Praktikum 1 zur Vorlesung IT-Sicherheit

Thema BSI Grundschutz und Mindeststandards

Der IT-Grundschutz ist die Vorgehensweise des Bundesamts für Sicherheit in der Informationstechnik (BSI) zur strukturieren Einführung von IT-Sicherheitsmanagement und von IT-Sicherheitskonzepten in Institutionen. Die Vorgehensweise wurde 2018 komplett überarbeitet.

In der Vorlesung wurde die Vorgehensweise für Sicherheitskonzepte gemäß IT-Grundschutz kurz erläutert. Dieses Praktikum dient zur Vertiefung der Grundschutz Methodik.

Die Grundschutz Methodik ist beschrieben im IT-Grundschutz-Kompendium des BSI: Webseite des BSI (bsi.bund.de) => Themen: IT-Grundschutz => IT-Grundschutz-Kompendium. Im Praktikum finden Sie die pdf-Version des Kompendiums auf dem Desktop im Ordner *IT-Sicherheit/ITS P1.*

Das Vorgehen für Sicherheitskonzepte umfasst dabei folgende Schritte:

Strukturanalyse	Ist-Aufnahme der zu schützenden Gesamtstruktur
Schutzbedarfsfeststellung	Ermittlung des Schutzbedarfs für die Gesamtstruktur
Modellierung	„Nachbauen“ der Gesamtstruktur mit Grundschutz-Bausteinen (Lego-Prinzip)
IT-Grundschutz-Check	Überprüfung, ob alle Anforderungen aus den Bausteinen der Modellierung umgesetzt sind.
Umsetzungsplanung	Planung der Umsetzung bislang nicht oder nicht ausreichend erfüllter Anforderungen

1. Vorbereitung zu Hause: IT-Grundschutz Kompendium

1.1 Grundlegende Anforderungen an einen geregelten IT-Betrieb

Im Kapitel *Schichtenmodell und Modellierung* werden im Abschnitt *Modellierung* die Bausteine gelistet. Danach gibt es einen Abschnitt *Bearbeitungsreihenfolge der Bausteine*.

Welche Bedeutung haben dabei die Kennzeichnungen R1, R2 und R3?

Recherchieren Sie, welche Bausteine *vorrangig* umzusetzen sind, da sie die Grundlage für einen effektiven Sicherheitsprozess bilden? (es müssten 12 Stück sein)

Kürzel	Name des Bausteins

1.2 Struktur der Grundschutz-Bausteine

Gehen Sie zum Baustein ISMS.1

Machen Sie sich mit dem generellen Aufbau der Bausteine vertraut. Welche standardisierte Gliederung haben die Bausteine?

Abschnitt 1	
Abschnitt 2	
Abschnitt 3	
Abschnitt 4	
Abschnitt 5	

Welche 3 *Arten von Anforderungen* werden in den Bausteinen unterschieden? Wie viele Anforderungen der jeweiligen Art enthält der Baustein ISMS.1

	Anforderungsart	Anzahl
1		
2		
3		

1.3 Einschub: ISO/IEC 27000 Standards

Im Baustein ISMS.1 wird unter „Weiterführende Informationen“ neben den BSI-Verweisen auf zwei weitere Standards verwiesen. Welche sind das?

1	
2	

Einer dieser beiden Standards ist normativ, d.h. soviel wie „eine Norm setzend“. Gemäß dieser Norm können sich Unternehmen zertifizieren lassen. Welcher der beiden Standards ist das?

_____

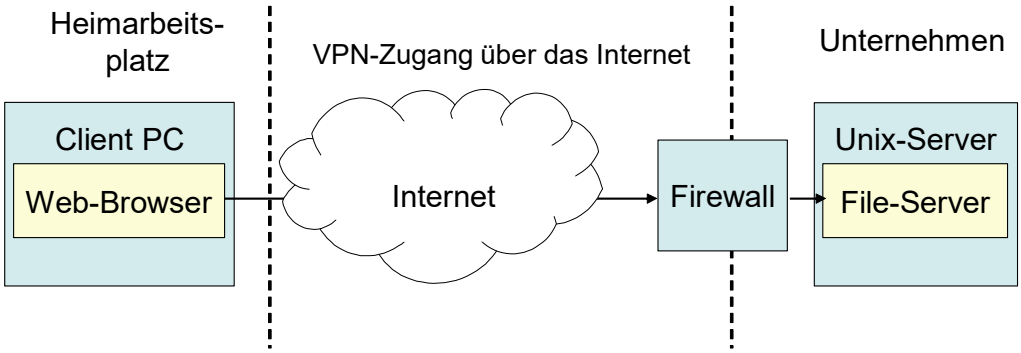
Die Standards gehören zur Reihe der ISO/IEC 27000 Standards.

Recherchieren Sie, welcher Standard der Reihe *Informationssicherheits Risiko Management* behandelt?

Welcher Standard der Reihe listet konkrete Schutzmaßnahmen für die Speicherung *personenbezogener Daten* in *Public Clouds*?

1.4 Ab hier im Praktikumstermin: Modellierung einer gegeben IT-Infrastruktur:

Die zu modellierende IT-Infrastruktur ist in der nachstehenden Abbildung angegeben.



Ein Client-PC greift per Browser vom Heimarbeitsplatz über das Internet auf einen firmeninternen Fileserver zu, der auf einem Unix-Server läuft. Die Firmenanbindung erfolgt per VPN über eine Firewall.

Die Infrastruktur habe einen normalen Schutzbedarf. Anforderungen welcher Arten (=> s. Aufgabe 1.2) sind daher für die Infrastruktur relevant?

Führen Sie eine Modellierung gemäß IT-Grundschutz durch. D. h. ermitteln Sie, welche Grundschutz-Bausteine für die Infrastruktur benötigt werden. (Die in Aufgabe 1.1 ermittelten grundlegenden Bausteine brauchen NICHT wiederholt zu werden.)
Eine Übersicht der Bausteine finden Sie im Kapitel *Schichtenmodell und Modellierung* werden im Abschnitt *Modellierung.* Hilfreich ist auch die auf der Webseite des GS-Kompendiums auffindbare *mindmap – Übersicht über die Bausteinstruktur*.

Bsp.: Für den Client PC wird der Baustein SYS 2.1 Allgemeiner Client verwendet.

Bedenken Sie, dass der PC und der Server eine Räumlichkeit zum Betrieb erfordern. Beachten Sie zusätzlich Frage 5 auf Seite 99 im Grundschutz-Onlinekurs (pdf im Ordner *IT-Sicherheit/ITS P1*).

Tragen Sie die benötigten Bausteine in der nachstehenden Tabelle ein.

Kürzel	Name des Bausteins	Anzahl Anforderungen
SYS 2.1	Allgemeiner Client	27

1.5 Anforderungen und Gefährdungen

Gehen Sie zur *Kreuzreferenztabelle zu elementaren Gefährdungen* des Bausteins SYS.1.1. Hier ist für jede Anforderung angegeben, gegen welche Gefährdungen sie wirkt. Die Tabellen finden Sie in der pdf-Version des Kompendiums.

Dem Schutz vor welchen Gefährdungen dient die Anforderung SYS.1.1.A2?

Welche Anforderungen des Bausteins SYS.1.1 dienen zum Schutz gegen Gefährdung G 0.30?

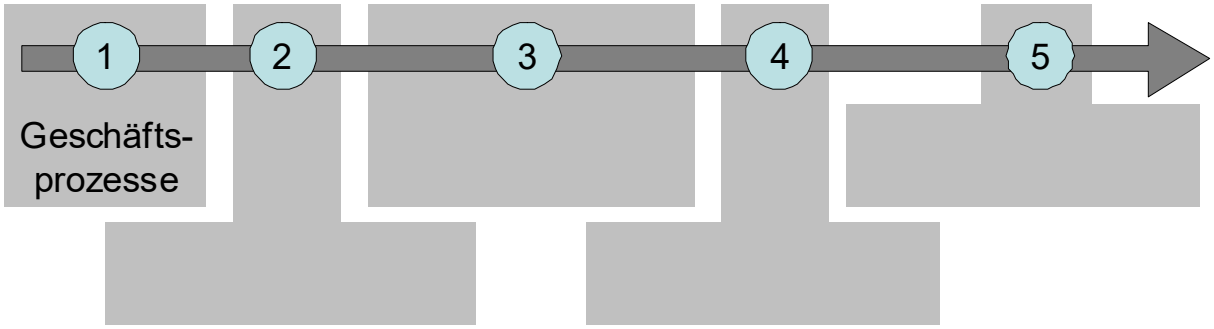
2. Online-Kurs IT-Grundschutz

Neben dem IT-Grundschutz-Kompendium gibt es einen Online-Kurs IT-Grundschutz. Eine pdf-Version finden Sie im Ordner *IT-Sicherheit/ITS P1* und auch frei im Internet. Die pdf-Version dient als Grundlage für die folgenden Aufgaben zu den Lektionen 3, 4, 5, 6 und 8.

Im Folgenden geht es darum, Sie etwas besser mit dem Vorgehen vertraut zu machen.

2.1 Strukturanalyse (Lektion 3)

Im Rahmen der Strukturanalyse erfolgt die Ist-Aufnahme der zu schützenden Gesamtstruktur. Was wird ausgehend von den Geschäftsprozessen erhoben? (bitte in nachstehender Abbildung eintragen, siehe z.B. Lehreinheit 3.3)



Bei vielen der Schritte erfolgt die Dokumentation der Erhebung in tabellarischer Form.

Welche Daten werden dabei in der *Tabelle für die Anwendungen* pro Anwendung dokumentiert? (Lehreinheit 3.4, Beispieltabelle Recplast GmbH)

Die Anwendungen werden den Geschäftsprozessen über eine Kreuzreferenztabelle zugeordnet.

2.2 Schutzbedarfsfeststellung (Lektion 4)

Der Schutzbedarf ist ein Maß für den *Schaden*, der bei Verletzung der Grundwerte Verfügbarkeit, Integrität bzw. Vertraulichkeit entsteht. Der Online-Kurs unterscheidet die Schadenskategorien normal (begrenzt), hoch (beträchtlich) und sehr hoch (katastrophal).

Grundsätzlich vererbt sich der Schutzbedarf von den Geschäftsprozessen über die Anwendungen auf die IT-Systeme. (Lehreinheit 4.3 + 4.4)

Nach welchem Prinzip bemisst sich in der Regel der Schutzbedarf eines IT-Systems, wenn mehrere Anwendungen auf diesem IT-System laufen?

Weshalb kann der Schutzbedarf eines IT-Systems ggf. höher sein, als der Schutzbedarf jeder einzelnen Anwendung, die dass System benötigt? Wie nennt sich der Effekt?

Da Sie Lektion 5: *Modellierung* bereits in Aufgabe 1 geübt haben, gehen wir direkt zur Lektion 6.

2.4 IT-Grundschutz-Check (Lektion 6)

Im Rahmen des IT-Grundschutz-Checks wird geprüft, ob die Anforderungen aus den Grundschutz-Bausteinen, die im Rahmen der Modellierung ermittelt wurden, auch durch geeignete Maßnahmen in der Institution umgesetzt sind.

Welche 4 verschiedenen Erfüllungsgrade kann es dabei für jede Anforderung geben?

Für welchen Erfüllungsgrad sollte eine besondere Begründung dokumentiert werden?

3. Was das BSI sonst noch so macht

3.1 Wofür steht die Abkürzung ICS?

Suchen Sie unter BSI Publikationen nach der Publikation, in der die Top 10 Bedrohungen von ICS zu finden sind. Notieren Sie die ersten 3 der *TOP 10 Bedrohungen* aus dem Dokument.

Bedrohung 1	
Bedrohung 2	
Bedrohung 3	

Notieren Sie zu jeder der 3 Bedrohungen jeweils die erste der aufgelisteten Gegenmaßnahmen:

	Jeweilige Gegenmaßnahme Nr. 1
Bedrohung 1	
Bedrohung 2	
Bedrohung 3	

3.2 Für welche Bereiche hat das BSI Mindeststandards festgelegt?

Geben Sie 4 dieser Bereiche an:

Für wen gelten diese Mindeststandards? Wer hat sich daran zu halten?

Werfen Sie einen Blick in den Mindeststandard zum MDM. Um sich mit Grundfunktionen eines MDM kurz vertraut zu machen, lesen Sie die folgenden Anforderungen und notieren Sie die Inhalte in Stichpunkten.

MDM.04	
MDM.13	
MDM.14	
MDM.26	

4. Gibt es etwas ähnliches wie das BSI auch auf europäischer Ebene?

Wofür steht die Abkürzung ENISA? Was bedeutet die Abkürzung Buchstabe für Buchstabe?

Das BSI veröffentlicht jährlich einen *Jahresbericht zur Lage der IT-Sicherheit* in Deutschland. Wie heißen die entsprechenden Berichte der ENISA?

5. Selbsttest zur IT-Grundschutz Vorgehensweise

Im IT-Grundschutz Online-Kurs gibt es am Ende jeder Lektion Testfragen. Von diesen wurden hier jeweils Fragen ausgewählt, die sich mit begrenztem Sachverstand – ohne zu tief in die Details einzusteigen – beantworten lassen müssten. Versuchen Sie es!

(Natürlich dürfen Sie gerne versuchen, auch die anderen Testfragen zu beantworten. Aber diese erfordern teilweise Detailwissen und setzen ein halbwegs vollständiges Durcharbeiten der jeweiligen Lektion voraus. Das ist innerhalb der Praktikums-Doppelstunde kaum machbar.)

Am Ende des Onlinekurs-Dokuments sind die Lösungen zu den Testfragen angegeben. Versuchen Sie, die Fragen zu beantworten, prüfen Sie Ihre Antworten und überlegen Sie, weshalb die Musterlösungen korrekt und sinnvoll sind.

5.1 Strukturanalyse Testfragen (Lerneinheit 3.8)

Beantworten Sie Aufgaben 1,3 und 5 zur Strukturanalyse.

	a	b	c	d
Aufgabe 1: Richtige Antwort(en)				
Aufgabe 3: Richtige Antwort(en)				
Aufgabe 5: Richtige Antwort(en)				

5.2 Schutzbedarfsfeststellung Testfragen (Lerneinheit 4.8)

Beantworten Sie Aufgaben 1 bis 4 zur Schutzbedarfsfeststellung.

	a	b	c	d
Aufgabe 1: Richtige Antwort(en)				
Aufgabe 2: Richtige Antwort(en)				
Aufgabe 3: Richtige Antwort(en)				
Aufgabe 4: Richtige Antwort(en)				

5.3 Modellierung Testfragen (Lerneinheit 5.6)

Beantworten Sie Aufgaben 1, 4 und 5. (Aufgabe 4 betrifft eigentlich Umsetzungsplanung)

	a	b	c	d
Aufgabe 1: Richtige Antwort(en)				
Aufgabe 4: Richtige Antwort(en)				
Aufgabe 5: Richtige Antwort(en)				

5.4 IT-Grundschutz Check Testfragen (Lerneinheit 6.6)

Beantworten Sie Aufgaben 1 und 6.

	a	b	c	d
Aufgabe 1: Richtige Antwort(en)				
Aufgabe 6: Richtige Antwort(en)				

5.5 Umsetzungsplanung Testfragen (Lerneinheit 8.6)

Beantworten Sie Aufgaben 2 und 3.

	a	b	c	d
Aufgabe 2: Richtige Antwort(en)				
Aufgabe 3: Richtige Antwort(en)				