Ein Managementsystem für die Informationssicherheit einführen

Fach	IT-Technik
Lernfeld	LF 4: Schutzbedarfsanalyse im eigenen Arbeitsbereich durchführen
Querverweise zu weiteren Lernfeldern des Lehrplans	LF 1: Das Unternehmen und die eigene Rolle im Betrieb beschreiben LF 2: Arbeitsplätze nach Kundenwunsch ausstatten LF 3: Clients in Netzwerke einbinden LF 7: Cyber-physische Systeme ergänzen LF 11b, 11d, 11 (SE): Betrieb und Sicherheit vernetzter Systeme gewährleisten
Zeitrahmen	12 Unterrichtstunden
Benötigtes Material	Beamer und Dokumentenkamera, Rechner für je zwei Schüler/innen mit Office-Software, Informationsblätter, zentrale Dateiablage, Übungs-Rechner oder -Laptops, USB-Sticks

Kompetenzerwartungen

Die Schülerinnen und Schüler …

- beschreiben den BSI IT-Grundschutz anhand selbsterstellter Kriterien.
- stellen die zum Aufbau eines ISMS nötigen Schritte dar und vergleichen diese.
- setzen standardisierte Verfahren zur Erhöhung der Informationssicherheit ein und überprüfen diese.
- ermitteln, anhand bestimmter Kriterien welcher Schutz für Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik angemessen ist.
- verstehen die Informationssicherheit als kontinuierlichen Prozess und wenden diese an.
- verschlüsseln USB-Datenträger und die Festplatten tragbarer IT-Systeme und bewerten deren Nutzen.

Aufgabe

1. **Orientieren:**

   Die Werbeagentur GAB GmbH wurde in der letzten Zeit häufiger von Malware, speziell von Emotet, befallen. Dadurch wurde Ransomware eingeschleust. Wichtige Firmendaten wurden durch Verschlüsselung unbrauchbar gemacht und es wurde ein Lösegeld für deren Entschlüsselung verlangt.
   Aus diesem Grund macht die Firmenleitung die Informationssicherheit zur Chefsache und beschließt, dass in der GAB GmbH ein Managementsystem für die Informationssicherheit (Information Security Management System - ISMS) eingeführt werden soll.
   Die Schülerinnen und Schüler als Mitarbeiter der Firma JackSEC GmbH werden im Team die GAB GmbH beraten und dort die Einführung des ISMS begleiten.
   Zunächst verschaffen sie sich einen Überblick darüber, wie die Informationssicherheit bedroht werden kann. Dazu sehen sie sich ein passendes Video (www.youtube.com/watch?v=M6aaYralX2g) an und besprechen kurz die 6 dargestellten Probleme in Teamarbeit.

2. **Informieren:**

   Um weiter in das Thema ISMS einzusteigen, informiert der Senior Analyst der JackSEC GmbH (Lehrkraft) seine Schüler-Teams über einen Vortrag dazu. Mit Hilfe eines Info-Textes zum IT-Grundschutz und zu ISMS und mit den ISMS-Vortragsfolien beantworten die Teams die dazu vorbereiteten Fragen und laden die Antworten auf die zur Verfügung gestellte Dateiablage hoch. Der Senior Analyst sichtet die Antworten und bespricht diese anschließend mit den einzelnen Teams.

3. **Planen:**

   Um den Weg zum Aufbau eines ISMS genauer planen zu können, informieren sich die Schüler-Teams zunächst über die Tätigkeit des Informationssicherheitsbeauftragten (ISB). Anschließend befassen sie sich mit den Inhalten und der Erstellung des zentralen ISMS-Strategiedokuments, der Informationssicherheitsleitlinie.
   Zur Vorbereitung der nächsten Schritte sehen sich die Schülerinnen und Schüler einzeln ein Video an, das eine Zusammenfassung zur Erstellung eines Sicherheitskonzeptes zeigt (www.youtube.com/watch?v=dPhufJqQf7A).

4. Durchführen:

Um noch tiefer in die Verfahrensweisen des BSI IT-Grundschutzes einzusteigen, bearbeiten die Schülerinnen und Schüler selbstständig und eigenverantwortlich vorgegebene Lerneinheiten des Online-Kurs IT-Grundschutz mit dem Ziel, die Testfragen am Ende jeder Lektion beantworten zu können. Dabei steht ihnen auch während dieser Lernphase der Senior Analyst der JackSEC GmbH (Lehrkraft) als Unterstützer und Moderator zur Verfügung.

Im nächsten Schritt beschäftigen sich die Teams mit dem wichtigsten Teil des IT-Grundschutzes, dem Sicherheitskonzept, das dazu dient, im Unternehmen vorhandene IT-Sicherheitsdefizite zu ermitteln. Zu Beginn ist dazu eine Strukturanalyse nötig, bei der alle Schutzobjekte (Assets) erfasst und festgelegt werden. Um diese umfangreiche Analyse für die Schülerinnen und Schüler greifbarer zu machen, müssen die Teams zunächst an einem Beispiel darstellen, wie aus einem Netzplan ein bereinigter Netzplan entstanden ist. Auch das Erfassen der IT-Systeme und Räume wird an dem im Online-Kurs IT-Grundschutz dargestellten Beispielunternehmen und einer dazu vorbereiteten Tabelle praktisch umgesetzt. Jetzt wird an einigen, von den Teams selbst gewählten, Schutzobjekten beispielhaft eine Schutzbedarfsfeststellung durchgeführt. Schließlich wird den Teams auf Basis der Schutzbedarfs-Erfassungstabelle der IT-Systeme das Maximumprinzip, der Kumulationseffekt und der Verteilungseffekt dargestellt.

Die Schülerinnen und Schüler beenden diese Phase der Lernsituation in Partnerarbeit, indem sie

aus einem Video (www.youtube.com/watch?v=MmHO4apXCW8) entnehmen, wie der häufigste Fehler vermieden werden kann, der möglicherweise bei der Umsetzung eines ISMS passiert.

Damit die IT-Praxis nicht zu kurz kommt, arbeiten die Schülerinnen und Schüler am Ende der Lernsituation im Team und lernen den IT-Grundschutz-Baustein "INF.9 Mobiler Arbeitsplatz" kennen. Die Gruppen sollen praktisch umsetzbare Vorschläge dazu zu machen, wie Festplatten und USB-Datenträger sicher verschlüsselt werden können, dies praktisch umsetzen, der Lehrkraft demonstrieren und ihre Vorschläge in Form eines Kochrezepts dokumentieren.

5. Kontrollieren und Bewerten:

Am Ende diskutieren die Schülerinnen und Schüler in Gruppen über Aufgabenstellungen, Schwierigkeiten und Lösungs-Alternativen und geben Feedback. Über ein vorbereitetes Formular können sie auch ihren eigenen Lernfortschritt beurteilen.

Hinweis zum Unterricht

Der IT-Grundschutz ist ein sehr umfangreiches Verfahren, deshalb ist es völlig ausreichend, wenn den Schülerinnen und Schülern der Wesenskern der Schutzbedarfsanalyse anschaulich gemacht wird. Die zentrale Dateiablage hilft, die Arbeitsergebnisse zu sichern und so den Lernfortschritt der einzelnen Teams im Blick zu haben. Im Idealfall wird die Lernsituation komplett über einen entsprechenden Mebis-Kurs bearbeitet.
Für die praktischen Übungen sind durchweg administrative Rechte nötig. Ideal sind Übungs-Rechner, die sich auch von den Schülerinnen und Schülern einfach am Ende der Praxisphase restaurieren lassen. Für die Übungen zum Verschlüsseln der Datenträger wird ein Klassensatz schneller (>40MB/s) USB3-Sticks benötigt.

Querverweise zu anderen Fächern/Fachrichtungen

Diese Lernsituation schafft Grundlagenwissen zur konkreten Umsetzung von IT-Sicherheit, das in praktisch allen technischen Fächern/Lernfeldern der IT-Berufe benötigt wird. Die Verbindung von betriebswirtschaftlichen und technischen Inhalten wird hier besonders deutlich, da ja die durch ein ISMS geschützten primären Assets immer die wesentlichen Geschäftsprozesse eines Unternehmens sind.

Quellen- und Literaturangaben

- BSI - Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/
- ISMS: https://de.wikipedia.org/wiki/Information_Security_Management_System
- BSI IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
- Online-Kurs IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/itgrundschutzschulung_node.html

Anhang

- Lernsituation
- Vortragsfolien

IT-Technik

ISMS - Ein Managementsystem für die Informationssicherheit

Aufgabe

Die Werbeagentur GAB GmbH wurde in der letzten Zeit häufiger von Malware befallen. Aus diesem Grund beschließt die Firmenleitung, ein Managementsystem für die Informationssicherheit einzuführen. Sie als MitarbeiterIn der Firma JackSEC GmbH werden zusammen mit Ihrem Team die GAB GmbH beraten und dort die Einführung des Informations-Sicherheits-Management-Systems (ISMS) begleiten.

Ziele

- Probleme und Lösungen in der Informationssicherheit genauer darstellen
- die zum Aufbau eines ISMS nötigen Schritte darstellen
- bei der Umsetzung von Informationssicherheit geplant und zielgerichtet vorgehen
- Ermitteln, welcher Schutz für Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist
- Strukturanalyse und Schutzbedarfsfeststellung genauer kennenlernen
- USB-Datenträger und tragbare IT-Systeme verschlüsseln

LS_02_Managementsystem für die Informationssicherheit.doc

Arbeitsanleitung

Hinweis: Für die weitere Bearbeitung beachten Sie bitte die Hinweise zum Unterricht!

1 Ausgangssituation - Das Problem

Die Werbeagentur GAB GmbH wurde in der letzten Zeit häufiger von Malware, speziell von Emotet, befallen. Dadurch wurde Ransomware eingeschleust. Wichtige Firmendaten wurden durch Verschlüsselung unbrauchbar gemacht und es wurde ein Lösegeld für deren Entschlüsselung verlangt.

Aus diesem Grund macht die Firmenleitung die Informationssicherheit zur Chefsache und beschließt, dass in der GAB GmbH ein Managementsystem für die Informationssicherheit (*Information Security Management System* - ISMS) eingeführt werden soll.

Sie als MitarbeiterIn der Firma JackSEC GmbH werden zusammen mit Ihrem Team die GAB GmbH beraten und dort die Einführung des Informations-Sicherheits-Management-Systems (ISMS) begleiten.

2 Bedrohte Informationssicherheit

Aufgabe: Zunächst möchten Sie sich mit Ihrem Team einen Überblick darüber verschaffen, wie die Informationssicherheit bedroht werden kann. **A**
Schauen Sie sich dazu dieses Video (www.youtube.com/watch?v=M6aaYralX2g) an und besprechen Sie die 6 dargestellten Probleme kurz in Ihrem Team.
Zählen Sie diese Probleme nachfolgend auf.

3 Ein ISMS nach BSI IT-Grundschutz

A

Aufgabe: Ein Senior Analyst der JackSEC GmbH (Lehrkraft) wird Sie mit einem Vortrag zum Thema ISMS informieren.
Beantworten Sie anschließend mit Hilfe des Info-Textes zum IT-Grundschutz und zu ISMS auf S.10 im Anhang und mit den ISMS-Vortragsfolien die folgenden Fragen. Einigen Sie sich in Ihrem Team jeweils auf eine Antwort. Laden Sie Ihre Antworten zusammen mit den Fragen auf die zur Verfügung gestellte Dateiablage hoch. Der Senior Analyst bespricht anschließend die Antworten mit Ihnen.

1.) Was ist ein ISMS und wozu wird es (vor allem in größeren Firmen) benötigt?

2.) Was wird unter dem BSI IT-Grundschutz-Verfahren (IT-Grundschutz-Methode) verstanden?

3.) Der BSI-Grundschutz und die ISO 27001 sind sind Verfahrensweisen, um ein ISMS umzusetzen. Welches dieser Verfahren macht genauere Angaben über notwendige IT-Schutzmaßnamen?

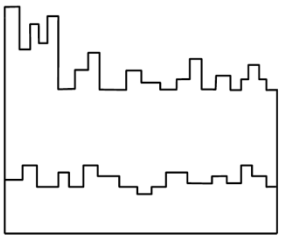
4.) Welche Bestandteile bilden den Kern des BSI-Grundschutzes?

5.) Was ist ein "BSI-Grundschutz Baustein"?

6.) Beschreiben Sie kurz die drei Varianten der Absicherung nach dem BSI IT-Grundschutz-Verfahren.

7.) Im Rahmen der Kernabsicherung wird von "Kronjuwelen" gesprochen. Was heißt das?

8.) Die folgende Grafik taucht häufig auf, wenn es um das Thema BSI IT-Grundschutz geht.



a) Zeigen Sie daran die drei Absicherungs-Varianten
b) Skizzieren Sie die Linie für den normalen Schutzbedarf hinein.
c) Markieren Sie die Assets der Kronjuwelen.

9.) Erklären Sie an einer grafischen Darstellung die einzelnen ISMS-Schritte/Phasen.

10.) Auf Initiative der Geschäftsleitung der GAB GmbH wird zur Einführung des ISMS ein IT-Sicherheitsmanagement-Team gebildet. Hierbei ist die Bestimmung des Informations-sicherheitsbeauftragten (ISB) ein wichtiger Schritt. Welche Aufgaben hat der ISB?

11.) Wozu dient das "Sicherheitskonzept"?

12.) Mit dem Begriff "Schutzobjekt" (engl. *Asset*) werden genau die fachlichen und technischen Werte eines Unternehmens bezeichnet, für die im Sicherheitskonzept Schutzmaßnahmen festgelegt werden müssen. Schutzobjekte sind z.B. Informationen, Anwendungen, IT- oder IoT-Systeme, Netze, Räume aber auch zuständige Mitarbeiter. Nennen Sie mindestens 5 konkrete Beispiele für Schutzobjekte.

13.) Beschreiben Sie einen Fall, bei dem es sinnvoll ist, ein bestehendes ISMS anzupassen.

14.) Was sind "Awareness-Aktivitäten"?

4 Aufbau eines ISMS

Aufgabe: Auf Initiative der Geschäftsleitung der GAB GmbH wird zur Einführung des ISMS ein IT-Sicherheitsmanagement-Team gebildet. Hierbei ist die Bestimmung des Informationssicherheitsbeauftragten (ISB) ein wichtiger Schritt. Welche Aufgaben hat der ISB? A

Aufgabe: Das zentrale Strategiedokument für die Informationssicherheit in einem Betrieb ist die Informationssicherheitsleitlinie (Security Policy). Erklären Sie, warum die Informationssicherheitsleitlinie so wichtig ist. A

Aufgabe: Im Anhang auf S.12 finden Sie ein Beispiel für eine betriebliche Informationssicherheitsleitlinie. Zum weiteren Verständnis beantworten Sie dazu folgende Fragen: A

1.) Welche Person/welches Team hat diese Informationssicherheitsleitlinie erstellt?

2.) An welchem Ort gilt diese Informationssicherheitsleitlinie?

3.) Was ist eine "Stabsfunktion"?

4.) Wie wird das zu erstellende ISMS genannt?

5.) In welchem Punkt wird verlangt, dass alle Mitarbeiter die Inhalte der Leitlinie kennen und umsetzen müssen?

6.) Aus welchem Grund ist der Firma Qualsoft die Informationssicherheit sehr wichtig?

Aufgabe: Zur Vorbereitung auf die nächsten Schritte sollten Sie sich diesen Film ansehen, der eine Zusammenfassung zur Erstellung eines Sicherheitskonzeptes zeigt. (www.youtube.com/watch?v=dPhufJqQf7A) A

Aufgabe: Jetzt werden Sie noch tiefer in die Verfahrensweisen des BSI IT-Grundschutzes einsteigen. Bearbeiten Sie dazu selbstständig und eigenverantwortlich im Online-Kurs IT-Grundschutz (auch als PDF-Datei) die unten angegebenen Lerneinheiten mit dem Ziel, die Testfragen am Ende jeder Lektion beantworten zu können. Der Senior Analyst der JackSEC GmbH (Lehrkraft) steht Ihnen auch während dieser Lernphase als Unterstützer und Moderator zur Verfügung. A

Lektion 2: Sicherheitsmanagement
Lektion 3: Strukturanalyse
Lektion 4: Schutzbedarfsfeststellung
Lektion 5: Modellierung gemäß IT-Grundschutz
Lektion 6: IT-Grundschutz-Check

5 Das Sicherheitskonzept

Das Sicherheitskonzept (auch *Sichheitskonzeption* genannt) ist der wichtigste Teil des IT-Grundschutzes und dient dazu, **vorhandene IT-Sicherheitsdefizite** zu **ermitteln**.
Wesentliche Schritte sind: Geltungsbereich (Informationsverbund) festlegen, Strukturanalyse (Schutzobjekte festlegen), Schutzbedarfsfeststellung, Modellierung, IT-Grundschutz-Check, evtl. Risikoanalyse und die Umsetzungsplanung.

Aufgabe: Bei der **Strukturanalyse** werden alle Schutzobjekte (Assets) erfasst und festlegt. Dazu gehört auch der Netzplan (siehe Online-Kurs: Lerneinheit 3.5: Netzplan erheben). Dieser wir meist in einer "bereinigten" Art verwendet. Im Anhang auf S.14 sind ein detaillierter und ein bereinigter Netzplan dargestellt. Stellen Sie mithilfe von Markierungen, Pfeilen, Kreisen und Anmerkungen dar, wie daraus der bereinigte Netzplan entstanden ist. **A**

Aufgabe: Ein wichtiger Teilschritt der Strukturanalyse ist das Erfassen der IT-Systeme und Räume. Die folgende Tabelle zeigt dazu einen Auszug. Buchstaben kennzeichnen den Typ eines IT-Systems (z.B. **D**: Desktop-PC, **L**: Laptop, **S**: Server, **N**: Netzwerkkomponente).
Ergänzen Sie in der Tabelle die Laptops der Geschäftsführung, alle Switches, die Desktops der Finanzbuchhaltung und die Domänencontroller. **A**

IT-Systeme			
Bezeichung und Beschreibung	**Raum/Standort** BG: Bad Godesberg BB: Beuel	**Anzahl**	**Benutzer/ Verantwortlich**
N001 Router Internetanbindung *Dieser Router regelt die Kommunikation zwischen dem Internet und dem internen Netz.*	*Serverraum/BG*	*1*	*Administratoren/ IT-Betrieb*

Bei der **Schutzbedarfsfeststellung** wird für jedes erfasste und festgelegte Schutzobjekt die Höhe des benötigten Schutzes bestimmt. Diese Fragen müssen dabei beantwortet werden:
- Wie viel Schutz benötigen die festgelegten Schutzobjekte?
- Welche Schutzobjekte benötigen mehr Schutz als der Standard angibt?
- Wie kommen wir zu den genauen Einschätzungen des Schutzbedarfs?

Der Schutzbedarf ist davon abhängig, welcher Schaden entstehen kann, wenn für ein Schutzobjekt die Schutzziele *Vertraulichkeit*, *Integrität* oder *Verfügbarkeit* verletzt werden. A

Aufgabe: Ordnen Sie die verletzten Schutzziele den folgenden Beschreibungen zu:

a) *Die Korrektheit von Informationen ist nicht mehr gewährleistet.*

b) *Vertrauliche Informationen werden unberechtigt weitergegeben.*

c) *Autorisierte Benutzer werden am Zugriff auf Informationen und Systeme behindert.*

Der Schaden, der von einer Verletzung der Schutzziele ausgehen kann, kann sich auf verschiedene **Schadensszenarien** beziehen, z.B.:

1 Verstöße gegen Gesetze, Vorschriften oder Verträge
2 Beeinträchtigungen des informationellen Selbstbestimmungsrechts
3 Beeinträchtigungen der persönlichen Unversehrtheit
4 Beeinträchtigungen der Aufgabenerfüllung
5 negative Innen- oder Außenwirkung
6 finanzielle Auswirkungen

Das IT-Grundschutz-Verfahren empfiehlt, dass jede Institution die zu erwartenden Schäden anhand von Schadensszenarien in **drei Schutzbedarfskategorien** einteilt.

Schutzbedarfs-Kategorie	**Schadens-auswirkungen**	**Beeinträchtigung der Aufgaben-erfüllung**	**maximale Ausfallzeit**	**finanzieller Schaden** z.B. bezogen auf den Monatsumsatz
normal	begrenzt und überschaubar	tolerabel	mehrere Tage	< 1 %
hoch	beträchtlich	nicht tolerabel	einzelne Tage	1 - 10 %
sehr hoch	katastrophal	Existenz bedrohend	Stunden	> 10 %

Aufgabe: Ergänzen Sie die Tabelle um mindestens 2 weitere beliebige Beispiele! A

Beispiel für ein betroffenes Schutzobjekt	**Schutzbedarfskategorie und Schutzziele**			**Schadens-szenarien** Mehrfachnen-nung möglich
	Vertraulichkeit	**Integrität**	**Verfügbarkeit**	
zentraler Datenbankserver der Produktion	*normal*	*hoch*	*sehr hoch*	*4, 5, 6*
Dateiserver der Personalabteilung	*sehr hoch*	*hoch*	*normal*	*1, 2, 5, 6*

Maximumprinzip, Kumulationseffekt, Verteilungseffekt

Aufgabe: Auszug aus der Erfassungstabelle für den Schutzbedarf der IT-Systeme (siehe detaillierter Netzplan im Anhang auf S.14).

A

Bezeich-nung	Beschreibung des Systems	Schutzziel und Schutzbedarf	Begründung
S001	Domänen-controller	Vertraulichkeit:	
		Integrität:	
		Verfügbarkeit:	
S002	Dateiserver	Vertraulichkeit:	
		Integrität:	
		Verfügbarkeit:	
S003	Druckserver	Vertraulichkeit:	
		Integrität:	
		Verfügbarkeit:	
S007	Virtualisierungs-server	Vertraulichkeit: **hoch**	***Maximumprinzip:*** Der Domänencontroller beinhaltet das Active Directory und damit die Anmeldeinformationen aller Mitarbeiter.
		Integrität: **hoch**	***Maximumprinzip:*** Der Dateiserver verwaltet Dateien, deren Korrektheit für den Geschäftsbetrieb sichergestellt sein muss.
		Verfügbarkeit: **hoch**	***Kumulationseffekt:*** Sowohl der Domänencontroller als auch der Dateiserver haben jeder hohe Verfügbarkeits-anforderungen. Daraus ergibt sich für den Virtualisierungsserver ein sehr hoher Schutzbedarf. Alle virtualisierten Systeme können aber innerhalb kurzer Zeit auf dem anderen Virtualisierungsserver zur Verfügung gestellt werden. Durch diesen ***Verteilungseffekt*** reduziert sich der Schutzbedarf auf ein nur noch hohes Niveau.

Erklären Sie das Maximumprinzip:

Erklären Sie den Kumulationseffekt:

Erklären Sie den Verteilungseffekt:

In der Tabelle werden das Maximumprinzip und Kumulations- und Verteilungseffekte angewandt. Ergänzen Sie bei *Domänencontroller*, *Dateiserver* und *Druckserver* die Schutzbedarfskategorien (*normal, hoch, sehr hoch*), so dass dies alles zusammenpasst.

IT-Technik - Ein Managementsystem für die Informationssicherheit S. 8

A

Aufgabe: Bei der GAB GmbH ist die Einführung des ISMS schon weit fortgeschritten. Sie und Ihr Team sind sehr aufmerksam und achten auf mögliche Probleme. Insbesondere möchten Sie den häufigsten Fehler vermeiden, der bei der Umsetzung eines ISMS passieren kann. Dieser ist in diesem Video (www.youtube.com/watch?v=MmHO4apXCW8) beschrieben.

a) Nennen Sie den Fehler.

b) Machen Sie einige Vorschläge, wie dieser Fehler vermieden werden kann.

6 Praxis - Datenträger verschlüsseln

Verschlüsselung tragbarer IT-Systeme und Datenträger

A

Informieren

1.) Das ISMS-Team der GAB GmbH hat auf Basis des IT-Grundschutz-Bausteins "INF.9 Mobiler Arbeitsplatz" eine "Sicherheitsrichtlinie für mobile Arbeitsplätze" erstellt. Welche Zielsetzung wird mit dem IT-Grundschutz-Baustein "INF.9 Mobiler Arbeitsplatz" verfolgt?

2.) Betrachten Sie im IT-Grundschutz-Baustein INF.9 den Punkt "*2 Gefährdungslage*".
Einige Unterpunkte beschreiben die Verletzung des Schutzziels "Vertraulichkeit".
Geben Sie Nummer und Bezeichnung dieser Unterpunkte an.

3.) Warum wird im Unterpunkt INF.9.A9 der Standardanforderungen dieses IT-Grundschutz-Bausteins die "*Verschlüsselung tragbarer IT-Systeme und Datenträger*" vorgeschlagen?

Planen

4.) In der "*Sicherheitsrichtlinie für mobile Arbeitsplätze*" wird bei der GAB GmbH auch die Verschlüsselung der Notebook-Festplatten der Außendienstmitarbeiter gefordert. Ebenfalls müssen alle USB-Datenträgern die Firmen-Daten enthalten verschlüsselt werden.
Sie als MitarbeiterIn der Firma JackSEC GmbH werden vom ISB der GAB GmbH beauftragt, mit Ihrem Team mehrere praktisch umsetzbare Vorschläge dazu zu machen, wie Festplatten und USB-Datenträger sicher verschlüsselt werden können.
Hinweis: Sollten Probleme auftreten, wird Sie Ihr Senior Analyst (Lehrkraft) unterstützen.

5.) Sie stellen Ihre ausgearbeiteten Vorschläge dem ISB des GAB ISMS-Teams (Lehrkraft) kurz vor und entscheiden gemeinsam mit dem ISB, welchen Vorschlag Sie mit Ihrem Team umsetzen werden.

Ausführen und kontrollieren

6.) Setzen Sie mit Ihrem Team den ausgewählten Vorschlag praktisch um und demonstrieren Sie dem ISB (Lehrkraft) das Ergebnis Ihrer Arbeit. Ihr Vorgehen haben Sie in Form eines Kochrezepts dokumentiert, so dass die Außendienstmitarbeiter der GAB Festplatten und USB-Datenträger selbst verschlüsseln können. Dieses Dokument haben Sie auf die zur Verfügung gestellte Dateiablage hochgeladen.

Bewerten

7.) In einem kurzen Feedback-Gespräch diskutieren Sie Lösungen, Schwierigkeiten und weitergehende Möglichkeiten, diese Aufgabe in Zukunft effektiver lösen zu können.

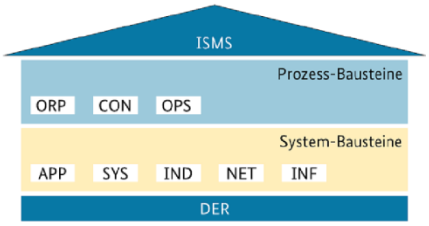
7 Anhang

7.1 Info-Text zum IT-Grundschutz und zu ISMS

Der IT-Grundschutz ist eine umfangreiche Dokumentensammlung, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben wird. Das Werk soll Behörden und Unternehmen ein Verfahren bieten, ihre Informationen und digitalen Systeme zu schützen. Der IT-Grundschutz wird laufend aktualisiert, um auf neue Techniken und neue Bedrohungen reagieren zu können.

Elemente des IT-Grundschutz
Der IT-Grundschutz besteht aus mehreren Dokumenten. In den **vier BSI-Standards** (200-1, 200-2, 200-3 und 100-4) wird das Verfahren erläutert, wie der IT-Grundschutz anzuwenden ist.
Das **IT-Grundschutz-Kompendium** enthält die konkreten Sicherheitsanforderungen und Umsetzungshinweise zum sicheren Umgang mit Informationen in unterschiedlichen Einsatzumgebungen.
Mit dem IT-Grundschutz-Kompendium kann folgende Frage beantwortet werden:
Welche Infrastruktur in meiner Institution ist auf welche Art gefährdet und wie kann ich sie schützen?

IT-Grundschutz-Kompendium
Das IT-Grundschutz-Kompendium enthält die sog. *Bausteine*, die alle Bereiche der Informationssicherheit abdecken (z.B. Anwendungen, Systeme, Kommunikationsverbindungen und Räume).

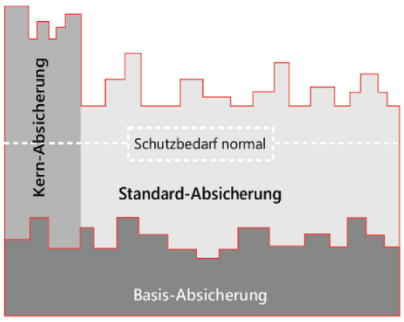


Um die Auswahl zu erleichtern, sind die Bausteine im IT-Grundschutz-Kompendium zunächst in prozess- und systemorientierte Bausteine aufgeteilt und diese jeweils in einzelne Baustein-Gruppen untergliedert. (ISMS, ORP, ... , INF, DER). Jede Gruppe deckt einen Teilbereich der Informationssicherheit ab.

Schichtenmodell der IT-Grundschutz-Bausteine

IT-Grundschutz-Bausteine
Um die Anwendung der Bausteine zu vereinfachen, sind diese immer gleich aufgebaut:
- kurze Beschreibung des Themengebiets und Überblick über die Gefährdungen mit Beispelen
- konkrete Sicherheitsanforderungen, abhängig vom Schutzbedarf (Basis, Standard, erhöhter SB)
- genaue beschriebene Sicherheitsmaßnahmen, wie diese Anforderungen erfüllt werden können

Basis-, Kern- und Standardabsicherung
Das IT-Grundschutz-Verfahren sieht drei Varianten vor: Basis-, Kern- und Standardabsicherung



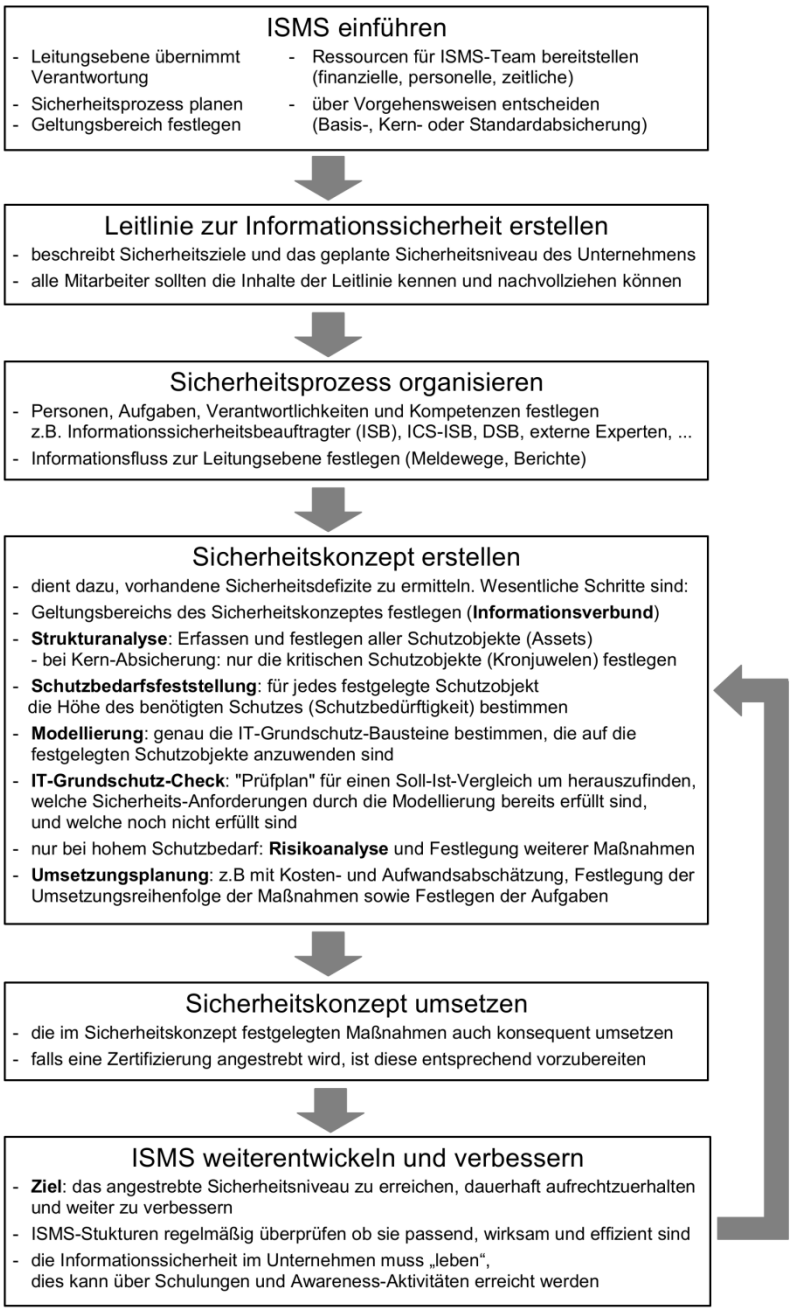
Die **Basisabsicherung** sorgt für eine grundlegende Erst-Absicherung und soll schnell die größten Risiken senken, um dann eine gründlichere Absicherung darauf aufzubauen. Sie ist für kleinere Institutionen gedacht, die noch am Anfang ihres Sicherheitsprozesses stehen.

Die **Kernabsicherung** konzentriert sich zunächst auf einen kleinen, aber sehr wichtigen Teil eines Unternehmens (*Kronjuwelen*) und sichert diese Schutzobjekte schon sofort gründlich ab, bevor später der Schutz auf andere Unternehmensbereiche ausgedehnt wird.

Die Basis- und Kern-Absicherung sind mögliche Einstiegsvarianten mit dem Ziel, mittelfristig ein vollständiges Sicherheitskonzept gemäß der Standard-Absicherung zu erstellen und umzusetzen.

Die **Standard-Absicherung** ist die empfohlene IT-Grundschutz-Vorgehensweise. Sie hat eine angemessene und ausreichende Absicherung für alle Prozesse und Bereiche des Unternehmens mit normalem Schutzbedarf als Ziel. Durch eine geeignete Umsetzung wird ein Sicherheitsniveau erreicht, das angemessen ist und ausreicht, um geschäftsrelevante Informationen zu schützen.

Die Phasen des Sicherheitsprozesses



7.2 Beispiel: Informationssicherheitsleitlinie

Unternehmen und Geschäftszweck der Qualsoft GmbH
Unser Unternehmen ist ein innovativer Dienstleister bei der Entwicklung kundenspezifischer Software.

Unser Unternehmen ist gegliedert in Verwaltung, Marketing/Vertrieb und Software-Entwicklung. Letztere ist auch für den Betrieb unserer IT verantwortlich.

Zurzeit ist Wiesbaden unser zentraler und einziger Standort.

Geltungs- und Anwendungsbereich
Der Wettbewerb verlangt neben der Produktion und Lieferung qualitativ hochwertiger Software auch den Nachweis der Qualität und Sicherheit interner Prozesse. Die vorliegende Informationssicherheits-leitlinie adressiert dieses Erfordernis im Hinblick auf die Sicherheit der Informationsverarbeitung innerhalb unseres Unternehmens. Sie gilt somit für das gesamte Unternehmen.

Anforderungen, Risiken und Ziele
Das Vertrauen unserer Kunden und letztlich unser Geschäftserfolg beruhen darauf, dass wir insbesondere

- die gesetzlichen Vorgaben und hier nicht zuletzt die Datenschutzgesetze einhalten,
- unsere Betriebsgeheimnisse schützen,
- die Vertraulichkeit der Daten unserer Kunden wahren,
- unsere Projekte und Dienstleistungen in der geplanten bzw. zugesicherten Zeit abwickeln,
- integere Produkte (Software) sicher ausliefern und archivieren.

Vor diesem Hintergrund ist der Geschäftserfolg unseres Unternehmens davon abhängig, dass wir bestehende Risiken für die genannten Ziele erkennen, durch geeignete Maßnahmen vermeiden bzw. mindern und Restrisiken geeignet behandeln.

Zu den Risiken zählen die unvollständige bzw. nicht korrekte Einhaltung von gesetzlichen Vorgaben, die unbefugte und ggf. unbemerkte Weitergabe von Betriebsgeheimnissen, die Verletzung von Vorgaben unserer Kunden aufgrund von Systemausfall, Datenverlust, unbefugter Preisgabe von Informationen.

Bedeutung der Sicherheit
Vor dem Hintergrund der externen und internen Anforderungen, vor allem aber den Sicherheitsan-forderungen unserer Kunden muss Informationssicherheit ein integraler Bestandteil unserer Unternehmenskultur sein.
Jeder Mitarbeiter / jede Mitarbeiterin muss sich der Notwendigkeit der Informationssicherheit bewusst sein und die grundsätzlichen Auswirkungen von Risiken auf den Geschäftserfolg kennen.

Grundsätzliche Regelungen

1. Die Leitung hat zur Umsetzung der Sicherheitsziele eine Stabsfunktion "Informationssicherheit" eingerichtet und dieser die Aufgaben übertragen, einheitliche Vorgaben für den Sicherheits-prozess zu erstellen, für ausreichende Sensibilisierung aller Mitarbeiter/innen zu sorgen, sowie die Einhaltung der Sicherheitsrichtlinien angemessen zu überprüfen bzw. überprüfen zu lassen.
2. Alle Organisationseinheiten wirken jeweils durch einen Vertreter / eine Vertreterin im Sicherheits-forum mit, in dem die wesentlichen Richtlinien und Arbeiten koordiniert werden. Die Leitung dieses Sicherheitsforums obliegt der Stabsfunktion "Informationssicherheit".
   Insbesondere wird im Sicherheitsforum ein Gesamtsicherheitskonzept erarbeitet und der Leitung zur Genehmigung vorgelegt.

3. Nach Maßgabe dieser Leitlinie ist zunächst jede Organisationseinheit unseres Unternehmens für die Sicherheit der eigenen Daten und deren Verarbeitung verantwortlich ("Informationseigner"). Im Rahmen dieser Verantwortung wird jede Organisationseinheit eine Aufstellung ihrer Assets (Daten, Systeme und Prozesse) anfertigen, eine Risikoanalyse und -bewertung nach einheitlichem Muster durchführen und in regelmäßigen Abständen sowie nach gravierenden Änderungen aktualisieren.
4. Dort, wo eine Klassifizierung von Informationen und verarbeitender Systeme erforderlich ist, wird in ergänzenden Richtlinien der Umgang mit solchen Informationen und Systemen separat geregelt.
5. Zur Wahrung der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität (soweit anwendbar) von Daten und Systemen sind auf der Basis der Risikoeinschätzungen geeignete Maßnahmen in einem Sicherheitskonzept darzustellen und geeignet umzusetzen.
6. Durch geeignete technische, organisatorische und infrastrukturelle Maßnahmen ist der Zugang zu sensiblen Systemen, zu Sicherheitszonen und kritischen Infrastruktureinrichtungen sowie der Zugriff zu kritischen Informationen und Anwendungen zu kontrollieren und nur für Befugte zu ermöglichen. Zutritts- und Zugriffsberechtigungen werden nur nach formalisierten Antrags-verfahren bei Bedarf vergeben und entzogen. Dabei sind die Informationseigner einzubinden.
7. Die Mitarbeiter/innen unseres Unternehmens erhalten bei Bedarf für den jeweiligen Arbeitsplatz spezielle Sicherheitsregeln, die insbesondere eine Meldepflicht bei Sicherheitsvorkommnissen beinhalten.
8. Vor dem Hintergrund der oben genannten Sicherheitsziele sind angemessene Nachweise über die Einhaltung aller Sicherheitsmaßnahmen zu erbringen und zu archivieren.
9. Die die Informationssicherheit betreffenden Unterlagen, Berichte, etc. sind einem geordneten Dokumentmanagement zu unterwerfen, in dem die Erstellung, Freigabe, Verteilung, Archivierung geregelt sind.
10. Der Stabsfunktion "Informationssicherheit" wird aufgegeben, der Leitung quartalsweise Berichte über die Sicherheitslage des Unternehmens zuzuleiten.

Verpflichtungen

Die Leitung wird die Sicherheitsorganisation und den Sicherheitsprozess aktiv unterstützen. Unser Unternehmen wird sich an dem Standard ISO 27001 orientieren und die Management-Elemente dieses Standards realisieren. Diese umfassen die Durchführung von regelmäßigen internen Audits, eine geeignete Dokumentenlenkung, die Managementbewertung und die Anwendung des Modells der kontinuierlichen Verbesserung (PDCA).

Jeder Mitarbeiter / jede Mitarbeiterin ist verpflichtet, die allgemeinen sowie die für den jeweiligen Arbeitsplatz geltenden Sicherheitsrichtlinien zu beachten und einzuhalten.

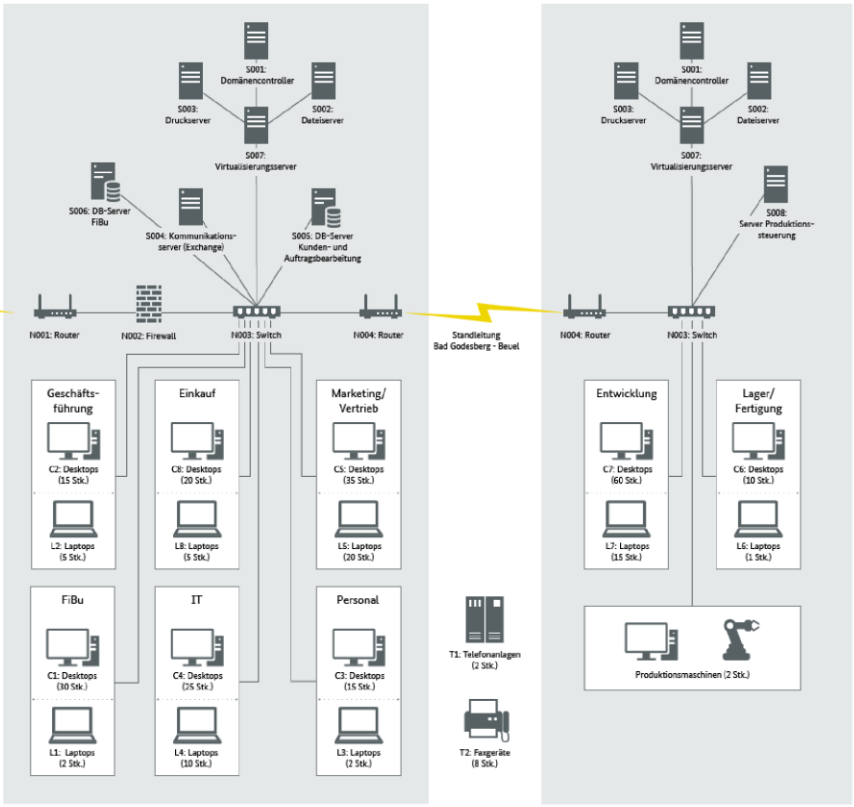
Die vorliegende Sicherheitsleitlinie ist grundsätzlich nur unternehmensintern zu halten.
Bei Bedarf wird die Leitung darüber befinden, ob sie an Dritte (z.B. Kunden, Vertragspartner, Lieferanten) weitergegeben werden kann.

Diese Sicherheitsleitlinie tritt am 01.01.2020 in Kraft.

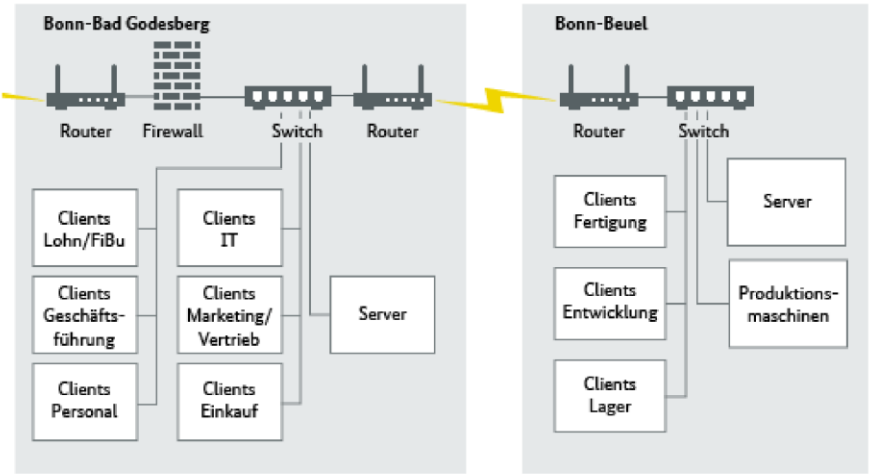
Wiesbaden, 01.01.2020

Dr Na

7.3 Beispiel: Detaillierter und bereinigter Netzplan



detaillierter Netzplan



bereinigter Netzplan

8 Feedback

A

Mit diesem Bogen können Sie Ihren eigenen Lernfortschritt beurteilen.
Bitte machen Sie 1 Kreuz pro Zeile!

	25%	50%	75%	100%
Wieviele theoretische Aufgaben haben Sie bearbeitet? Schätzung!				
Wieviele praktische Aufgaben haben Sie bearbeitet? Schätzung!				

ich stimme	gar nicht zu	eher nicht zu	zu	völlig zu
Hat der Unterricht Ihre Selbstständigkeit gefördert?				
Ich war gefordert, selbstständig Informationen zu beschaffen und auszuwerten.				
Ich war gefordert, eigene Entscheidungen zu treffen.				
Ich habe Lösungsmöglichkeiten entwickelt und in praktisches Handeln umgesetzt.				
Hat der Unterricht Ihre Teamfähigkeit gestärkt?				
Ich war gefordert, partnerschaftlich mit anderen zusammenzuarbeiten.				
Ich musste auch mal unangenehme Arbeiten übernehmen.				
Ich war gefordert, Vereinbarungen einzuhalten.				
Hat der Unterricht die Kommunikationsfähigkeit gefördert?				
Ich war gefordert, schwierige Sachverhalte angemessen und klar darzustellen.				
Ich musste mich mit unterschiedlichen Meinungen auseinandersetzen.				
Ich war gefordert, Kritik konstruktiv zu formulieren.				
Hat der Unterricht die Methodenkompetenz gefördert?				
Ich war gefordert, Ergebnisse zu strukturieren und zu präsentieren.				
Ich musste schwierige Problemstellungen in einzelne zur Lösung notwendige Arbeitsschritte zerlegen.				
Hat der Unterricht Ihr Verantwortungsbewusstsein gefördert?				
Ich musste mich an gemeinsame Vereinbarungen halten.				
Ich war gefordert, die übernommenen Aufgaben zuverlässig zu erledigen und zu Ende zu führen.				
Hat der Unterricht Ihr Wissen erweitert?				
Ich bin mit den theoretischen Aufgaben gut zurecht gekommen.				
Ich bin mit den praktischen Aufgaben gut zurecht gekommen.				

nach: http://bk-suedstadt.de/fileadmin/dateien/01_Bildungsgaenge/02_Berufsschule/05_EH/eva_ls_schueler.htm

9 Fragen

- die folgenden Fragen stammen aus dem Fragenpool. Sie zeigen den Umfang und die Intensität der Unterrichtsinhalte und dienen zur Vorbereitung auf Leistungskontrollen und Abschlussprüfung
- *manchmal* haben schwierige Fragen ein Sternchen "*", schwierigere zwei "**"
- es werden KEINE Lösungen bereitgestellt, Ziel ist es, dass SIE die Lösungen selbst erstellen!
- Nachfragen, Anmerkungen, Lob und Kritik können Sie an Ihre Lehrkraft richten

1.) Nennen Sie mindestens 5 Fälle bei denen die Informationssicherheit bedroht wird.

2.) Erläutern Sie an Beispielen, welche Schutzziele der Informationssicherheit bei mobilen Arbeitsplätzen bedroht sind.

3.) Was ist ein ISMS und warum ist es vor allem in größeren Firmen nötig?

4.) Wozu dient eine Informationssicherheitsleitlinie (Security Policy)?

5.) Welche Aufgaben hat der Informationssicherheitsbeauftragte (ISB)?

6.) Nennen Sie mindestens 3 Punkte, die Sie in eine "Sicherheitsrichtlinie für mobile Arbeitsplätze" aufnehmen würden.

7.) Was wird unter dem BSI IT-Grundschutz-Verfahren (IT-Grundschutz-Methode) verstanden?

8.) Der BSI-Grundschutz und die ISO 27001 sind Verfahrensweisen, um ein ISMS umzusetzen. Welches dieser Verfahren macht genauere Angaben über notwendige IT-Schutzmaßnamen?

9.) Aus welchen Bestandteile besteht der BSI-Grundschutz?

10.) Zeigen Sie an einer grafischen Darstellung die einzelnen ISMS-Schritte/Phasen.

11.) Was ist ein "BSI-Grundschutz Baustein"?

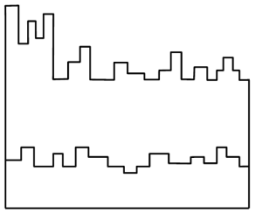
12.) Ein Mitarbeiter behauptet, dass das IT-Grundschutz-Kompendium eine Sammlung von "Kochrezepten" ist. Was könnte er damit gemeint haben?

13.) Beschreiben Sie kurz die drei Varianten der Absicherung nach der BSI IT-Grundschutz-Verfahren.

14.) Im Rahmen der Kernabsicherung wird von "Kronjuwelen" gesprochen. Was heißt das?

15.) Worin unterscheiden sich die "Kronjuwelen" von den anderen Assets?

16.) Die folgende Grafik taucht häufig auf, wenn es um das Thema BSI IT-Grundschutz geht.



a) Zeigen Sie daran die drei Absicherungs-Varianten.
b) Skizzieren Sie die Linie für den normalen Schutzbedarf hinein.
c) Markieren Sie die Assets der Kronjuwelen.

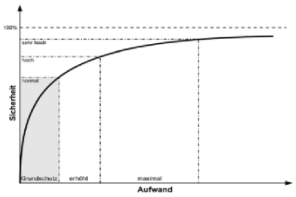
17.) Wozu dient das "Sicherheitskonzept"?

18.) Bei der Strukturanalyse werden alle Schutzobjekte aus den Bereichen Anwendungen (A), Geschäftsprozesse (G), IT-Systeme (I), Netzplan (N), Räume (R) erfasst und festgelegt. Geben Sie die Buchstaben der Bereiche in der Reihenfolge an, wie der IT-Grundschutz die Erfassung empfiehlt.

19.) Erläutern Sie den Begriff "Schutzbedarf".

20.) Was ist eine "Schutzbedarfsfeststellung"?

21.) Erläutern Sie die nebenstehende Grafik.



ISMS

Managementsystem für Informationssicherheit

Agenda

- ISMS
- ISO 27000 und BSI IT-Grundschutz
- BSI IT-Grundschutz
- Informationssicherheit - Aufwand und Nutzen
- Phasen des Informationssicherheitsprozesses
- Strukturanalyse
- Schutzbedarf

Begriffs-Wirrwarr

Wo 09.09.2020

ISMS - *Information Security Management System*

⇒ „Managementsystem für Informationssicherheit“

⇒ Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft
- zu definieren,
- zu steuern,
- zu kontrollieren,
- aufrechtzuerhalten
- und fortlaufend zu verbessern.

⇒ **Frage**: Wie wird ein ISMS installiert?

⇒ Standards: ISO 27001 und BSI-Standard 200-1

- *Betreiber Kritischer Infrastrukturen (KRITIS) benötigen ein ISMS nach ISO 27001*
- *ISMS erhöhen wirksam die Informationssicherheit: wegen der systematischen Analyse-Prozesse und wegen der Stärkung des Sicherheitsbewusstseins der Mitarbeiter*

Vergleich: ISO 27000 und BSI IT-Grundschutz

Kriterien	ISO 27000-Reihe	BSI IT-Grundschutz
Herausgeber	ISO	BSI
Zielgruppe	Organisationen jeder Größenordnung	Organisationen jeder Größenordnung und öffentliche Verwaltung
Dokumentation	ca. 400 Seiten	ca. 5.000 Seiten
Detaillierung	minimalistisch, wenig konkret	maximal detailliert, mit regelmäßiger Überarbeitung
Aufbau	Maßnahmenempfehlungen	umfassende Bausteine mit Gefährdungen und Maßnahmen
Umfang des Maßnahmenkataloges	ca. 150 Maßnahmen	ca. 1.100 Maßnahmen
Risikoanalyse	grundsätzlich	enthalten (nur für höheren Schutzbedarf nötig)
Umsetzung	allgemeingültig formulierte Maßnahmen umsetzen	Auswahl konkret formulierter Maßnahmen umsetzen
Zertifizierung	ISO-Zertifizierung weltweit anerkannt	ISO-Zertifizierung nach IT-Grundschutz

IT-Grundschutz

⇒ vom BSI entwickeltes Verfahren zum Umsetzen eines ISMS

⇒ **Ziel:** mit Standard-Sicherheitsmaßnahmen ein akzeptables Sicherheitsniveau erreichen

⇒ eine aufwändige Sicherheits- und Risikoanalyse entfällt, da zunächst mit pauschalisierten Gefährdungen gearbeitet wird

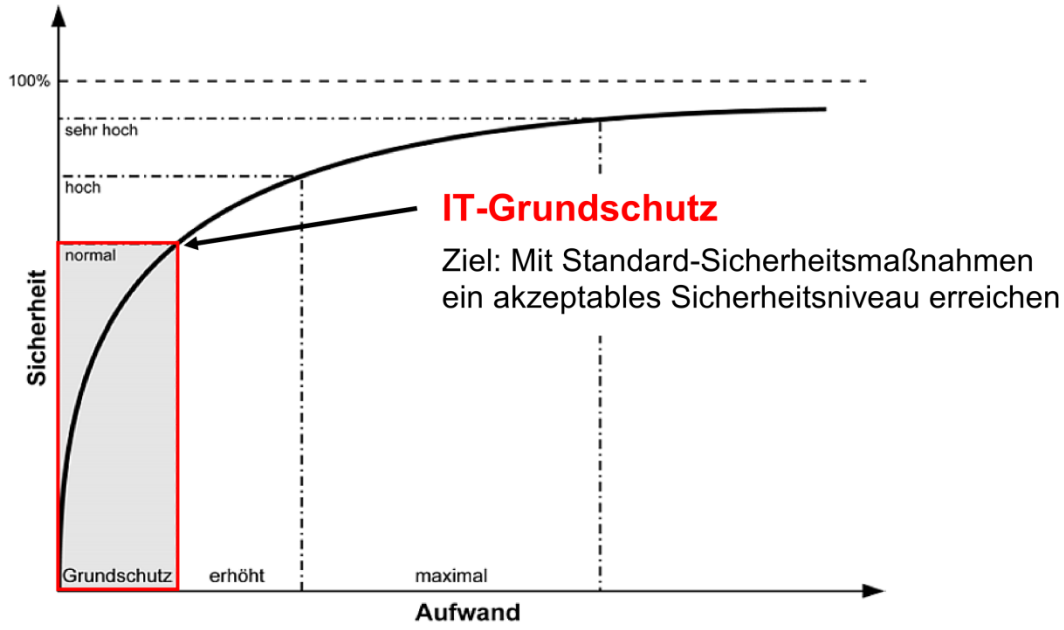
⇒ mit den IT-Grundschutz-Kompendium erhält man „Kochrezepte“ für ein normales Sicherheitsniveau

⇒ so ist es auch „Laien“ möglich, die notwendigen Maßnahmen festzustellen und dann zusammen mit Fachleuten umzusetzen

⇒ der IT-Grundschutz ist im BSI-Standard 200-2 festgelegt

Informationssicherheit - Aufwand und Nutzen

(Aufwandskurve)



Bestandteile des IT-Grundschutz

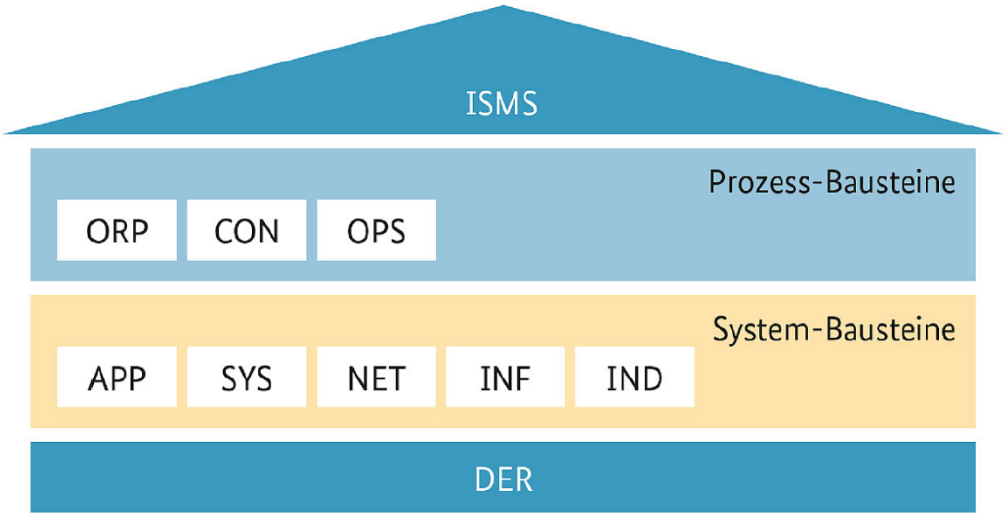
⇒ BSI-Standards zum IT-Grundschutz
- Empfehlungen für den organisatorischen Rahmen
- systematische Methoden zur Entwicklung von Sicherheitskonzepten

- BSI-Standard 200-1: *Managementsysteme für Informationssicherheit (ISMS)*
- BSI-Standard 200-2: *IT-Grundschutz-Methodik*
- BSI-Standard 200-3: *Risikomanagement*
- BSI-Standard 100-4: *Notfallmanagement*

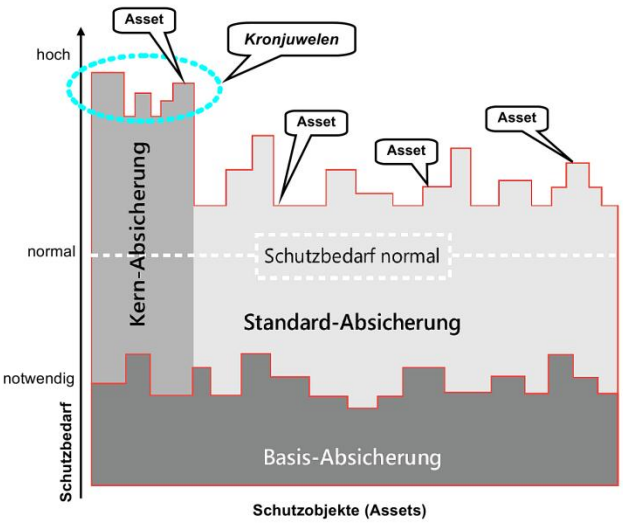
⇒ IT-Grundschutz-Kompendium
- hilft, die in den BSI-Standards formulierten Empfehlungen umzusetzen
- enthält Standard-Sicherheitsmaßnahmen für typische Geschäftsprozesse, Anwendungen und IT-Systeme

weitere Informationen im Online-Kurs IT-Grundschutz

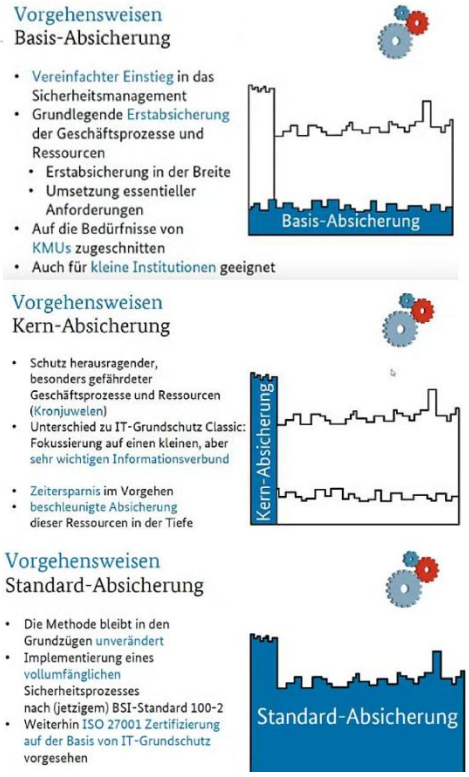
Schichten-Modell IT-Grundschutz



Varianten der Absicherung



aus: www.youtube.com/watch?v=8bBFgKbQPUI
anschaulicher Vergleich bei 12:30



ISMS - Managementsystem für Informationssicherheit

Phasen des Informationssicherheitsprozesses

ISMS einführen

- Leitungsebene übernimmt Verantwortung
- Sicherheitsprozess planen
- Geltungsbereich festlegen
- Ressourcen für ISMS-Team bereitstellen (finanzielle, personelle, Zeit)
- über die Vorgehensweise entscheiden (Basis-, Kern- oder Standardabsicherung)

↓

Leitlinie zur Informationssicherheit erstellen

↓

Sicherheitsprozess organisieren

↓

Sicherheitskonzept erstellen

↓

Sicherheitskonzept umsetzen

↓

ISMS weiterentwickeln und verbessern

↺

IT-Sicherheitsmanagement

Planungs- und Lenkungsaufgabe,
die erforderlich ist,
um einen durchdachten und
wirksamen Prozess zur Herstellung
von Informationssicherheit aufzubauen
und kontinuierlich umzusetzen.

Informationssicherheit ist **Chefsache**!

Informationssicherheit ist kein
statischer Zustand, sondern ein
ständiger Prozess!

ISMS - Managementsystem für Informationssicherheit

Informationssicherheits-Leitlinie

⇒ beschreibt Sicherheitsziele

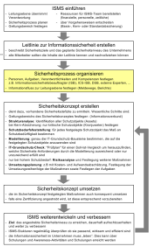
⇒ und das geplante Sicherheitsniveau des Unternehmens

⇒ alle Mitarbeiter sollten die Inhalte der Leitlinie kennen

⇒ **und** nachvollziehen können

siehe Beispiel dazu in der Unterlage!

ISMS - Managementsystem für Informationssicherheit

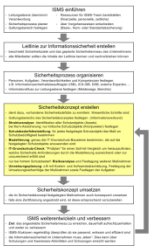


Sicherheitsprozess organisieren

⇒ Personen, Aufgaben, Verantwortlichkeiten und Kompetenzen festlegen, z.B.
- Informationssicherheitsbeauftragter (ISB, CISO)
- ICS-Informationssicherheitsbeauftragte (ICS-ISB)
  industrielle Steuerungen (*Industrial Control Systems*, ICS)
- Datenschutzbeauftragter (DSB)
- externe Experten, usw.

⇒ Informationsfluss zur Leitungsebene festlegen
- Meldewege
- Berichte

ISMS - Managementsystem für Informationssicherheit



Sicherheitskonzept erstellen

Das Sicherheitskonzept dient dazu, vorhandene IT-Sicherheitsdefizite zu ermitteln!

Wesentliche Schritte sind:

- Geltungsbereichs des Sicherheitskonzeptes festlegen (**Informationsverbund**)
- **Strukturanalyse**: Erfassen und festlegen aller Schutzobjekte (*Assets*)
  bei *Kern-Absicherung*: nur die kritischen Schutzobjekte (*Kronjuwelen*) festlegen
- **Schutzbedarfsfeststellung**: für jedes festgelegte Schutzobjekt
  die Höhe des benötigten Schutzes (Schutzbedürftigkeit) bestimmen
- **Modellierung**: genau die IT-Grundschutz-Bausteine bestimmen, die auf die festgelegten Schutzobjekte anzuwenden sind
- **IT-Grundschutz-Check**: "Prüfplan" für einen Soll-Ist-Vergleich um herauszufinden, welche Sicherheits-Anforderungen durch die Modellierung bereits erfüllt sind, und welche noch nicht erfüllt sind
- nur bei hohem Schutzbedarf: **Risikoanalyse** und Festlegung weiterer Maßnahmen
- **Umsetzungsplanung**: z.B mit Kosten- und Aufwandsabschätzung, Festlegung der Umsetzungsreihenfolge der Maßnahmen sowie Festlegen der Aufgaben

ISMS - Managementsystem für Informationssicherheit

Sicherheitskonzept umsetzen

⇒ die im Sicherheitskonzept festgelegten Maßnahmen auch konsequent umsetzen

⇒ falls eine Zertifizierung angestrebt wird, ist diese hier entsprechend vorzubereiten

ISMS - Managementsystem für Informationssicherheit

ISMS weiterentwickeln und verbessern

Ziel: das angestrebte Sicherheitsniveau
- zu erreichen,
- dauerhaft aufrechtzuerhalten
- und weiter zu verbessern

⇒ ISMS-Stukturen regelmäßig überprüfen,
- ob sie passend,
- wirksam
- und effizient sind

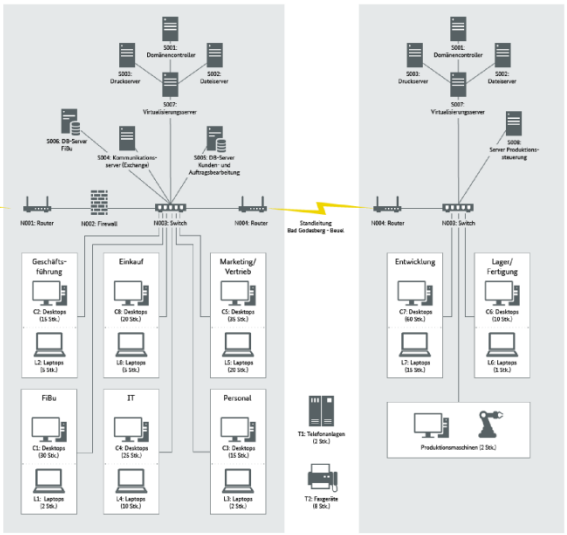
⇒ die Informationssicherheit im Unternehmen muss „leben“.
- dies kann über Schulungen und Awareness-Aktivitäten erreicht werden

Strukturanalyse: Schutzobjekte erfassen und festlegen

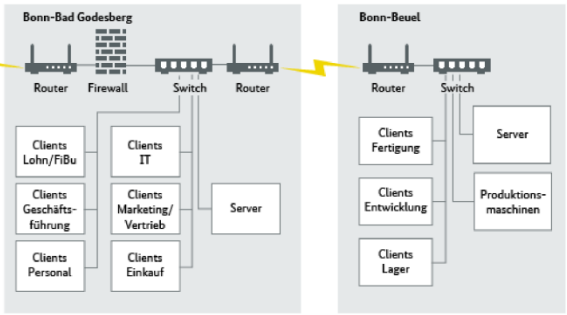
Bezeichnung	Beschreibung des Systems	Schutzziel und Schutzbedarf	Begründung
S007	Virtualisierungsserver	Vertraulichkeit: **hoch**	*Maximumprinzip:* Der Domain Controller beinhaltet das Active Directory und damit die Anmeldeinformationen aller Mitarbeiter.
		Integrität: **hoch**	*Maximumprinzip:* Der Dateiserver verwaltet Dateien, deren Korrektheit für den Geschäftsbetrieb sichergestellt sein muss.
		Verfügbarkeit: **hoch**	*Kumulationseffekt:* Sowohl der Domain Controller als auch der Dateiserver haben jeder hohe Verfügbarkeitsanforderungen. Daraus ergibt sich für den Virtualisierungsserver ein sehr hoher Schutzbedarf. Alle virtualisierten Systeme können aber innerhalb kurzer Zeit auf dem anderen Virtualisierungsserver zur Verfügung gestellt werden. Durch diesen *Verteilungseffekt* reduziert sich der Schutzbedarf auf ein nur noch hohes Niveau.
N001	Internet-Router	Vertraulichkeit: **hoch**	Es werden auch vertrauliche Informationen über die Internet-Anbindung übertragen, wenn ein Kunde oder Geschäftspartner eine verschlüsselte Kommunikation nicht unterstützt.
		Integrität: **normal**	Fehlerhafte Daten können in der Regel leicht erkannt werden.
		Verfügbarkeit: **normal**	Ein Ausfall der Internet-Anbindung kann für 24 Stunden toleriert werden.

Strukturanalyse: Bereinigen eine Netzplans

(Strukturanalyse == alle Schutzobjekte erfassen und festlegen)



detaillierter Netzplan



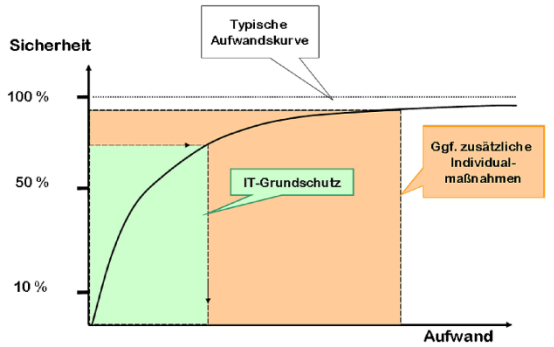
bereinigter Netzplan

bereinigen: aus einem detailliertem Netzplan durch Zusammenfassen und Gruppieren den Umfang auf das tatsächlich Benötigte beschränken

Schutzbedarf

⇒ Höhe des benötigten Schutzes, um Schäden abzuwenden
⇒ der Schutzbedarf orientiert sich am Ausmaß des drohenden Schadens
⇒ Schutzbedarf der Anwendungen, IT-Systeme, Kommunikationsverbindungen und IT-Räume
⇒ Institutionsweit Schutzbedarfskategorien anhand von Schadensszenarien festlegen

Schutzbedarfs-Kategorie	**Schadens-auswirkungen**	**Beeinträchtigung** der Aufgabenerfüllung	**maximale Ausfallzeit**	**finanzieller Schaden** z.B. bezogen auf den Monatsumsatz
normal	begrenzt und überschaubar	tolerabel	mehrere Tage	< 1 %
hoch	beträchtlich	nicht tolerabel	einzelne Tage	1 - 10 %
sehr hoch	katastrophal existenzbedrohend	existenzbedrohend	Stunden	> 10 %



Aufwandskurve für IT-Grundschutz (aus: Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen (KMU))

BSI Begriffs-Wirrwarr

Alle Begriffe in einer Zeile haben eine sehr ähnliche oder die selbe Bedeutung!

Informationssicherheit, IT-Sicherheit, Datensicherheit, Cyber-Sicherheit, *safety, security*

IT-Grundschutz-Verfahren, IT-Grundschutz-Methodik, IT-Grundschutz-Methode

IT-Grundschutz-Kompendium, Grundschutz-Kataloge, Grundschutz-Handbuch

Institution, Firma, Unternehmen, Behörde

Sicherheitskonzept, Sicherheitskonzeption

Informationsverbund, Geltungsbereich

Schutzobjekt, Asset, Zielobjekt, Objekt

Strukturanalyse, Inventur, Werteinventar, Inventar

Schutzziele, Grundwerte, (Vertraulichkeit, Integrität, Verfügbarkeit)

Schutzbedarf, Schutzbedürftigkeit, Schutzbedarfskategorie

Schutzbedarfsfeststellung, Schutzbedarfsanalyse

Modellierung, Auswahl der Maßnahmen