle
- Elemente und Regeln verbaler und nonverbaler Kommunikation
- typische Kommunikationsmuster und Umgang mit diesen
- typische Konflikte, deren Ursachen und Symptome

Werkzeuge/Methoden

- Präsentations- und Moderationstechniken
- Motivationsmethoden
- Visualisierungstechniken
- Methoden zur Benutzereinweisung
- Informations- und Wissensvermittlung

3.1.3.4.3 Beispiel: Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit

Um IT-Sicherheit konsequent und nachhaltig in einem Unternehmen zu etablieren, muss jeder Mitarbeiter seinen Beitrag zur Informationssicherheit kennen und leisten. Dazu wurden im konkreten Fall zunächst einmal Workshops für die unterschiedlichen Mitarbeitergruppen angeboten, in denen folgenden Themen behandelt wurden:

- Risiken und Bedrohungen im IT-Umfeld
- Grundwerte der IT-Sicherheit
- Vorstellung der unternehmensweiten Sicherheitsrichtlinie, bezogen auf die Mitarbeitergruppen
- Verantwortlichkeiten und Meldewege
- Wie kann der Mitarbeiter zur IT-Sicherheit beitragen?
- Wie werden sicherheitsrelevante Vorfälle erkannt?
- Wo bekommt der Mitarbeiter Informationen zur IT-Sicherheit?

Die Themenauswahl entsprach den Vorgaben des BSI-Grundschutzhandbuchs M 2.198 und wurde mittels Folienvortrag und Praxisbeispielen, durchgeführt an einem Testnetzwerk mit zwei Rechnern, präsentiert.

3.1.3.5 Unterstützen der Partner bei sicherheitstechnischen Maßnahmen

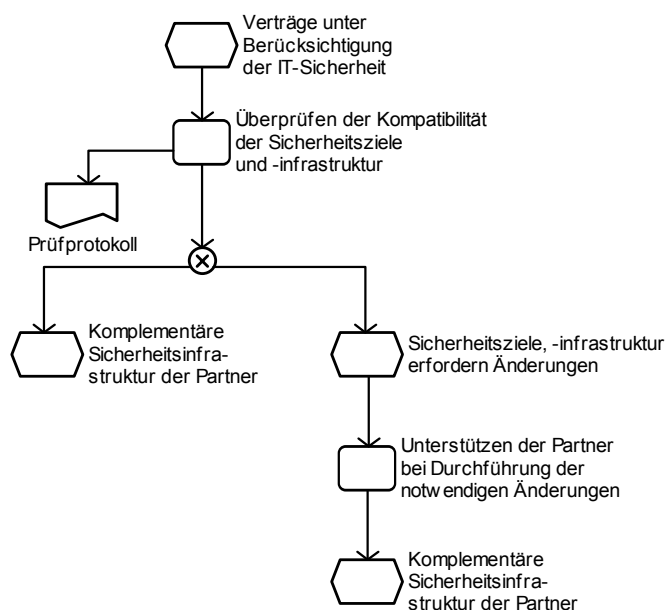


Abbildung 13: Unterstützen der Partner bei sicherheitstechnischen Maßnahmen.

3.1.3.5.1 Tätigkeiten: Unterstützen der Partner bei sicherheitstechnischen Maßnahmen

- Überprüfen der Kompatibilität der Sicherheitsziele und Sicherheitsinfrastruktur bei und mit Partnern.

Partner im Sinne dieses Teilprozesses sind alle Unternehmen und Stellen, mit denen Daten getauscht werden. Das können Auftragnehmer, Auftraggeber, Dienstleister (Outsourcing) oder auch selbstständige Partner sein. Besonders wichtig sind die Tätigkeiten in diesem und dem nächsten Teilprozess dann, wenn eine ständige Verbindung (z. B. per VPN) zwischen den Partner besteht. Die tatsächlich durchzuführenden Tätigkeiten des IT-Sicherheitskoordinators hängen dann von der konkreten Situation und seiner vereinbarten Funktion ab.

- Unterstützen der Partner bei der Durchführung der Änderungen zum Erreichen der notwendigen Sicherheitsstandards und -maßnahmen

3.1.3.5.2 Kompetenzfelder: Unterstützen der Partner bei sicherheitstechnischen Maßnahmen

Fähigkeiten/Fertigkeiten

- Sicherheitsziele verstehen und ihre angemessene Umsetzung in Sicherheitsinfrastrukturen beurteilen können
- Kompatibilität und Komplementarität von Sicherheitsinfrastrukturen und ihren Komponenten (Systeme, Netze usw.) beurteilen können
- Abhängigkeiten identifizieren und ihre Auswirkungen beurteilen können
- notwendige, sicherheitstechnische Änderungen vertreten und durchsetzen können

Wissen

- Sicherheitsstrategien, Ziele und Infrastrukturen
- Sicherheitsmaßnahmen
- IT-Systeme, Netze und Infrastrukturen
- Netzwerktechnik und -topologie

- Netzwerk- und Kommunikationsprotokolle, Dienste, Schnittstellen
- System- und Kommunikationsarchitekturen
- spezielle Techniken (z. B. Fernzugriff, VPN)

Werkzeuge/Methoden

- Analysetechniken
- Überwachungstechniken

3.1.3.5.3 Beispiel: Unterstützen der Partner bei sicherheitstechnischen Maßnahmen

Nachdem die Partner die Einführung eines VPNs unterstützen, muss das Netzwerk, das Zugriffe auf das Internet bisher in den Außenstellen z. T. über ISDN-Modems realisiert, umgestellt werden. Zugriffe dürfen nur noch über die Unternehmens-Firewall und den zentralen Antiviren-Server der Hauptstelle erfolgen. Die Anbindung der Außenstellen erfolgt über VPN-Router. Dadurch müssen die Sicherheitsziele und die Sicherheitsinfrastruktur der Außenstellen geändert werden.

3.1.3.6 Gegenseitiges Informieren der Partner über sicherheitsrelevante Änderungen

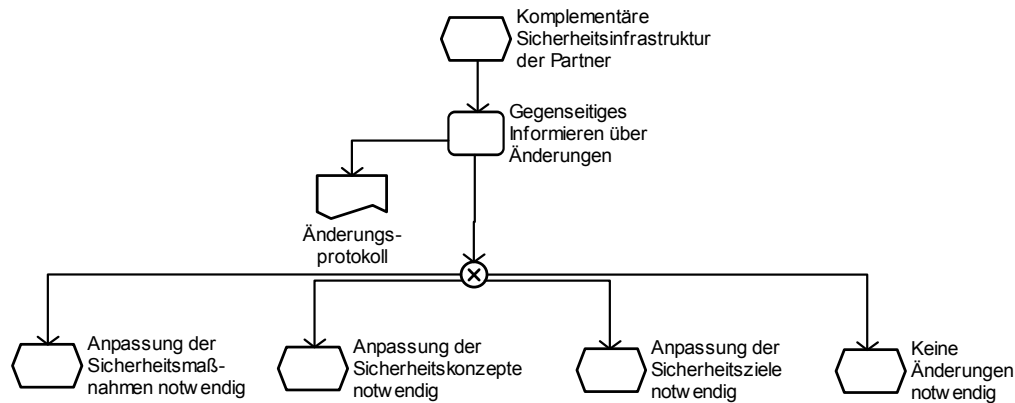


Abbildung 14: Gegenseitiges Informieren der Partner über sicherheitsrelevante Änderungen.

3.1.3.6.1 Tätigkeiten: Gegenseitiges Informieren der Partner über sicherheitsrelevante Änderungen

- gegenseitiges Informieren der Partner über sicherheitsrelevante Änderungen, um ggf. Änderungen auch kurzfristig vornehmen zu können (vgl. auch Teilprozess 3.1.3.5 Unterstützen der Partner bei sicherheitstechnischen Maßnahmen)

3.1.3.6.2 Kompetenzfelder: Gegenseitiges Informieren der Partner über sicherheitsrelevante Änderungen

Fähigkeiten/Fertigkeiten

- für die Partner relevante Änderungen erkennen und kommunizieren können
- von Partnern mitgeteilte Änderungen beurteilen können
- Bedeutung von Änderungen für die eigenen und Fremdsysteme abschätzen können
- Sitzungen/Besprechungen vorbereiten, leiten und protokollieren können

Wissen

- Sicherheitsinfrastrukturen (eigene, Partner)
- Einstufung sicherheitsrelevanter Änderungen und Vorkommnisse

Werkzeuge/Methoden

- Kommunikations- und Moderationstechniken
- Protokollführung

3.1.3.6.3 Beispiel: Gegenseitiges Informieren der Partner über sicherheitsrelevante Änderungen

Im konkreten Fall mussten durch die Anbindung der Außenstellen die Sicherheitsmaßnahmen, die Sicherheitskonzepte und die Sicherheitsziele organisatorisch als auch hardwaremäßig angepasst werden. Außerdem wurde vereinbart, einmal im Monat eine Sitzung aller Zuständigen abzuhalten, um auf dem gleichen Informationsstand zu bleiben.

3.1.3.7 Beraten bei der Anpassung und Konkretisierung der Sicherheitsziele

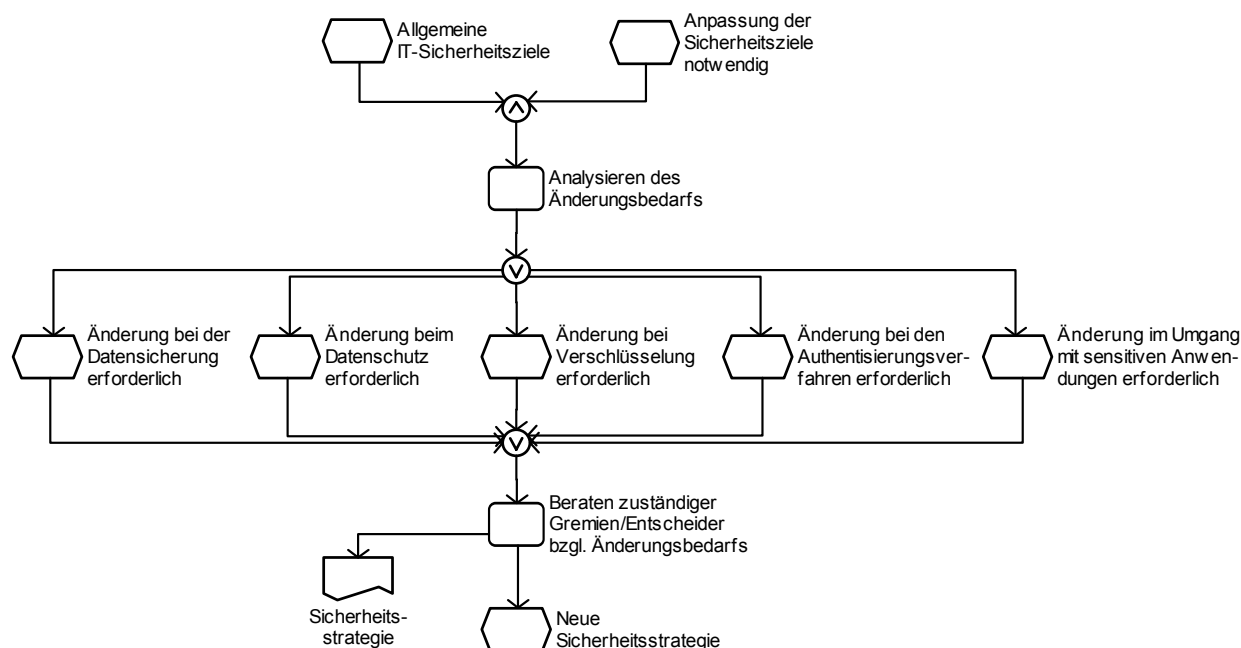


Abbildung 15: Beraten bei der Anpassung und Konkretisierung der Sicherheitsziele.

Wie bereits im Zusammenhang mit dem Referenzprozess (vgl. 3.1.1 Referenzprozess IT-Sicherheitskoordination) beschrieben, beruht der Prozess „Koordinieren der IT-Sicherheit“ und damit auch dieser und alle folgenden Teilprozesse auf zwei wesentlichen Annahmen:

1. Das Unternehmen, in dem der IT Security Coordinator tätig ist, hat bereits Sicherheitsziele festgelegt und einen Sicherheitsprozess – zumindest in Ansätzen – eingerichtet.
2. Die Verantwortung für die IT-Sicherheit liegt bei der Unternehmensleitung bzw. dem Management. Strategische Leitaussagen wurden bereits getroffen, konzeptionelle Vorgaben gemacht und organisatorische Rahmenbedingungen geschaffen.

Sollen oder müssen die Sicherheitsziele oder der Sicherheitsprozess geändert werden, wird der IT Security Coordinator aufgrund seiner fachlichen Kompetenz beratend hinzugezogen.

An dieser Stelle weicht der hier dargestellte Prozess von dem BSI-Grundschriftzhandbuch in der Reihenfolge ab: Im BSI-Grundschriftzhandbuch werden die Sicherheitsziele erst im Rahmen der Erstellung der IT-Sicherheitsleitlinie festgelegt und dokumentiert. Hier wird davon ausgegangen, dass entsprechende Ziele (Beispiele finden sich im BSI-Grundschriftzhandbuch M 2.192, Abschnitt 3: „Bestimmung der IT-Sicherheitsziele“), Verantwortlichkeiten (BSI-Grundschriftzhandbuch M 2.191: „Etablierung des IT-Sicherheitsprozesses“) und Organisationsstrukturen (BSI-Grundschriftzhandbuch M 2.193: „Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit“) bereits existieren. Der IT Security Coordinator übernimmt also die Rolle des IT-Sicherheitsbeauftragten.

Sind die genannten Voraussetzungen in einem Unternehmen noch nicht erfüllt, so kann der IT Security Coordinator selbstverständlich auch die Aufgabe übernehmen, diese Strukturen zu schaffen. Dabei muss er eng mit der Unternehmensleitung zusammenarbeiten. Die Teilprozesse „Beraten bei der Anpassung und Konkretisierung der Sicherheitsziele“ und „Entwerfen der Sicherheitsleitlinien“ müssen dann entsprechend angepasst werden (vgl. dazu BSI-Grundschriftzhandbuch M 2.191, M 2.192 und M 2.193).

3.1.3.7.1 Tätigkeiten: Beraten bei der Anpassung und Konkretisierung der Sicherheitsziele

- Analysieren des Änderungsbedarfs in Hinblick auf die notwendigen Änderungen bei den Sicherheitszielen in den Bereichen Datensicherung, Datenschutz, Verschlüsselung, Authentisierungsverfahren, sensitive Anwendungen usw.
- Beraten der zuständigen Gremien (auch des Betriebsrats) und Entscheider bezüglich des Änderungsbedarfs und der Sicherheitsstrategie

3.1.3.7.2 Kompetenzfelder: Beraten bei der Anpassung und Konkretisierung der Sicherheitsziele

Fähigkeiten/Fertigkeiten

- Sicherheitsziele im Hinblick auf ihre Angemessenheit für das Unternehmen, einzelne Bereiche und geplante Änderungen beurteilen können
- Bedeutung der IT für die Aufgabenerfüllung des Unternehmens beurteilen können
- Bedrohungspotenzial für das Unternehmen, die Bereiche und Systeme abschätzen können
- komplexe Zusammenhänge erfassen und - in Bezug auf die IT-Sicherheit - beurteilen können
- Bedeutung von Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Systemen beurteilen können
- Auswirkungen von IT-Sicherheitszwischenfällen einschätzen können, betroffene Systemkomponenten und -bereiche identifizieren können
- Vertraulichkeit der zu verarbeitenden Daten einschätzen können
- notwendiges Maß an IT-Sicherheit aufgrund der geplanten Änderung festlegen können
- IT-Sicherheitsmaßnahmen, die dem Sicherheitsniveau entsprechen, entwickeln können, speziell in den Bereichen Datensicherheit, Datenschutz, Verschlüsselung, Authentisierung und sensitive Anwendungen
- IT-Sicherheitsmaßnahmen in Hinblick auf Aufwände, Kosten und Nutzen einschätzen können
- Änderungen an Sicherheitszielen, -strategien und -niveau kommunizieren und die notwendigen Aufwände vertreten können
- Konsequenzen unterschiedlicher Maßnahmen (und ihrer Nichtdurchführung) deutlich machen können
- Alternativlösungen entwickeln können

Wissen

- IT-Sicherheitsziele, -strategien, -niveaus und ihre praktischen Konsequenzen
- IT-Sicherheitsmaßnahmen, ihre Aufwände, Kosten und Nutzen
- IT-Infrastruktur, IT-Anwendungen
- Datenschutz, Datensicherheit
- Funktionsweise von Scannern/Sniffern, Würmern, Viren, Trojanern und Hybriden
- Funktionsweise gängiger Hacker-Software
- Funktionsweise und Risiken von Firewalls und Proxys
- einschlägige gesetzliche Grundlagen

Werkzeuge/Methoden

- BSI-Grundschutzhandbuch

3.1.3.7.3 *Beispiel: Beraten bei der Anpassung und Konkretisierung der Sicherheitsziele*

Durch die grundlegenden Änderungen in der Netzwerkstruktur der Außenstellen war es notwendig, die Sicherheitsziele zu überprüfen. Daher wurde eine Analyse unter Einbezug der entsprechenden Gremien durchgeführt. Dabei lag die Gesamtverantwortung bei der Unternehmensleitung, der IT-Sicherheitskoordinator leitete und koordinierte aber die Gruppe, die das neue Konzept erarbeitete. Die Sicherheitsziele wurden anhand der Klassifizierung der IT-Anwendungen bestimmt. Gemäß den im BSI-Grundschutzhandbuch vorgegebenen Kriterien wurde den Anwendungen das jeweils notwendige Sicherheitsniveau (von niedrig bis maximal) zugeordnet. Aufwand und Nutzen der entsprechenden erforderlichen Maßnahmen wurde beurteilt.

Insbesondere im Bereich der Datensicherung musste ein umfassend neues Konzept erarbeitet werden. Dieses umfasste die Definition, welche Daten zukünftig zentral gehalten und gesichert werden und welche Daten lokal in den Außenstellen gehalten und gesichert werden.

3.1.3.8 Entwerfen der Sicherheitsleitlinien

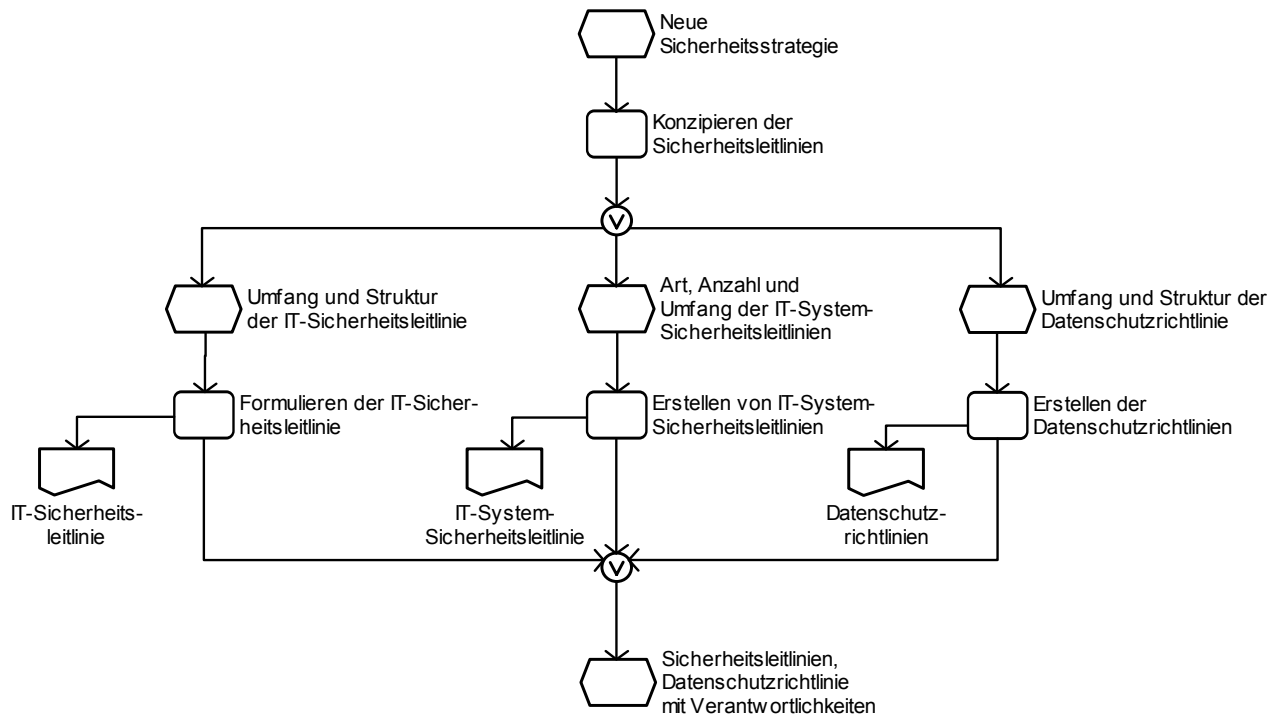


Abbildung 16: Entwerfen der Sicherheitsleitlinien.

Dieser Teilprozess sollte gemäß BSI-Grundschutzhandbuch M 2.192 durchgeführt werden.

3.1.3.8.1 Tätigkeiten: Entwerfen der Sicherheitsleitlinien

- Konzipieren der Sicherheitsleitlinien gemäß der Sicherheitsstrategie
- Formulieren der IT-Sicherheitsleitlinie
- Erstellen der IT-System-Sicherheitsleitlinien
- Erstellen der Datenschutzrichtlinien

3.1.3.8.2 Kompetenzfelder: Entwerfen der Sicherheitsleitlinien

Fähigkeiten/Fertigkeiten

- Sicherheitsstrategie verstehen können
- angemessene Sicherheitsleitlinien konzipieren können
- Umfang und Struktur der Sicherheitsleitlinie festlegen können
- notwendige IT-System-Sicherheitsleitlinien ableiten und strukturieren können
- notwendige Datenschutzrichtlinie ableiten und strukturieren können
- eindeutige Verantwortlichkeiten festlegen können
- Leitlinien angemessen formulieren können
- Leitlinien bekannt machen und kommunizieren können
- Funktionalität von Systemen, ihrer externen Schnittstellen und ihrer Anforderungen an die Einsatzumgebung identifizieren und beschreiben können
- Bedrohungen, gegen die das System geschützt werden soll, identifizieren und beschreiben können

- Aktionen, die Personen oder technische Prozesse auf Daten oder Programmen ausführen dürfen, identifizieren und beschreiben können
- die Schutzbedürftigkeit der Systemobjekte identifizieren und beschreiben können
- Restrisiken, die der Betreiber des Systems akzeptieren kann, beschreiben können
- alle IT-Sicherheitsmaßnahmen, die vom System einzuhalten sind, auf allgemeiner Ebene beschreiben können
- Schwachstellen des Systems erkennen und beschreiben können

Wissen

- Informationsklassifizierung und -kontrolle
- Informationseigentümer und -treuhänder
- Nutzerkonzepte
- Systemzugangskontrollen
- Sicherheit von Informationssystemen während ihres Lebenszyklus'
- Sicherheitsrisikoanalysen
- Sicherheitsmanagement
- IT-Infrastruktur, IT-Anwendungen, Systemschnittstellen
- Datenübertragungstechniken und -systeme
- Netzwerk- und Kommunikationsprotokolle
- Sicherheitsdokumente und Richtlinien für ihre Erstellung

3.1.3.8.3 Beispiel: Entwerfen der Sicherheitsleitlinien

Zur Erstellung der IT-Sicherheitsrichtlinie wurde eine Entwicklungsgruppe einberufen. Die Mitglieder der Gruppe umfassten Administratoren mit Vorkenntnis im Bereich IT-Sicherheit, ein Mitglied der IT-Leitung mit der Aufgabe, direkt an das Management zu berichten, als auch IT-Anwender. Die Gesamtverantwortung oblag der Unternehmensleitung.

Die verabschiedete Sicherheitsrichtlinie umfasste die Kernpunkte:

- Stellenwert der IT-Sicherheit im Unternehmen
- Sicherheitsziele, Sicherheitsstrategie
- Unterstützung durch die Unternehmensleitung
- Beschreibung für die Umsetzung (Organisationsstruktur, vgl. BSI-Grundschutzhandbuch M 2.193)

Für die Bereiche Firewall, Virenschutz, E-Mail und Internetzugriff wurden zusätzliche IT-System-Sicherheitsleitlinien erstellt.

Die IT-Sicherheitsrichtlinie wurde schriftlich fixiert und im Unternehmen bekannt gegeben.

3.1.3.9 Durchführen von IT-Strukturanalysen

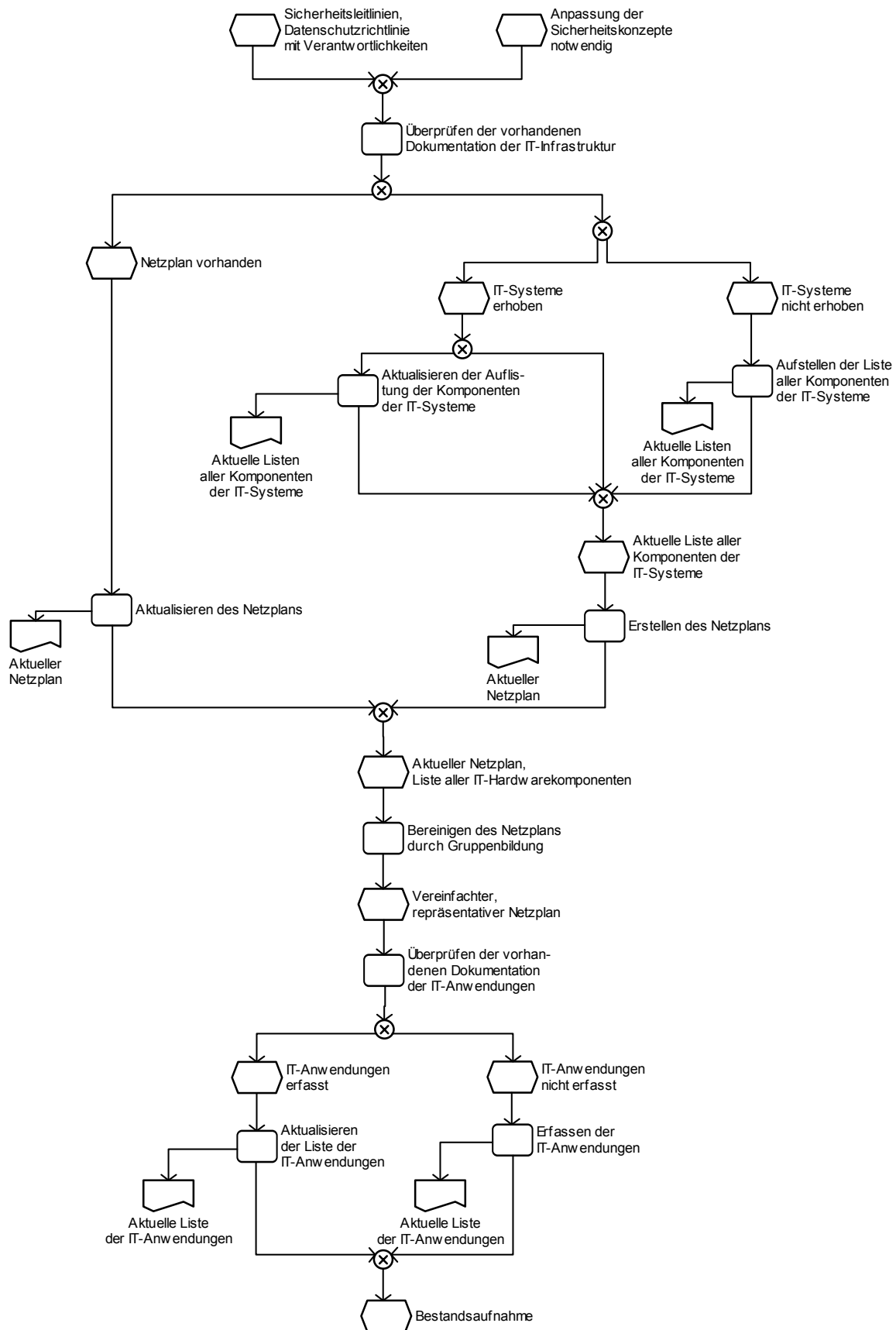


Abbildung 17: Durchführen von IT-Strukturanalysen.

3.1.3.9.1 Tätigkeiten: Durchführen von IT-Strukturanalysen

- Überprüfen der vorhandenen Dokumentation der IT-Infrastruktur
- Aufstellen bzw. Aktualisieren der Liste aller IT-Systeme und ihrer Komponenten
- Aufstellen bzw. Aktualisieren des Netzplans
- Bereinigen des Netzplans durch Gruppenbildung
- Überprüfen der vorhandenen Dokumentation der IT-Anwendungen
- Erfassen bzw. Aktualisieren aller IT-Anwendungen zur vollständigen Bestandsaufnahme

3.1.3.9.2 Kompetenzfelder: Durchführen von IT-Strukturanalysen

Fähigkeiten/Fertigkeiten

- technische Dokumentationen verstehen und auf Korrektheit und Aktualität prüfen können
- IT-Systeme und ihre Komponenten vollständig und korrekt erfassen und darstellen können
- Netzpläne lesen, prüfen, erstellen und aktualisieren können
- sinnvolle Gruppen von IT-Systemen bilden können
- Komplexität reduzieren können
- Strukturen erfassen und darstellen können
- IT-Anwendungen (einschließlich Versionen) vollständig und korrekt erfassen und darstellen können
- sorgfältig arbeiten können (penibel, frustrationstolerant, hartnäckig)
- mit Anwendern und Zuständigen unterschiedlicher Hierarchieebenen angemessen kommunizieren können
- im Team arbeiten können, dabei klare Verantwortlichkeiten schaffen und wahrnehmen können
- Vertrauen schaffen, ggf. auch mit einer gewissen Autorität auftreten können

Wissen

- technische Dokumentation, Netzpläne
- IT-Systeme, Infrastrukturen, Komponenten, Anwendungen
- Netzwerktechnik und -topologie
- Datenübertragungssysteme und -techniken, Hardware-Schnittstellen
- System- und Kommunikationsarchitekturen
- Netzwerk- und Kommunikationsprotokolle, Schnittstellen
- Funktionsweise von Scannern/Sniffern, Würmern, Viren, Trojanern und Hybriden
- Funktionsweise gängiger Hacker-Software
- Modelle menschlicher Kommunikation

Werkzeuge/Methoden

- Tools zur Erstellung von Netzplänen
- Tools zur IT-System-, Anwendungs- und Versionsverwaltung
- Dokumentationssysteme

3.1.3.9.3 Beispiel: Durchführen von IT-Strukturanalysen

Die IT-Strukturanalyse bedarf in diesem Fall vor allem der Aktualisierung des Netzplans:

Der Netzwerkplan wurde graphisch auf alle aktuellen, aber auch alle geplanten IT-Systeme angepasst.

Client- und Server-Computer, aktive Netzkomponenten, Netzverbindungen zwischen diesen Systemen, Netzwerkprotokolle, Netzwerkadressen als auch Verbindungen nach außen wurden dargestellt.

Zu jedem der dargestellten Objekte gehörten weiterhin Informationen wie eine eindeutige Bezeichnung, Typ und Funktion, die Plattform, der Standort, der zuständige Administrator sowie die Art der Netzanbindung und die Netzadresse.

Die Netzverbindungen zwischen den Systemen und für die Verbindungen nach außen wurden wie folgt beschrieben: die Art der Verkabelung, die maximale Datenübertragungsrate, verwendete Netzprotokolle, Details zum externen Netz.

Der nächste Schritt bestand darin, gleichartige Komponenten zu einer Gruppe zusammenzufassen. Die Komponenten konnten einer Gruppe zugeordnet werden, wenn diese alle vom gleichen Typ waren, gleich oder nahezu gleich konfiguriert sind, gleich oder nahezu gleich in das Netz eingebunden sind, den gleichen administrativen und infrastrukturellen Rahmenbedingungen unterliegen und die gleichen Anwendungen bedienen.

Zur Reduzierung des Aufwands wurden die jeweils wichtigsten auf den betrachteten IT-Systemen laufenden oder geplanten IT-Anwendungen erfasst. Anschließend wurden die Anwendungen jeweils denjenigen IT-Systemen zugeordnet, die für deren Ausführung benötigt werden. Dies waren die IT-Systeme, auf denen die IT-Anwendungen verarbeitet wurden, oder auch diejenigen, die Daten dieser Anwendung halten.

Das Ergebnis stellte eine Übersicht in tabellarischer Form dar, welche wichtigen IT-Anwendungen auf welchen IT-Systemen bearbeitet oder von welchen IT-Systemen genutzt oder übertragen wurden.

3.1.3.10 Feststellen des Schutzbedarfs der Fachabteilungen

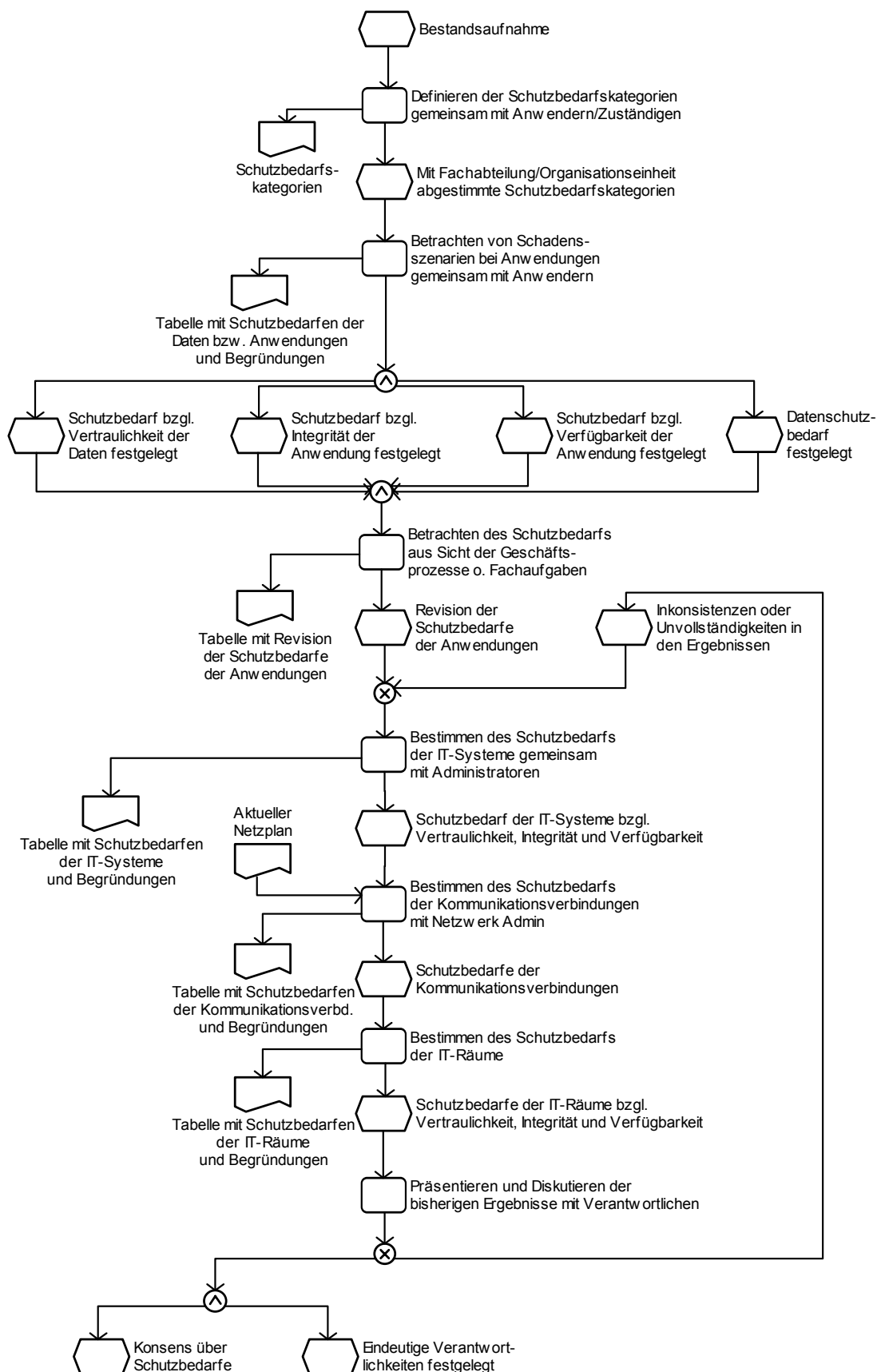


Abbildung 18: Feststellen des Schutzbedarfs der Fachabteilungen.

Dieser Teilprozess sollte gemäß BSI-Grundschutzhandbuch Abschnitt 2.2 „Schutzbedarfsfeststellung“ durchgeführt werden.

3.1.3.10.1 Tätigkeiten: Feststellen des Schutzbedarfs der Fachabteilungen

- Definieren der Schutzbedarfskategorien der Anwendungen gemeinsam mit den Anwendern bzw. Zuständigen
- Betrachten möglicher Schadensszenarien gemeinsam mit den Anwendern bzw. Zuständigen, um den notwendigen und sinnvollen Schutzbedarf der Anwendungen bezüglich Vertraulichkeit der Daten, Integrität und Verfügbarkeit der Anwendungen und des Datenschutzes festzulegen
- Betrachten des Schutzbedarfs aus Sicht der Geschäftsprozesse oder Fachaufgaben und ggf. Revision des für die Anwendungen festgelegten Schutzbedarfs
- Bestimmen des Schutzbedarfs der IT-Systeme und der Netzwerke gemeinsam mit den zuständigen Administratoren
- Bestimmen des Schutzbedarfs der IT-Räume
- Präsentieren und Diskutieren der bisherigen Ergebnisse mit Entscheidern in Hinblick auf Korrektheit, Konsens über Schutzbedarf und das Festlegen von Verantwortlichkeiten

3.1.3.10.2 Kompetenzfelder: Feststellen des Schutzbedarfs der Fachabteilungen

Fähigkeiten/Fertigkeiten

- Schadensszenarien auf ihre Angemessenheit prüfen, ggf. anpassen und ergänzen können
- Grenzen der Schutzbedarfskategorien festlegen können
- sich in die Anwendersicht hineinversetzen können
- Schäden abschätzen können (materiellen und immateriellen)
- mit Anwendern, Zuständigen, Administratoren angemessen kommunizieren, sie zielgerichtet befragen können
- IT-System und Komponenten bezüglich ihrer Schutzbedarfe beurteilen können
- IT-Anwendungen bezüglich ihrer Schutzbedarfe beurteilen können
- Kommunikationsverbindungen bezüglich ihrer Schutzbedarfe beurteilen können
- IT-Räume bezüglich ihrer Schutzbedarfe beurteilen können
- Schutzbedarfe gemeinsam mit den Zuständigen festlegen können
- Schutzbedarfe aus Sicht von Geschäftsprozessen oder Fachaufgaben beurteilen können
- Schutzbedarfe darstellen, kommunizieren und diskutieren können
- Schutzbedarfe einschließlich ihrer Begründung dokumentieren können
- Konsequenzen der Festlegung von Schutzbedarfen für IT-System, Anwendungen, Kommunikationsverbindungen, Räume ableiten, darstellen und in Nutzen, Kosten und Aufwänden (kurz-, mittel- und langfristig) beurteilen und begründen können
- Abhängigkeiten und Zusammenhänge feststellen und dokumentieren sowie angemessene Konsequenzen ableiten können
- Kumulations- und Verteilungseffekte beurteilen und berücksichtigen können

Wissen

- Schutzbedarfskategorien
- Schadensszenarien

- sicherheitsrelevante Gesetze, Vorschriften, Verträge (vgl. auch BSI-Grundschutzhandbuch, Abschnitt 2.2 „Schutzbedarfsfeststellung“, Abschnitt „Schadensszenario ,Verstoß gegen Gesetze/Vorschriften/Verträge“)
- Datenschutz, informationelles Selbstbestimmungsrecht
- Fachaufgaben, Geschäftsprozesse (bezogen auf das jeweilige Unternehmen)
- spezielle IT-Systeme, Anwendungen und ihre Auswirkungen
- Qualitätsmanagement und -sicherung
- Kosten und Nutzen von IT-Systemen, Infrastrukturen, Komponenten, Anwendungen
- kryptographische Sicherheitsmaßnahmen

Werkzeuge/Methoden

- BSI-Grundschutzhandbuch

3.1.3.10.3 Beispiel: Feststellen des Schutzbedarfs der Fachabteilungen

Die Schutzbedarfsfeststellung der erfassten IT-Struktur wurde für die Fachabteilungen in vier Schritten durchgeführt:

Definition der Schutzbedarfskategorien

Um zum späteren Zeitpunkt einen Schutzbedarf für die IT-Anwendungen und daraus abgeleitet für die IT-Systeme zuweisen zu können, wurden zunächst Schutzbedarfskategorien entwickelt.

Als Vorlage für die Schutzbedarfskategorien wurden die Tabellen des BSI-Grundschutzhandbuchs 2.2 und die Vorlagen der CD verwendet. Die dort beschriebenen Kategorien von „niedrig“ bis „sehr hoch“ wurden zusammen mit den Zuständigen der Fachabteilungen diskutiert, angepasst und definiert.

Bestimmung des Schutzbedarfs der IT-Anwendungen

Im nächsten Schritt wurden die Schadensszenarien erarbeitet, die aus der Sicht der Zuständigen tatsächlich eintreten könnten. Für die einzelnen Kategorien wurden Szenarien für die IT-Anwendungen betrachtet, die sich auf den Verlust der Vertraulichkeit, der Integrität und der Verfügbarkeit bezogen.

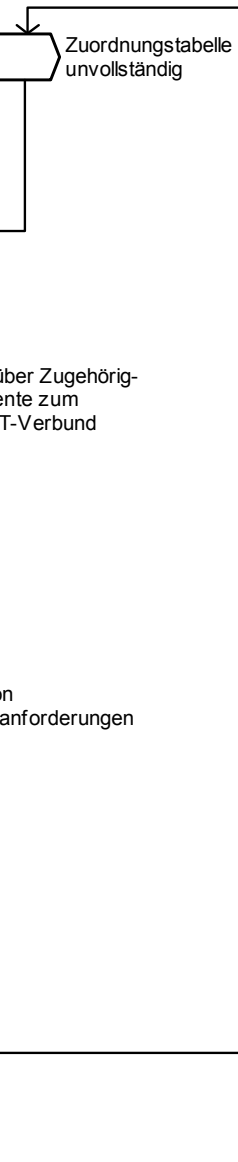
Die Ergebnisse wurden in einer Tabelle dokumentiert, die die einzelnen IT-Anwendungen und deren Schutzbedarf umfasste. Mit einbezogen wurde ebenfalls die Bedeutung der Anwendung für die Geschäftsprozesse.

Ableitung des Schutzbedarfs der einzelnen IT-Systeme

Anhand der Tabelle wurde der Schutzbedarf der IT-Systeme festgestellt. Dabei galt, dass der Schaden pro IT-System mit der schwerwiegendsten Auswirkung als Maßstab genommen wurde. Aber auch Abhängigkeiten zwischen den Systemen und das Auftreten mehrerer kleinerer Zwischenfälle auf verschiedenen Systemen und deren Auswirkung in der Summe wurden betrachtet.

Nach den IT-Systemen wurden die Kommunikationsverbindungen betrachtet und die Verbindungen zu den Außenstellen als kritisch eingestuft.

Es wurde eine Übersicht über die Räume erstellt, in denen IT-Systeme aufgestellt oder die für den IT-Betrieb genutzt werden. Der Schutzbedarf wurde für den zentralen Server-Raum als auch die Kommunikations- bzw. Server-Räume in den Außenstellen definiert.



g nach IT-Grund-

- IT-Verbund
elementen entspre-
rüh- bzw. Entwick-

3.1.3.11.2 Kompetenzfelder: Aufstellen des Grundschutzmodells

Fähigkeiten/Fertigkeiten

- Kriterien für Zuordnungen aufstellen und sinnvolle Zuordnungen vornehmen können
- Komplexität reduzieren können, sinnvolle Vereinfachungen vornehmen können, strukturieren können
- Strukturen und Systematiken verstehen und anwenden können
- Konzepte verstehen und interpretieren können
- Netz sinnvoll in Teilnetze aufteilen können
- modellieren können
- Vollständigkeit prüfen können
- sorgfältig arbeiten können (penibel, frustrationstolerant, hartnäckig)

Wissen

- Schichten des IT-Grundschutzmodells
- Bausteine des IT-Grundschutzhandbuchs
- übergeordnete Aspekte der IT-Sicherheit
- Sicherheit der Infrastruktur
- Sicherheit der IT-Systeme
- Sicherheit im Netz
- Sicherheit in Anwendungen
- Datenschutz, Datenschutzanforderungen und -maßnahmen

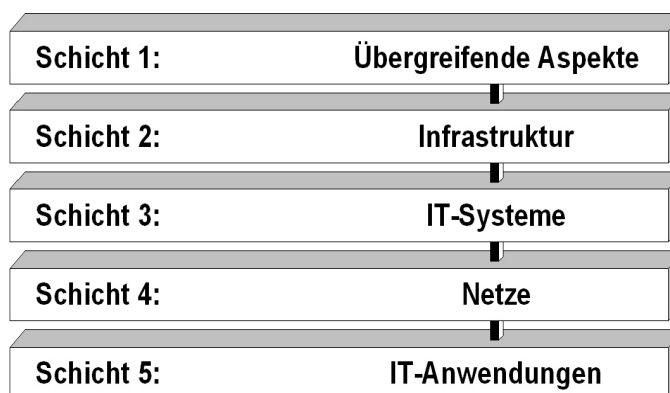
Werkzeuge/Methoden

- BSI-Grundschutzhandbuch

3.1.3.11.3 Beispiel: Aufstellen des Grundschutzmodells

Nachdem die notwendigen Informationen aus der IT-Strukturanalyse und der Schutzbedarfsfeststellung vorlagen, bestand die nächste zentrale Aufgabe darin, den betrachteten IT-Verbund mithilfe der vorhandenen Bausteine des IT-Grundschutzhandbuchs nachzubilden.

Dieses stellte für den geplanten IT-Verbund ein Entwicklungskonzept dar.



- Schicht 1 umfasst die übergreifenden Aspekte: IT-Sicherheitsmanagement, Organisation, Personal, Notfallvorsorge-Konzept, Datensicherungskonzept, Computer-

Virenschutzkonzept, Kryptokonzept, Behandlung von Sicherheitsvorfällen, Hard- und Software-Management und Standardsoftware.

- Schicht 2 umfasst die Sicherheit der Infrastruktur: Gebäude, Verkabelung, Büroraum, Server-Raum, Datenträgerarchiv, Raum für technische Infrastruktur, Schutzschrank, häuslichen Arbeitsplatz und das Rechenzentrum.
- Schicht 3 umfasst die Sicherheit der IT-Systeme: Unix-Systeme, tragbare PCs, PCs mit wechselnden Benutzern, PC unter Windows NT, Windows 2000 Client, Internet-PC, servergestütztes Netz, Unix-Server, Windows NT Netz und Windows 2000.
- Schicht 4 umfasst die Sicherheit im Netz: heterogene Netze, Netz- und Systemmanagement, Firewall und Remote Access.
- Schicht 5 umfasst die Sicherheit in Anwendungen: Datenträgeraustausch, E-Mail, WWW-Server und die Datenbanken.

Als Beispiel sollen hier die Bausteine des IT-Grundschutzhandbuchs zum Firewall auf der Schicht 4 dienen. Das Grundschutzhandbuch schlägt dazu folgende Maßnahmenbündel bezüglich Organisation, Hardware/Software und Kommunikation vor:

Organisation:

- M 2.70 Entwicklung eines Firewall-Konzeptes
- M 2.71 Festlegung einer Sicherheitspolitik für eine Firewall
- M 2.72 Anforderungen an eine Firewall
- M 2.73 Auswahl eines geeigneten Firewall-Typs
- M 2.74 Geeignete Auswahl eines Paketfilters (bei Beschaffungsbedarf)
- M 2.75 Geeignete Auswahl eines Application Gateway (bei Beschaffungsbedarf)
- M 2.76 Auswahl und Implementation geeigneter Filterregeln
- M 2.77 Sichere Anordnung weiterer Komponenten
- M 2.78 Sicherer Betrieb einer Firewall

Hardware/Software:

- M 4.47 Protokollierung der Firewall-Aktivitäten
- M 4.93 Regelmäßige Integritätsprüfung
- M 4.100 Firewalls und aktive Inhalte
- M 4.101 Firewalls und Verschlüsselung

Kommunikation:

- M 5.39 Sicherer Einsatz der Protokolle und Dienste
- M 5.45 Sicherheit von WWW-Browsern (bei Clients)
- M 5.46 Einsatz von Stand-alone-Systemen zur Nutzung des Internets
- M 5.59 Schutz vor DNS-Spoofing
- M 5.70 Adressumsetzung – NAT (Network Address Translation)
- M 5.71 Intrusion Detection und Intrusion Response Systeme

Um die Bedeutung der Bausteine zu verdeutlichen, soll nachfolgend die konkrete Umsetzung der Maßnahme M 5.59 „Schutz vor DNS-Spoofing“ dargestellt werden:

Bei der Firewall in der Hauptstelle handelt es sich um eine so genannte Unternehmens-Firewall, die aus drei Teilen besteht:

1. dem so genannten Firewalled Gateway, also dem Rechner, der mit mehreren Netzwerkkarten ausgestattet ist und das unsichere Netz, im konkreten Fall das Internet, vom gesicherten Netz trennt
2. dem Management Server, der die Log-Einträge des Firewalled Gateways übernimmt, das Regelwerk speichert und dieses bei der Installation auf das Firewalled Gateway überträgt
3. dem graphischen Interface, das auf jedem Windows-Rechner installiert werden kann und dem Administrator die Möglichkeit bietet, das Regelwerk für das Firewalled Gateway graphisch zu erstellen, auf dem Management Server zu speichern bzw. über diesen auf

dem Gateway zu installieren; über die GUI können auch die Log-Auswertungen und Statusabfragen gefahren werden

Für die Kommunikation der drei Systeme untereinander wurde festgelegt, dass in der Software der Firewall-Systeme für die Kommunikation untereinander keine Host-Namen verwendet werden, sondern die IP-Adressen eingetragen werden. Dadurch benötigt weder das Management-System noch das Firewalled Gateway einen Eintrag der Host-Namen in die `/etc/hosts` oder eine Verbindung zu einem DNS-Server.

3.1.3.12 Vergleichen von Ist- und Soll-Zustand in den Fachabteilungen

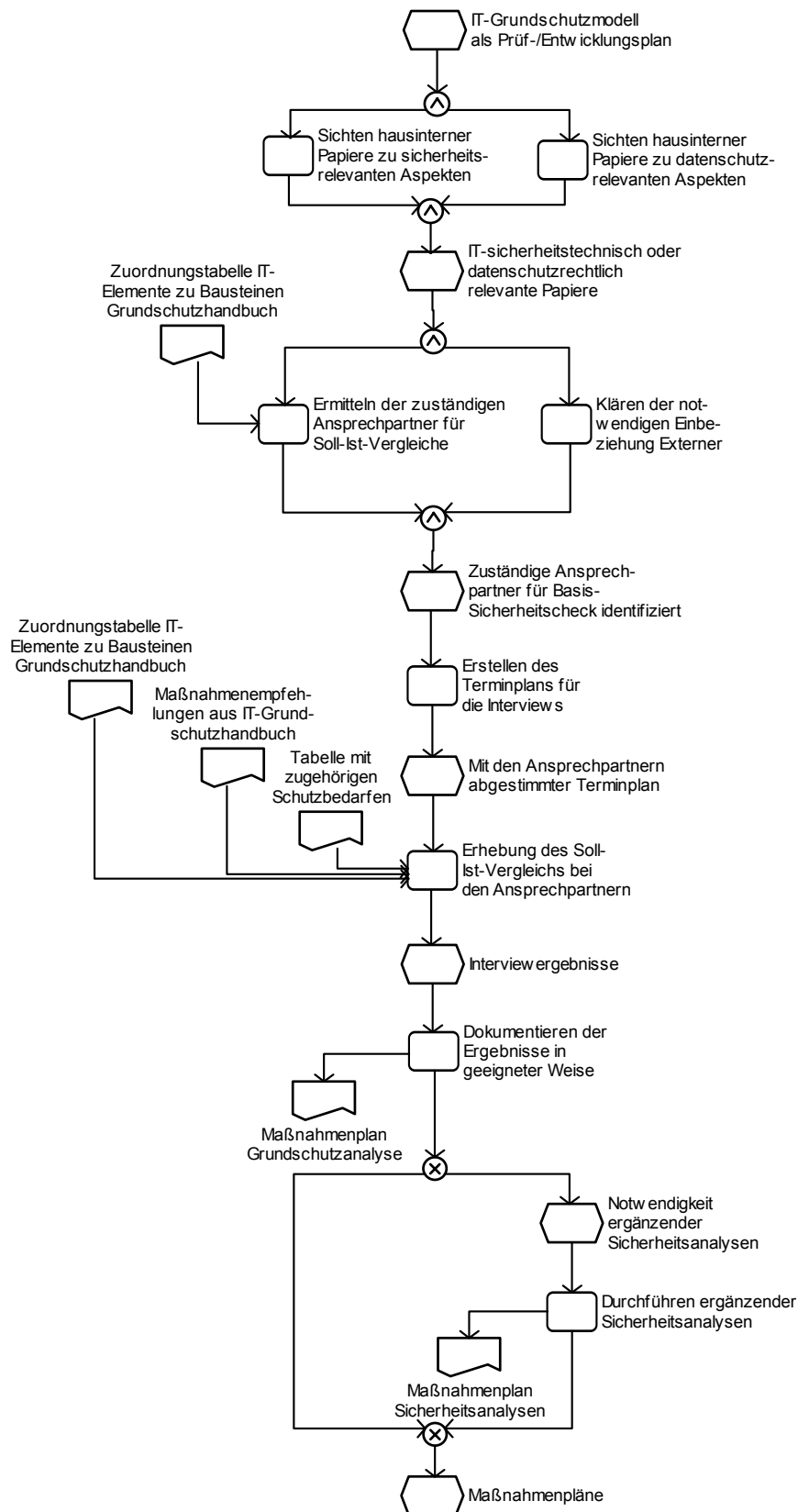


Abbildung 20: Vergleichen von Ist- und Soll-Zustand in den Fachabteilungen.

Zu diesem Teilprozess kann Abschnitt 2.4 „Basis-Sicherheitscheck“ des BSI-Grundschriftshandbuchs ergänzend verwendet werden.

3.1.3.12.1 Tätigkeiten: Vergleichen von Ist- und Soll-Zustand in den Fachabteilungen

- Sichten hausinterner Papiere zu sicherheitsrelevanten Aspekten
- Sichten hausinterner Papiere zu datenschutzrelevanten Aspekten
- Ermitteln hausinterner Ansprechpartner für Soll-Ist-Vergleiche im Rahmen des Sicherheitschecks
- Klären der notwendigen Einbeziehung Externer, Partner, Auftragnehmer wie Experten
- Erstellen des Terminplans für die Interviews mit den Ansprechpartnern für die Soll-Ist-Vergleiche
- Erheben des Soll-Ist-Vergleichs bei den Ansprechpartnern in Interviews oder Gruppengesprächen
- Dokumentieren der Ergebnisse in angemessener Weise in einem Maßnahmenplan
- falls notwendig: Durchführen ergänzender Sicherheitsanalysen gemäß Kap 2.5 des BSI-Grundschriftshandbuchs einschließlich des Aufstellens des entsprechenden Maßnahmenplans

3.1.3.12.2 Kompetenzfelder: Vergleichen von Ist- und Soll-Zustand in den Fachabteilungen

Fähigkeiten/Fertigkeiten

- IT-sicherheitsrelevante und datenschutzrelevante Schriftstücke (z. B. Organisationsverfügungen, Arbeitshinweise, Sicherheitsanweisungen, Manuals) identifizieren, verstehen und in ihrer Relevanz und ihrem Realitätsbezug beurteilen können, Verantwortliche für den Inhalt der Dokumente identifizieren können
- die für Ist-Soll-Vergleiche notwendigen Ansprechpartner identifizieren können
- Organigramm und ähnliche Informationsquellen zur Ermittlung von Zuständigen verwenden können
- geeignete Ansprechpartner festlegen können
- Termine festlegen, koordinieren und nachführen können
- Interviews zur Ermittlung von Ist-Soll-Vergleichen vorbereiten, durchführen, nachbereiten und auswerten können
- Checklisten erstellen können
- Gruppengespräche zur Ermittlung von Ist-Soll-Vergleichen vorbereiten, durchführen, nachbereiten und auswerten können
- Stichproben zur Verifizierung von Interviewergebnissen festlegen, durchführen und auswerten können
- problematische Gesprächssituationen und Konflikte moderieren und konstruktiv auflösen können
- Maßnahmenpläne aufstellen, kommunizieren und erläutern können
- Kosten und Aufwände für Maßnahmen schätzen können
- ergänzende Sicherheitsanalysen für sicherheitskritische Bereiche (ggf. gemeinsam mit entsprechenden Experten) durchführen können, dabei eigene Fähigkeiten und Grenzen realistisch einschätzen können
- Differenz-Sicherheitsanalyse durchführen können
- Risikoanalyse durchführen und statistische Annahmen und Daten bewerten können
- Penetrationstest durchführen können

Wissen

- Standard-Sicherheitsmaßnahmen, Hochschutz-Sicherheitsmaßnahmen
- Differenz-Sicherheitsanalyse, Risikoanalyse, Penetrationstest
- Grundkenntnisse Statistik
- typische Kommunikationsmuster und Umgang mit diesen
- typische Konflikte, deren Ursachen und Symptome

Werkzeuge/Methoden

- Interview-Techniken
- Kommunikations- und Moderationstechniken
- BSI-Grundschutzhandbuch
- IT-Grundschutz-Tool (BSI)

3.1.3.12.3 Beispiel: Vergleichen von Ist- und Soll-Zustand in den Fachabteilungen

Die Modellierung nach IT-Grundschutz wurde nun als Prüfplan benutzt, um anhand eines Soll-Ist-Vergleichs herauszufinden, welche Standard-Sicherheitsmaßnahmen ausreichend oder nur unzureichend umgesetzt sind.

Nach der Auswertung der hausinternen Papiere wurden unter Einbeziehung der Personalabteilung für den Bereich „Übergeordnete Aspekte, Personal“, externer Elektroinstallationsfirmen für den Bereich „Infrastruktur, Verkabelung“ sowie der zuständigen Administratoren für den Bereich „IT-Systeme, Netze und Anwendungen“ Termine abgestimmt und der Soll-Ist-Vergleich durchgeführt.

Anhand von Checklisten wurde festgestellt, welche Maßnahmen bereits komplett, teilweise oder gar nicht durchgeführt wurden.

Für die Dokumentation der Ergebnisse des Basis-Sicherheitschecks wurden die Formulare des BSI-Grundschutzhandbuchs verwendet.

3.1.3.13 Spezifizieren des Maßnahmenplans

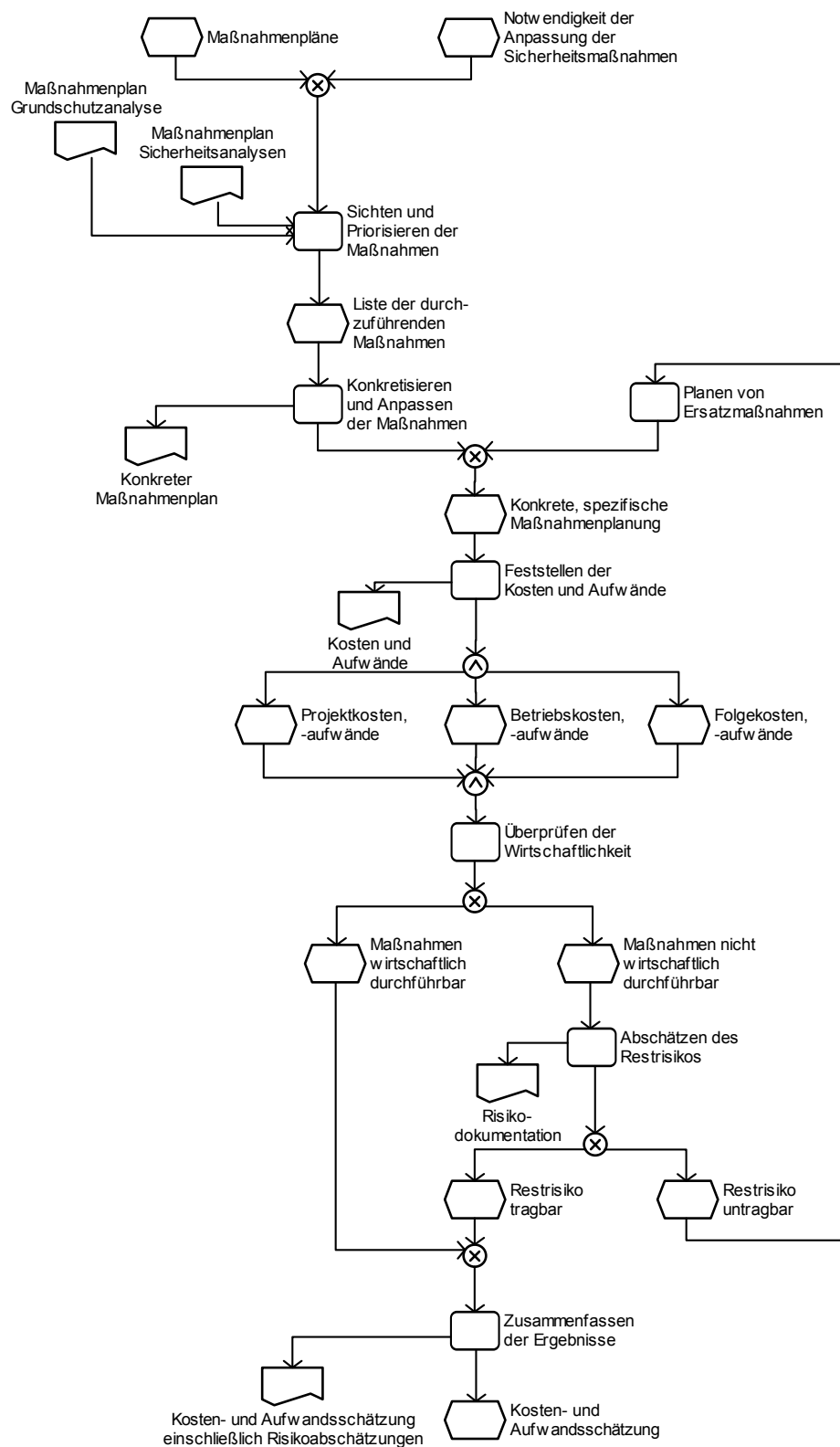


Abbildung 21: Spezifizieren des Maßnahmenplans.

3.1.3.13.1 Tätigkeiten: Spezifizieren des Maßnahmenplans

- Sichten und Priorisieren der Maßnahmen aus dem Maßnahmenplan in Hinblick auf durchzuführende Maßnahmen
- Konkretisieren und Anpassen der Maßnahmen bis hin zu einem konkreten Maßnahmenplan mit Prioritäten
- Feststellen der Kosten und Aufwände für die Einführung der sicherheitsrelevanten Maßnahmen (Projektkosten und -aufwände), für den Betrieb, die dauerhafte Durchführung der Maßnahme und für die Folgekosten der geplanten Maßnahmen
- Überprüfen der Wirtschaftlichkeit der Maßnahme; falls die Maßnahme wirtschaftlich nicht durchführbar ist: Abschätzen und Bewerten des Restrisikos
- Zusammenfassen der Ergebnisse zu Kosten-, Aufwands- und Risikoschätzungen

3.1.3.13.2 Kompetenzfelder: Spezifizieren des Maßnahmenplans

Fähigkeiten/Fertigkeiten

- Maßnahmenpläne auswerten können
- geplante Maßnahmen auf Zusammenhänge, Abhängigkeiten, Ersetzungsmöglichkeiten prüfen können
- geplante Maßnahmen konkretisieren und anpassen können
- zielgerichtetes Handeln beschreiben können
- Investitions- und laufende Kosten sowie Aufwände für Maßnahmen bestimmen können
- Restrisiken bestimmen und dokumentieren können
- begleitende Maßnahmen konzipieren und begründen können
- Management Summarys erstellen können

Wissen

- Sicherheitsmaßnahmen
- Prozessplanung, Prozesse und Organisationsstrukturen
- gängige Notfallvorsorgekonzepte und -tools
- Marktkenntnisse

3.1.3.13.3 Beispiel: Spezifizieren des Maßnahmenplans

Das Spezifizieren des Maßnahmenplans wurde in folgenden Schritten durchgeführt:

1. Sichten der Untersuchungsergebnisse: Zuerst wurden die fehlenden oder nur teilweise umgesetzten IT-Grundschutzmaßnahmen ausgewertet. Diese wurden in einer Tabelle einschließlich einer Priorität zusammengefasst.
2. Konsolidieren der Maßnahmen: Die noch umzusetzenden IT-Sicherheitsmaßnahmen wurden konsolidiert.
3. Kosten- und Aufwandsschätzung: Für jede zu realisierende Maßnahme wurde festgehalten, welche Investitionskosten und welcher Personalaufwand dafür benötigt werden. Gleichzeitig wurde festgelegt, ob diese wirtschaftlich umsetzbar, ob bestimmte Maßnahmen durch Ersatzmaßnahmen ersetzt werden können oder ob das Restrisiko, das durch die fehlende Maßnahme entsteht, tragbar ist.
4. Festlegung der Umsetzungsreihenfolge der Maßnahmen: Danach wurde eine Umsetzungsreihenfolge anhand der Priorität, der zwingenden zeitlichen Reihenfolge und der Wirkung der Maßnahmen festgelegt.
5. Festlegung der Verantwortlichkeit: Anschließend wurde festgelegt, wer bis wann welche Maßnahmen realisieren muss. Ebenso wurde festgelegt, wer für die Überwachung der Realisierung verantwortlich ist.
6. Realisierungsbegleitende Maßnahmen: Zu diesen Maßnahmen gehörte die Schulung der Mitarbeiter, z. B. die Schulung der Mitarbeiter zum ausgewählten und einzusetzenden Firewall-System.

3.1.3.14 Präsentieren der Vorschläge bei den Entscheidern

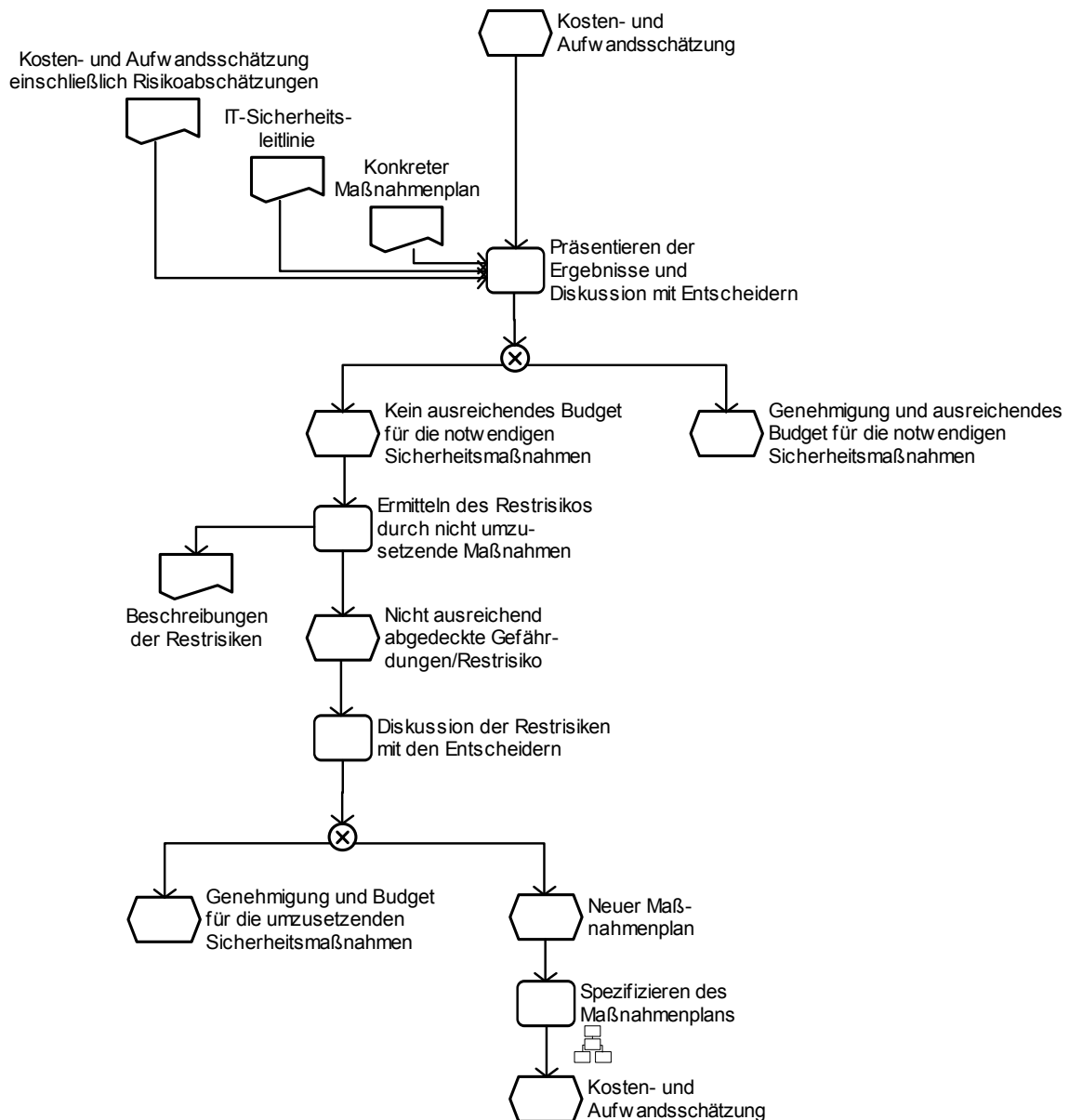


Abbildung 22: Präsentieren der Vorschläge bei den Entscheidern.

3.1.3.14.1 Tätigkeiten: Präsentieren der Vorschläge bei den Entscheidern

- Präsentieren der Ergebnisse bei Entscheidern (neben Leitungsebene ist auch der Betriebsrat einzubeziehen)
- Diskussion der Ergebnisse mit den Entscheidern mit dem Ziel, ein ausreichendes Budget für die Umsetzung der geplanten Sicherheitsmaßnahmen zu bekommen
- falls kein ausreichendes Budget zur Verfügung gestellt werden kann: Ermitteln und Dokumentieren der durch nicht umgesetzte Sicherheitsmaßnahmen entstehenden oder verbleibenden Risiken
- Diskussion dieser verbleibenden Risiken mit den Entscheidern, um eine Entscheidung über ein (erweitertes) Budget oder einen neuen Maßnahmenplan herbeizuführen

3.1.3.14.2 Kompetenzfelder: Präsentieren der Vorschläge bei den Entscheidern

Fähigkeiten/Fertigkeiten

- Präsentationen für unterschiedliche Zielgruppen vorbereiten, durchführen und nachbereiten können
- Argumentationsketten aufbauen können
- Diskussionen zu Sicherheitsmaßnahmen, ihrer Begründung, ihren Kosten vorbereiten und führen können
- Restrisiken ermitteln, dokumentieren und einschließlich ihrer möglichen Konsequenzen kommunizieren können
- Konflikte aushalten und konstruktiv beenden können

Wissen

- Risikoanalyse
- typische Kommunikationsmuster und Umgang mit diesen
- typische Konflikte, deren Ursachen und Symptome

Werkzeuge/Methoden

- BSI-Grundschutzhandbuch
- Kommunikationstechniken, Rhetorische Mittel
- Präsentationstools

3.1.3.14.3 Beispiel: Präsentieren der Vorschläge bei den Entscheidern

Die erarbeiteten Vorschläge wurden mittels einer Power Point Präsentation und der entsprechenden Hand-outs den Entscheidern dargestellt. Dabei hatte der IT-Sicherheitskoordinator die Sitzung vorher strategisch sinnvoll konzipiert und sich auch auf Einwände und Gegenargumente vorbereitet.

Insbesondere die Wichtigkeit der Vorschläge und die dadurch zu erreichenden Ziele der IT-Sicherheit wurden herausgestellt. Die verbleibenden Restrisiken wurden ebenfalls angesprochen.

3.1.3.15 Planen der Umsetzung

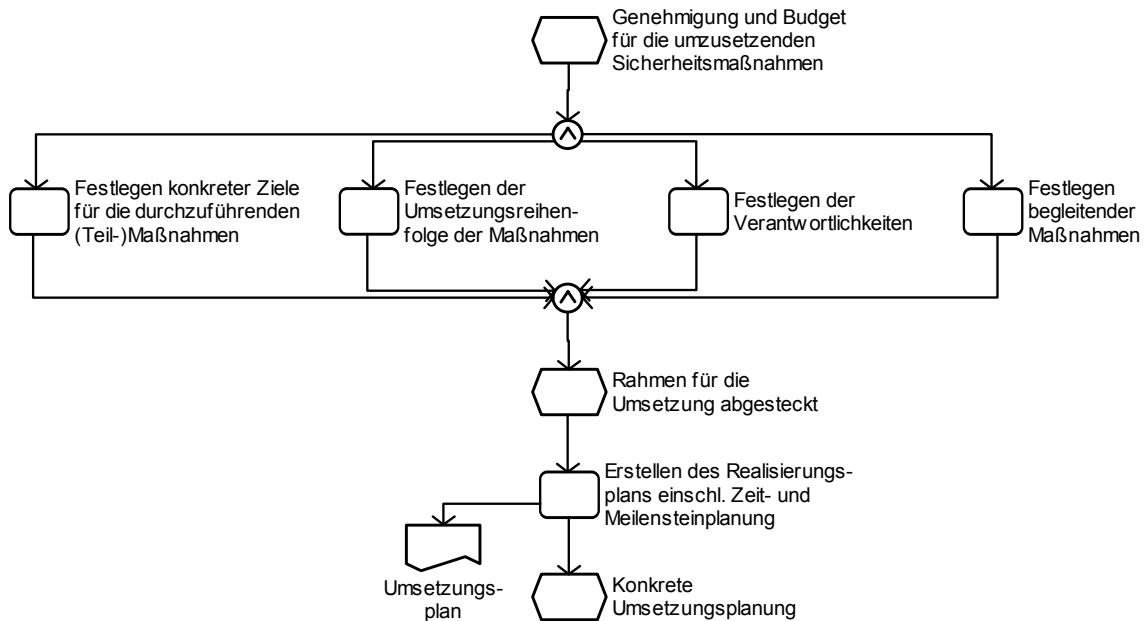


Abbildung 23: Planen der Umsetzung.

3.1.3.15.1 Tätigkeiten: Planen der Umsetzung

- Festlegen konkreter Ziele für die durchzuführenden Maßnahmen bzw. Maßnahmenteile
- Festlegen der Umsetzungsreihenfolge der Maßnahmen
- Festlegen der Verantwortlichkeiten für die Umsetzungen der Maßnahmen
- Festlegen begleitender Maßnahmen mit dem Gesamtziel, den Rahmen der Umsetzung der Maßnahmen abzustecken
- Erstellen eines Realisierungsplans für die Maßnahmen, einschließlich konkreter Zeit- und Meilensteinplanung

3.1.3.15.2 Kompetenzfelder: Planen der Umsetzung

Fähigkeiten/Fertigkeiten

- Maßnahmen konkret beschreiben können
- geplante Maßnahmen auf Durchführbarkeit und (ungewollte) Auswirkungen prüfen können
- durchzuführende Maßnahmen in sinnvolle zeitliche Reihenfolge bringen (gemäß sachlich-logischen Bezügen, Prioritäten, Auswirkungen, Schwachstellen etc.)
- Verantwortlichkeiten festlegen und durchsetzen können
- sinnvolle begleitende Maßnahmen auswählen und festlegen können (z. B. Schulungen)
- Verfügbarkeit von Ressourcen (finanzieller, technischer oder personaler Art) im Rahmen einer Ablaufplanung sicherstellen können
- Zeitplanung erstellen und Meilensteine festlegen können, Realisierungsplan erstellen können

Wissen

- Aufbau und Inhalt von Pflichtenheften/Maßnahmenplänen
- Planen von Prozessen, Auswirkungen auf Organisationsstrukturen
- Rationalisierungsmaßnahmen und Auswirkungen auf die IT-Sicherheit

Werkzeuge/Methoden

- Projektmanagement-Software

3.1.3.15.3 Beispiel: Planen der Umsetzung

Die bereits geplanten Maßnahmen zur Umsetzung wurden nach Genehmigung der Entscheider zeitlich definiert.

Danach wurde eine Umsetzungsreihenfolge anhand der Priorität, der zwingenden zeitlichen Reihenfolge und der Wirkung der Maßnahmen festgelegt.

Anschließend wurde festgelegt, wer bis wann welche Maßnahmen realisieren muss. Ebenso wurde festgelegt, wer für die Überwachung der Realisierung verantwortlich ist.

Zu diesen Maßnahmen gehörte die Schulung der Mitarbeiter, z. B. die Schulung der Mitarbeiter zum ausgewählten und einzusetzenden Firewall-System.

3.1.3.16 Begleiten der Umsetzung

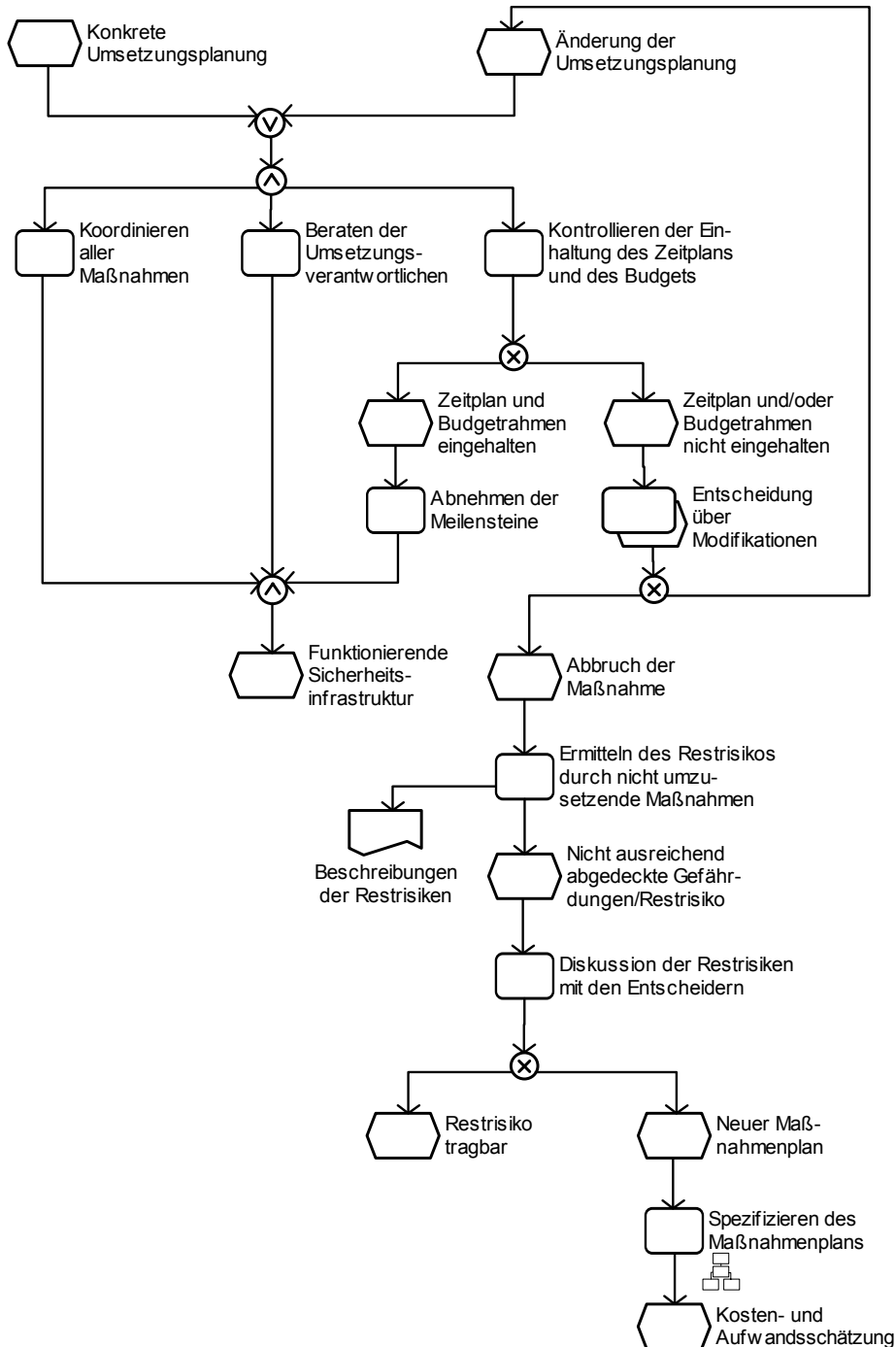


Abbildung 24: Begleiten der Umsetzung.

3.1.3.16.1 Tätigkeiten: Begleiten der Umsetzung

- Koordinieren aller Umsetzungsmaßnahmen
- Beraten der Umsetzungsverantwortlichen in Sicherheitsfragen
- Kontrollieren der Einhaltung des Zeitplans und des Budgets
- Abnehmen der Meilensteine mit dem Ziel einer funktionierenden, angemessenen Sicherheitsinfrastruktur

- falls bei der Umsetzung der Maßnahmen der Umsetzungsplan nicht eingehalten wird, muss über Abbruch oder Modifikation der Maßnahmenumsetzung entschieden werden; falls in diesem Zusammenhang Maßnahmen gar nicht umgesetzt werden können, muss wiederum das verbleibende Risiko ermittelt und mit den Entscheidern diskutiert werden

3.1.3.16.2 Kompetenzfelder: Begleiten der Umsetzung

Fähigkeiten/Fertigkeiten

- „die Fäden in der Hand behalten“ können
- umsetzungsrelevante Daten und Informationen zusammenführen und den jeweiligen Umsetzungsstatus erstellen können
- Aufwandssituation ermitteln und darstellen können
- Termsituation ermitteln und darstellen können
- Abweichungen zur Planung und Gründe dafür erkennen können
- Fortschritts-, Fertigstellungsgrade der Umsetzungen ermitteln und überwachen können
- Meilensteine und ihre Erreichung beurteilen können
- bei Problemen und Schwierigkeiten angemessen eskalieren können
- in Bezug auf sicherheitstechnische Belange bei der Umsetzung beraten und Entscheidungen treffen können
- Risikoanalyse durchführen können

Wissen

- Projektphasenmodelle, Projektlebenszyklus
- Projektüberwachung und -steuerung sowie mögliche Maßnahmen
- Dokumentationspflichten
- Grundlagen: Aufgaben und Organisation von Controlling
- Ressourcen-, Kostencontrolling
- Risikoanalyse

Werkzeuge/Methoden

- Moderation von Gesprächen und Besprechungen
- Methoden des Ablauf- und Terminmanagements (insbesondere zur Darstellung, Auswertung; z. B. Terminlisten, Fortschritts-, Balkendiagramme)
- Plan-Ist-Vergleiche
- Abweichungsanalysen

3.1.3.16.3 Beispiel: Begleiten der Umsetzung

Da sowohl die Hauptstelle als auch die Außenstellen zu einem definierten Zeitpunkt auf VPN umstellen mussten, lag ein besonderes Hauptaugenmerk auf der Umsetzung der für diesen Teil definierten Maßnahmen. Dabei wurden die Administratoren, insbesondere der Außenstellen, zentral beraten und unterstützt. Der IT-Sicherheitskoordinator war also vor allem koordinierend tätig.

3.1.3.17 Schulen der Mitarbeiterinnen und Mitarbeiter

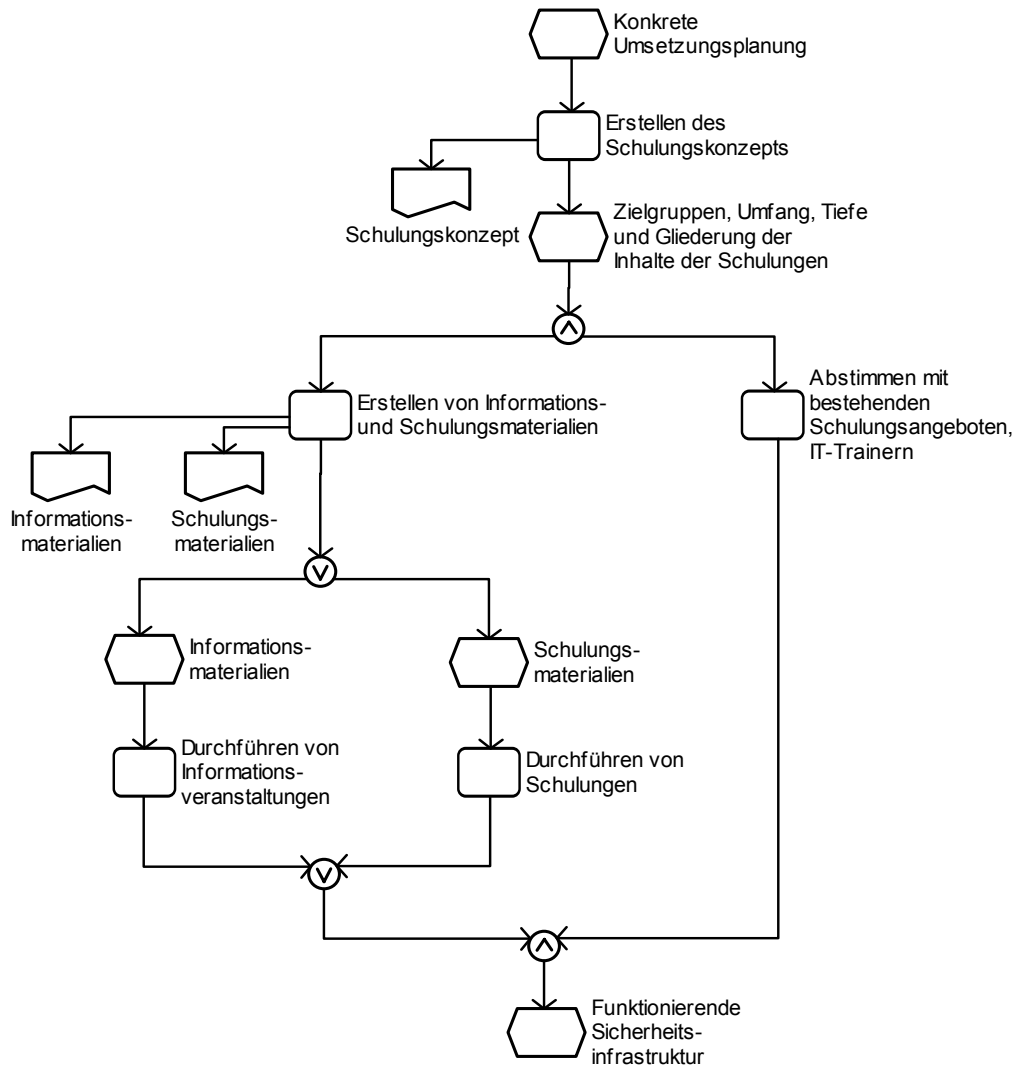


Abbildung 25: Schulen der Mitarbeiterinnen und Mitarbeiter.

Das Schulen der Mitarbeiterinnen und Mitarbeiter sollte in engem Zusammenhang mit dem Sensibilisieren (vgl. 3.1.3.4 „Sensibilisieren der Mitarbeiterinnen und Mitarbeiter für IT-Sicherheit“) stehen. Beides muss sich gegenseitig ergänzen.

3.1.3.17.1 Tätigkeiten: Schulen der Mitarbeiterinnen und Mitarbeiter

- Erstellen eines Schulungskonzepts über die neuen sicherheitstechnischen Maßnahmen, um Zielgruppen, Umfang, Gliederung und Inhalte der Schulungen festzulegen
- Erstellen von Schulungsmaterialien aus sicherheitstechnischer Sicht
- Abstimmen des Schulungskonzepts mit IT-Trainern und bestehenden Schulungsmaßnahmen, zusätzlich: Einbringen sicherheitsrelevanter Inhalte in bestehende Schulungsangebote
- Durchführen von Informationsveranstaltungen
- Durchführen von Schulungen für bestimmte Zielgruppen, alles mit dem Ziel einer funktionierenden Sicherheitsinfrastruktur

3.1.3.17.2 Kompetenzfelder: Schulen der Mitarbeiterinnen und Mitarbeiter

Fähigkeiten/Fertigkeiten

- Schulungskonzept erstellen und dabei vor allem die anzusprechenden Zielgruppen und die Ziele der Schulungen gemäß Sicherheitsstrategie und -konzept festlegen und begründen können
- Kompetenzen der zu Schulenden einschätzen können
- sich in andere Personen hineinversetzen können
- Schulungsmaterialien zu sicherheitstechnischen Belangen auswählen und erstellen können
- IT-Trainer/innen für sicherheitsrelevante Belange sensibilisieren können
- Schulungsunterlagen gemäß IT-Sicherheitskonzept modifizieren können
- Informationsveranstaltungen (z. B. mitarbeiter- oder produktbezogene IT-Sicherheitsmaßnahmen, Einsatz von Passwörtern, Datenschutz und Datensicherheit) vorbereiten, durchführen und nachbereiten können
- Schulungsveranstaltungen zu IT-Sicherheitsthemen (z. B. mitarbeiter- oder produktbezogene IT-Sicherheitsmaßnahmen, Einsatz von Passwörtern, Datenschutz und Datensicherheit, Notfallmaßnahmen, Social Engineering) vorbereiten, durchführen und nachbereiten können
- Schulungen und Informationsveranstaltungen thematisch und zeitlich (Dauer, Art, Wiederholungsrate) angemessen planen können
- Schulungen auf Aktualität und angemessene Inhalte prüfen können
- Einweisungen in sicherheitstechnische Belange durchführen können
- Einweisungskonzepte erstellen können
- präsentieren, moderieren und vermitteln können

Wissen

- didaktische Grundlagen, didaktische Gestaltung von Unterlagen
- Sensibilisierung, Motivation, Motivationstypen
- Lernprozesse (Gestaltung, Medien, Wege der Wissensvermittlung)
- Kommunikation und Kommunikationsmodelle
- Elemente und Regeln verbaler und nonverbaler Kommunikation
- typische Kommunikationsmuster und Umgang mit diesen
- aktuelle, produktbezogene Sicherheitsmaßnahmen
- Social Engineering
- sichere elektronische Kommunikation, Sicherheitsaspekte bestimmter IT-Systeme und Anwendungen, sichere Software-Entwicklung, Erstellung und Revision von IT-Sicherheitskonzepten

Werkzeuge/Methoden

- Präsentations- und Moderationstechniken
- Motivationsmethoden
- Visualisierungstechniken
- Informations- und Wissensvermittlung

3.1.3.17.3 Beispiel: Schulen der Mitarbeiterinnen und Mitarbeiter

Für die Schulung der Administratoren für den Bereich Firewall und VPN wurden ein entsprechender Schulungsanbieter ausgewählt und die Schulungen terminiert. Für die Schulungen wurden die Standard-Seminarunterlagen des Herstellers verwendet.

3.1.3.18 Durchführen von Funktionsprüfungen

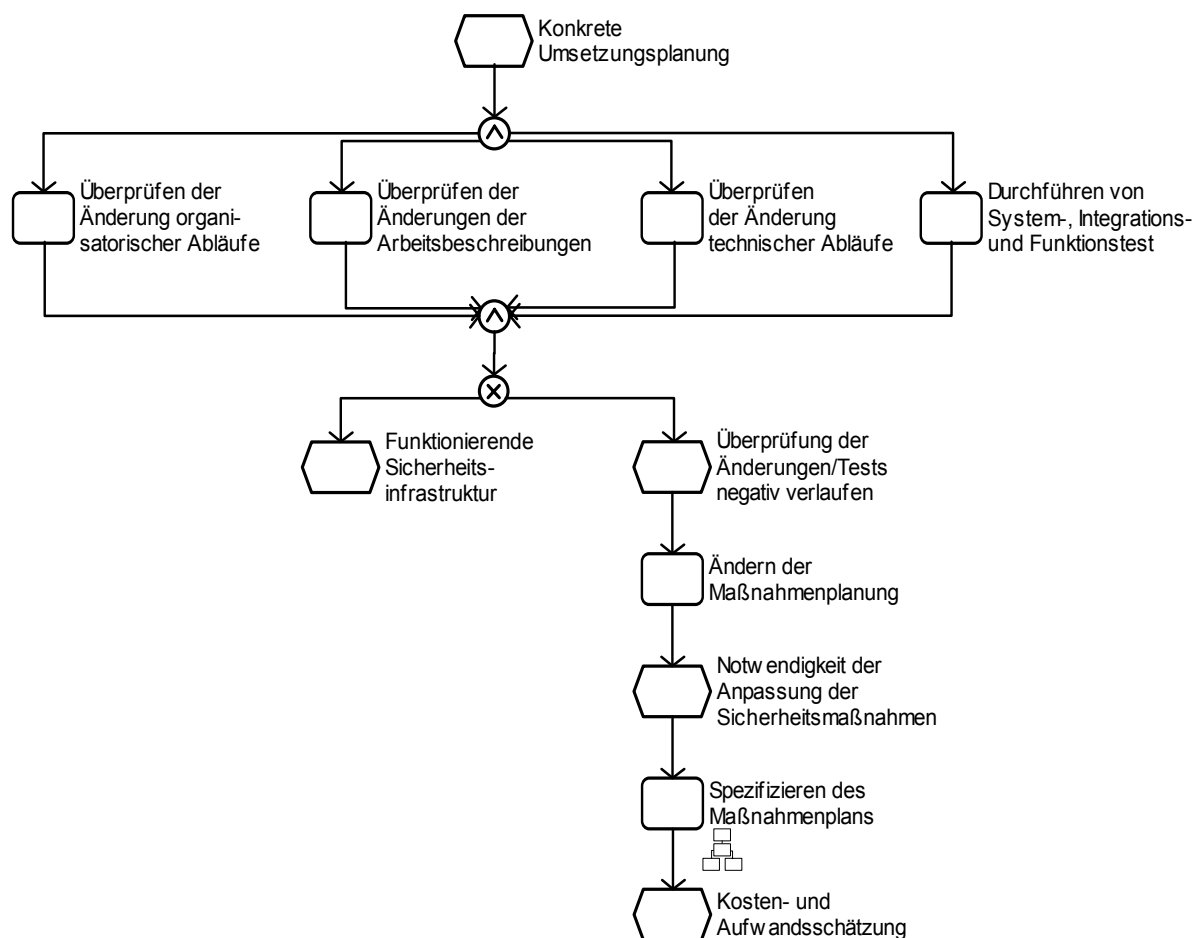


Abbildung 26: Durchführen von Funktionsprüfungen.

3.1.3.18.1 Tätigkeiten: Durchführen von Funktionsprüfungen

- Überprüfen der Änderungen der organisatorischen Abläufe gemäß Maßnahmenplan und -ziel
- Überprüfen der Änderungen der Arbeitsbeschreibungen gemäß Maßnahmenplan und -ziel
- Überprüfen der Änderungen der technischen Abläufe gemäß Maßnahmenplan und -ziel
- Durchführen von System-, Integrations- und Funktionstests
- auch hier ist das Ziel eine funktionierende Sicherheitsinfrastruktur: wenn die Überprüfungen oder Tests negativ verlaufen, sind Änderungen der Maßnahmenplanung durchzuführen bis hin zur erneuten Spezifikation von Maßnahmenplänen

3.1.3.18.2 Kompetenzfelder: Durchführen von Funktionsprüfungen

Fähigkeiten/Fertigkeiten

- durchgeführte Änderungen auf Funktionalität und Entsprechung mit dem Maßnahmenplan prüfen können
- in Zusammenarbeit mit Entwicklern oder Administratoren System-, Integrations- und Funktionstests durchführen können

- Ergebnisse der Prüfungen dokumentieren können
- bei negativem Ergebnis der Prüfung angemessene Maßnahmen ableiten und begründen können

Wissen

- Organisation, Arbeitsabläufe und -beschreibungen
- System-, Integrations- und Funktionstest
- Netzwerktechnik und -topologie
- Datenübertragungssysteme und -techniken, Hardware-Schnittstellen
- System- und Kommunikationsarchitekturen
- Netzwerk- und Kommunikationsprotokolle, Schnittstellen
- Funktionsweise von Scannern/Sniffern, Würmern, Viren, Trojanern und Hybriden
- Funktionsweise gängiger Hackersoftware

Werkzeuge/Methoden

[sehr von den spezifischen Maßnahmen abhängig]

3.1.3.18.3 Beispiel: Durchführen von Funktionsprüfungen

Im konkreten Fall wurden in der Umsetzung System- und Funktionstests durchgeführt.

Das definierte Regelwerk der Firewall wurde implementiert und mithilfe von Testsystemen auf die Funktionsweise geprüft. Insbesondere das Zusammenspiel der Firewall in der Hauptstelle mit den Firewalls der Außenstellen in Bezug auf VPN wurde getestet.

Da die Tests positiv verliefen, mussten keine Anpassungen vorgenommen werden.

3.1.3.19 Dokumentieren des gesamten IT-Sicherheitsprozesses

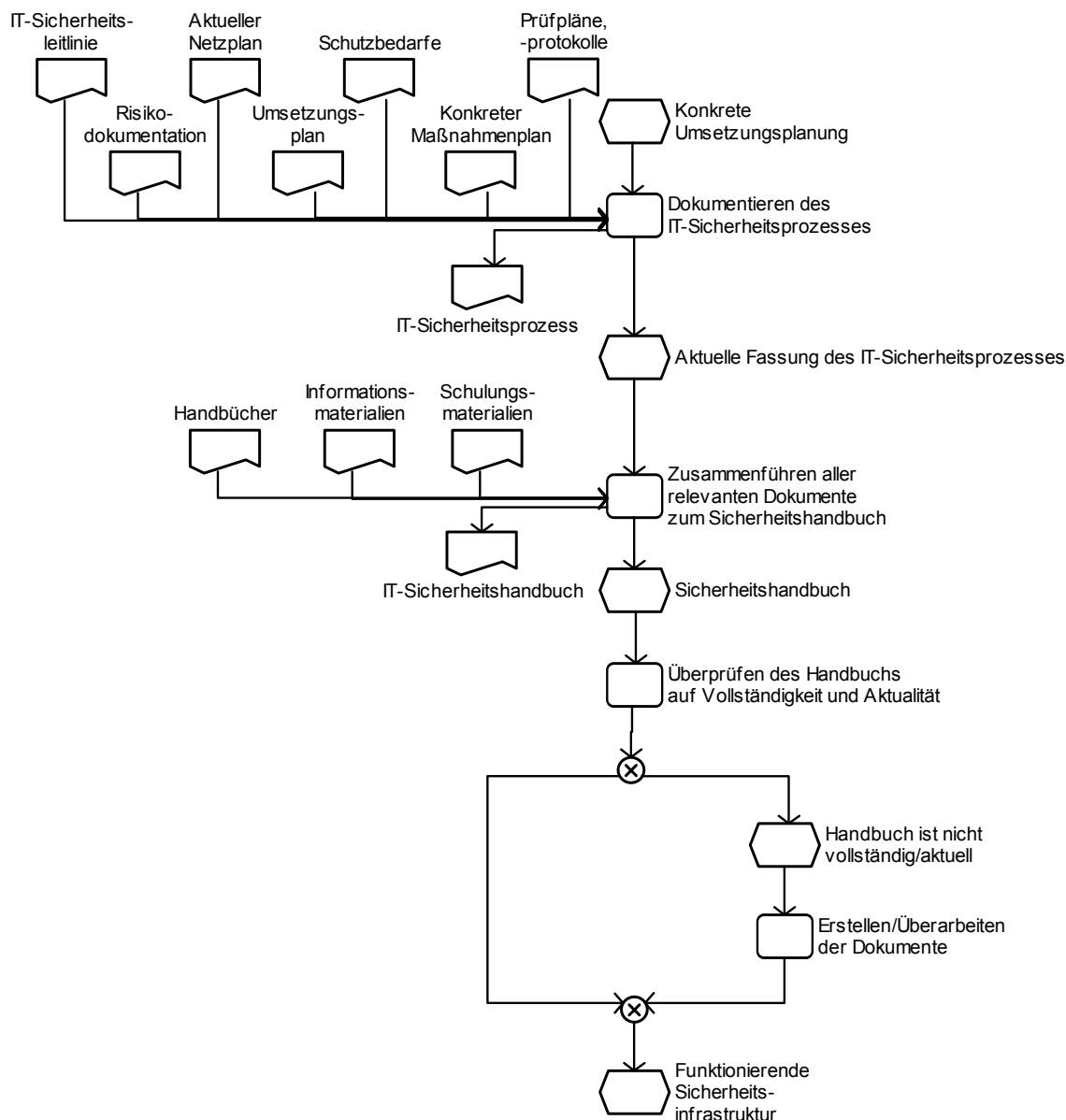


Abbildung 27: Dokumentieren des gesamten IT-Sicherheitsprozesses.

3.1.3.19.1 Tätigkeiten: Dokumentieren des gesamten IT-Sicherheitsprozesses

- Dokumentieren des IT-Sicherheitsprozesses gemäß BSI-Grundschutzhandbuch (Abschnitt M 2.201) und unter Zuhilfenahme von IT-Sicherheitsleitlinien, Risikodokumentation, Schutzbedarfsliste, aktuellem Netzplan, Umsetzungsplan, Dokumentation der Umsetzungsmaßnahmen sowie Prüfplänen und Prüfprotokollen
- Zusammenführen aller relevanten Dokumente zum Sicherheitshandbuch sowie zur Dokumentation der Datenschutzrichtlinien und -maßnahmen
- Überprüfen des Handbuchs auf Vollständigkeit und Aktualität und ggf. Überarbeiten des Handbuchs bzw. Erstellen der fehlenden Dokumente

3.1.3.19.2 Kompetenzfelder: Dokumentieren des gesamten IT-Sicherheitsprozesses

Fähigkeiten/Fertigkeiten

- Dokumente zielgruppenspezifisch strukturieren und aufbereiten können
- Dokumente auf sicherheitstechnische Relevanz beurteilen und entsprechend aufbereiten können
- sich in die Rolle des anderen versetzen können
- Informationen sinnvoll zusammenstellen und schriftlich fixieren können
- Nutzeradäquanz von Dokumentationen und ihrer Aufbereitung beurteilen können
- Aktualität und Vollständigkeit von sicherheitsrelevanten Dokumenten prüfen und nachhalten können

Wissen

- Dokumentationsrichtlinien, -standards
- Sicherheitshandbuch
- Sicherheitsprozess, -leitlinien, konzepte
- Arten der Informationsaufbereitung

Werkzeuge/Methoden

- Dokumentenverwaltung, Archivierung, Logging

3.1.3.19.3 Beispiel: Dokumentieren des gesamten IT-Sicherheitsprozesses

Für das Unternehmen wurde abschließend ein Sicherheitshandbuch mit dem Inhalt gemäß den allgemein anerkannten Grundsatzforderungen des BSI erstellt. Themen waren:

- Beschreibung der Sicherheitspolitik des Unternehmens
- Dokumentation der eingesetzten Sicherheitsprodukte
- verbindliche Verfahrensanweisungen zur Aufrechterhaltung der Sicherheit
- Verfahrensanweisungen für Reaktionen nach Sicherheitsbeeinträchtigungen (Disaster Recovery)
- Empfehlung von Informationsquellen bei Sicherheitsfragen