Goethe-Universität Frankfurt am Main
Lehrstuhl für Mobile Business & Multilateral Security

Wintersemester / ~~Sommersemester~~ .....2010.....

Matrikelnummer: ..... (Bitte auch auf jedes Lösungsblatt oben rechts eintragen!)

Fach: Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle (SEC)
Themensteller: Prof. Dr. Kai Rannenberg
Punktezahl: 90 Zugelassene Hilfsmittel: Keine

Wichtig: Durch Ihre Unterschrift in der Teilnehmerliste bestätigen Sie, folgende Prüfungsvorschriften zu beachten:

- Sie haben den nachfolgenden Text gelesen und stimmen allen Punkten zu.
- Sie fühlen sich gesund und sind in der Lage, an der Prüfung teilzunehmen.
- Sie haben sich über die Vorschriften der PO, die Teilnahme an Klausurprüfungen betreffend, informiert.
- Sie haben zur Kenntnis genommen, dass Sie für die ordnungsgemäße Abgabe der Klausur vor Verlassen des Prüfungsraumes selbst verantwortlich sind. Dazu gehört, dass Sie auf Ihrem Platz bleiben, bis alle Klausuren eingesammelt sind, und den Prüfungsraum nicht verlassen, bevor die Klausuren gezählt und die Vollständigkeit festgestellt wurde.
- Es sind keine Hilfsmittel erlaubt
- Das Mitbringen eines Mobiltelefons oder anderer elektronischer Kommunikationsmedien in die Klausur ist verboten. Zuwiderhandeln gilt als Täuschungsversuch.
- Bitte lassen Sie ausreichend Korrekturrand, und schreiben Sie deutlich und **nicht** mit Bleistift oder roter Tinte.

Im Falle einer **Erkrankung** während der Klausur beachten Sie bitte:

1. Vermerken Sie die Erkrankung in Ihrer Klausur (Unterschrift!) und informieren Sie die Aufsicht unverzüglich.
2. Geben Sie die Klausur und alle Prüfungsblätter ab und achten Sie darauf, dass die Abgabe in der Anwesenheitsliste vermerkt wird.
3. Falls Sie Hilfe benötigen, wenden Sie sich an die Aufsicht.
4. Gehen Sie **unmittelbar** zum Arzt und reichen Sie innerhalb von drei Arbeitstagen ein Attest, das Ihnen die Prüfungsunfähigkeit bescheinigt, beim Prüfungsamt ein.
5. Bei **wiederholter Erkrankung** im selben Studienabschnitt ist ein **amtsärztliches** Attest erforderlich, das die Prüfungsunfähigkeit bescheinigt:
   - ✓ Lassen Sie sich von der Aufsicht oder im Prüfungsamt ein Aufforderungsformular zur Vorstellung beim Amtsarzt geben.
   - ✓ Suchen Sie den Amtsarzt am selben Tag oder am nächsten Arbeitstag auf.

Die Bearbeitung der Klausur erfolgt direkt innerhalb dieses Klausurheftes. Beantworten Sie jede Frage an den dafür vorgesehenen Stellen unterhalb der Aufgabenstellung. Sollten der Platz nicht ausreichen verwenden Sie die zusätzlichen Ersatzblätter am Ende der Klausur nur, wenn der Platz nicht ausreicht, und machen Sie auf dem Aufgabenblatt kenntlich, auf welcher Seite die Weiterbearbeitung der Aufgabe erfolgt.

Bitte für die Korrektur freilassen!

Aufgabe:	1	2	3	4	5	6	7	8	9	Summe
Punkte:										

Punkte: ..... Note: .....

Unterschrift des Prüfers: .....

Aufgabe 1: Authentication (10 Punkte)

Alice ist Kunde bei der *Entenhausener Sparkasse* und nutzt regelmäßig Onlinebanking. Sie erhält eine E-Mail mit dem Betreff „Entenhausener Sparkasse – Aktualisierung Ihrer persönlichen Informationen“. Im Textkörper der E-Mail wird Alice aufgefordert, sich auf der Onlinebanking-Plattform einzuloggen und ihre Stammdaten auf Korrektheit zu prüfen, da eine Wartung des Systems durchgeführt wurde. Unter diesem Text befindet sich auch gleich ein Hyperlink mit dem Titel „Onlinebanking Plattform der Entenhausener Sparkasse - Login“. Alice klickt auf diesem Link. Auf der dann erscheinenden Webseite gibt Alice ihre Login-Daten ein und klickt auf „Login“. Daraufhin erscheint eine Fehlermeldung, die ihr mitteilt, dass der Login fehlgeschlagen ist und wiederholt werden muss. Ein paar Sekunden später wird sie automatisch wieder zur Login-Seite weitergeleitet. Der zweite Login-Versuch ist erfolgreich.

a) Welchem Angriff ist Alice höchstwahrscheinlich zum Opfer gefallen (2 Punkte)?
Password Spoofing oder auch Phishing.

b) Welche Schwächen eines solchen Authentifizierungsschemas (Nutzername/Passwort) ermöglichen diese Art von Angriffen (3 Punkte)?
- Identifizierung und Authentifizierung mittels Nutzername und Passwort bieten nur einseitige Authentifizierung.
- Der Nutzer weiß nicht, wer Nutzername und Passwort erhält.
- Der Nutzer kann nicht (mit Sicherheit) beurteilen, wer auf der anderen Seite der Verbindung sitzt.

c) Nennen und beschreiben Sie zwei Gegenmaßnahmen für diesen Angriff (5 Punkte).

Anzahl der gescheiterten Login-Versuche anzeigen:
- Wenn der erste Login-Versuch scheitert, man beim zweiten Versuch aber angezeigt bekommt, dass es bisher keine Authentifizierungsversuche ohne Erfolg gab, sollte man misstrauisch werden.

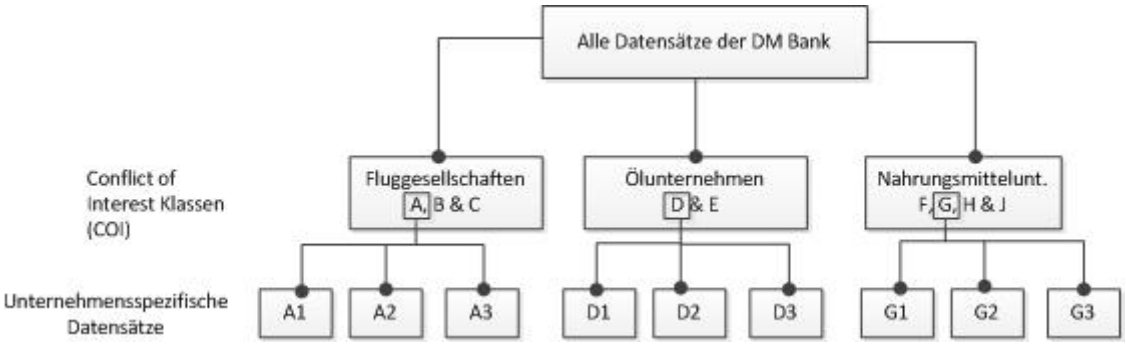
Gegenseitige Authentifizierung:
- Auch das System muss sich gegenüber dem Nutzer authentifizieren.

Trusted path:
- Beispiel: Strg+Alt+Entf in Windows (Task Manager) kann sicherstellen, dass der Nutzer mit dem Betriebssystem kommuniziert und nicht mit einer Schadenssoftware (spoofing program).

Multifaktor-Authentifizierung:
- Multifaktor-Authentifizierung mit zusätzlichem Authentication-Token, da Angriff dann allein mit Nutzername/Password nicht möglich.

Aufgabe 2: Access Control (10 Punkte)

Gegeben sei die Datenbank des Investmenthauses *DM Bank*, in der Investmentinformationen von verschiedenen Unternehmen gespeichert werden. Das folgende *Chinese Wall Model* zeigt die Datensätze jedes Unternehmens und die entsprechenden *Conflict of Interest (COI)* Klassen. Angenommen, Bob ist gerade der DM Bank als Analyst beigetreten und greift daraufhin zuerst auf die Datensätze von Fluggesellschaft A zu (er besitzt nun also Datensätze von Unternehmen A).



a) Kann Bob nun auf Datensätze von Fluggesellschaft B zugreifen? Begründen Sie Ihre Antwort (2 Punkte).

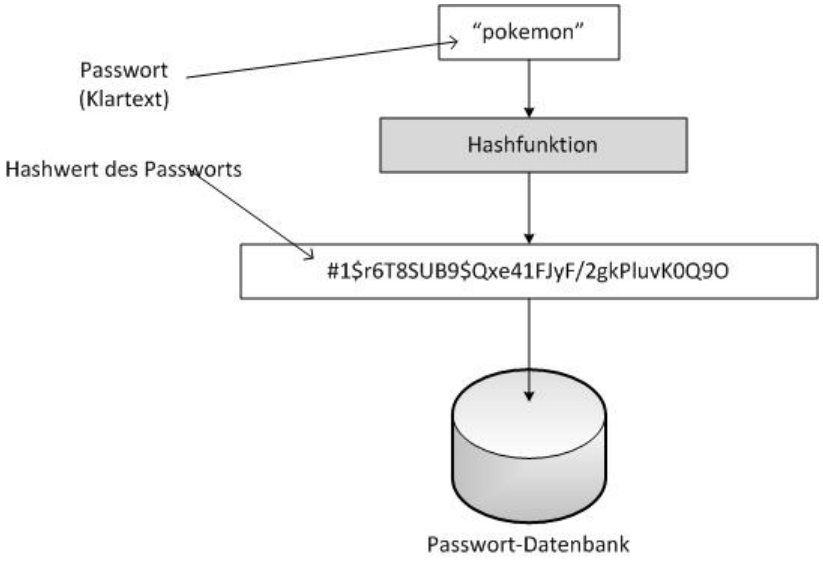
b) Kann Bob nun auf Datensätze von Ölunternehmen D zugreifen? Begründen Sie Ihre Antwort (2 Punkte).

c) Wie viele Analysten (inklusive Bob) werden mindestens benötigt, um auf Datensätze von allen Fluggesellschaften zugreifen zu können (3 Punkte)?

d) Angenommen, Bob greift nun auch auf Datensätze von Nahrungsmittelunternehmen G zu. Nennen Sie sämtliche Unternehmen aus allen COI Klassen, auf die Bob nicht zugreifen kann (heute und in der Zukunft) (3 Punkte).

Aufgabe 3: Cryptography / Electronic Signatures (10 Punkte)

Es ist keine gute Idee, Passwörter auf Rechnersystemen in Klartext zu speichern, da ein Angreifer, der Zugriff auf das System hat, an alle Passwörter gelangen kann. Ein sichererer Weg ist es, den Hashwert des Passworts zu speichern. Dies wird in der folgenden Grafik veranschaulicht.



a) Beschreiben Sie, warum dieser Ansatz sicherer ist. Beantworten Sie dabei auch die Frage, warum jemand, der auf die Passwortdatenbank zugreifen kann, die Passwörter trotzdem nicht herausfinden kann (2 Punkte).

b) Ist es möglich, dass zwei verschiedene Passwörter bei Anwendung einer Hashfunktion in einem identischen Hashwert resultieren? Begründen Sie Ihre Antwort (3 Punkte).

c) Angenommen, das System speichert die Passwörter nicht auf dem System. Wie kann dennoch überprüft werden, ob ein Nutzer bei der Authentifizierung das richtige Passwort eingegeben hat (5 Punkte)?

Aufgabe 4: Datenschutz (12 Punkte)

a) Nennen und beschreiben Sie vier Prinzipien der EU-Datenschutzrichtlinie (0,5 Punkte pro Nennung, 1 Punkt pro Beschreibung).

- **Intention and notification:** The processing of personal data must be reported in advance to a Data Protection Authority.
- **Transparency:** The person involved must be able to see who is processing her data for what purpose.
- **Finality principle:** Personal data may only be collected and processed for specific, explicit and legitimate purposes.
- **Legitimate grounds of processing:** The processing of personal data must be based on a foundation referred to in legislation, such as permission, agreement, and such.
- **Quality:** Personal data must be as correct and as accurate as possible
- **Data subject's rights:** The parties involved have the right to take cognisance of and to update their data as well as the right to raise objections.
- **Processing by a processor:** This rule states that, with the transfer of personal data to a processor, the rights of the data subject remain unaffected and that all restrictions equally apply to the processor.
- **Security:** A controller must take all meaningful and possible measures for guarding the personal data.
- **Transfer of personal data outside the EU:** The traffic of personal data is permitted only if that country offers adequate protection.

b) In der Vorlesung wurden verschiedene Technologien zum Datenschutz vorgestellt („Privacy Enhancing Technologies“). Das System „Idemix“ für anonyme Credentials ist eines davon. Beschreiben Sie den Zweck von anonymen Credentials (2 Punkte) und nennen Sie vier Eigenschaften, die solch ein System haben muss (je 1 Punkt).

Anonymous Credentials are used to prove privileges or attributes of their owner without revealing its identity, e.g. to prove, that

- a device contains an unrevoked Trusted Platform Module (TPM); this is also called Direct Anonymous Attestation
- the owner possesses a subscription and is of the required age, e.g. for an identity management system supporting anonymous video download

Such a system needs to have the following properties:

- Unforgeability of credentials
- Unlinkability of credentials
- No credential sharing
- Consistency of credentials

Aufgabe 5: Biometrie (8 Punkte)

a) Ein biometrisches System habe eine *False Acceptance Rate (FAR)* von 0,01. Wie groß ist die Wahrscheinlichkeit, dass eine Person bei 100 Authentifizierungsversuchen mindestens einmal unberechtigterweise akzeptiert wird (2 Punkte)?

$p(n) = 1 - (1-p)^n$
$p = FAR = 0{,}01$
$n = 100$

➔ $p(100) = 1 - (1 - 0{,}01)^{100} = \underline{0{,}63 = 63\%}$

b) Nennen und beschreiben Sie vier Eigenschaften von Merkmalen zur biometrischen Identifikation (4 Punkte).

Eigenschaften von Merkmalen zur biometrischen Identifikation:
Universalität: Merkmal ist bei jeder Person vorhanden.
Einzigartigkeit: Merkmal ist bei jeder Person anders.
Permanenz: Merkmal ändert sich über die Zeit nicht oder nur minimal.
Erfassbarkeit: Merkmal lässt sich quantitativ erheben.

c) Wählen Sie ein beliebiges physiologisches Merkmal aus, das für biometrische Systeme genutzt werden kann. Nennen Sie je zwei Vor- und Nachteile von biometrischen Systemen, die auf diesem physiologischen Merkmal aufbauen (2 Punkte).

Fingerabdruckanalyse:
Vorteile:
- Sehr gut erforschtes Verfahren
- Hohe Einzigartigkeit des Merkmals
- Billige Sensoren
- Verfahren zur Identifikation geeignet

Nachteile:
- Gute Lebenderkennung relativ aufwendig
- Hygienische Bedenken
- 5% aller Personen haben keine sinnvoll nutzbaren Fingerabdruckmerkmale
- Nicht fälschungssicher

Iris Scanner:
Vorteile:
- Hohe Einzigartigkeit
- Hohe zeitliche Konstanz
- Einfache Lebenderkennung durch Pupillenreflex
- Verfahren zur Identifikation geeignet

Nachteile:
- Merkmalsveränderung durch Krankheit
- Beleuchtung, Brille, Kontaktlinsen
- Kosten
- Nutzerakzeptanz
- Benutzerverhalten bei aktiven Systemen

Gesichtserkennung:

Vorteile:

- Hohe Benutzerfreundlichkeit
- Hohe Akzeptanz
- Gesicht ist immer (wenigstens teilweise) sichtbar
- Kann unbeobachtet aufgenommen und überprüft werden

Nachteile:

- Geringe relative zeitliche Konstanz
- Niedrige Einzigartigkeit
- Keine Kooperation erforderlich
- Kann unbeobachtet aufgenommen und überprüft werden

Aufgabe 6: Computer System Security (10 Punkte)

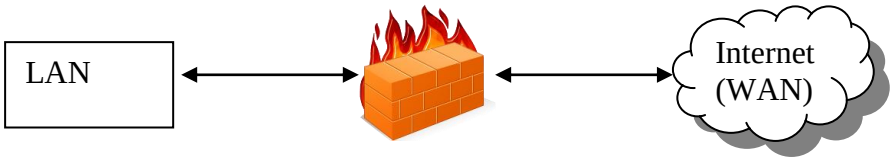
Nennen Sie 5 gängige Typen von Viren, und beschreiben Sie diese kurz. **(10 Punkte)**.

Aufgabe 7: Network Security (10 Punkte)

a) Was verstehen Sie im Kontext Netzwerksicherheit unter einer Firewall (2 Punkte)?

Eine Firewall ist ein spezialisierter netzwerkverbindender Rechner (Internetwork Gateway) der die Kommunikation zu und von einem der verbundenen Netze beschränkt/überwacht (inneres Netze/LAN) und dadurch die Ressourcen des Netzwerks gegen Bedrohungen von außen (WAN/Internet) schützt. Paketfilterung auf Basis von Regeln.

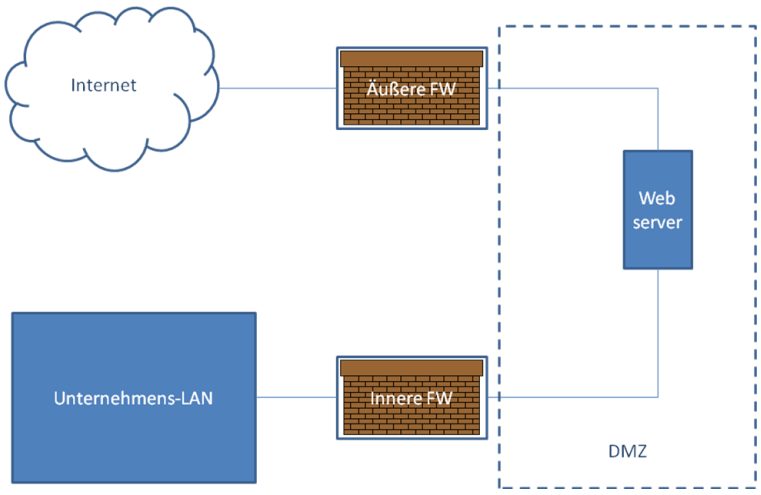
b) Skizzieren Sie kurz, wo sich eine Firewall in der Netzwerkinfrastruktur üblicherweise befindet (1 Punkt).



c) Beschreiben Sie: Was ist eine demilitarisierte Zone (DMZ) (2 Punkte)?

- Unter einer DMZ versteht man einen Netzwerkabschnitt/Segment in welchem eine Separation zwischen internem und externem Netzwerk stattfindet.
- Die "äußere Firewall" befindet sich zwischen dem Internet/WAN und der DMZ eine "innere Firewall" zwischen der DMZ und dem LAN
- Die DMZ stellt einen limitierten/kontrollierten öffentlichen Zugang und einen ebenso limitierten/kontrollierten Zugang aus dem LAN zu Servern in der DMZ zur Verfügung schottet den öffentlichen Zugang aber gegen das LAN vollständig ab.

d) Sie wollen vermeiden, dass Ihr Firmenwebserver unmittelbar am Unternehmens-LAN angeschlossen ist, aber er soll sowohl aus dem Internet als auch aus dem Unternehmens-LAN erreichbar sein. Skizzieren Sie kurz, wie eine solche Infrastruktur aussehen könnte und beschriften Sie die verwendeten Komponenten, Netze und Zonen (4 Punkte)?



e) Sie planen eine Niederlassung in einer anderen Stadt an Ihr Firmennetzwerk anzuschließen, damit die dortigen Mitarbeiter auf Daten auf den Servern der Zentrale zugreifen können. Aus Kostengründen verbinden Sie beide Standorte über das

Internet. Wie gewährleisten Sie, dass die über das Internet übertragenen Daten vertraulich bleiben (1 Punkt)?

VPN, Verschlüsselung, IPSec.

Aufgabe 8: Security Engineering (12 Punkte)

a) Vervollständigen Sie bitte den „Secure System Development Process“, in dem Sie die fehlenden Angaben für 1 – 4 eintragen (2 Punkte)? Erläutern Sie außerdem stichwortartig die Aufgabe(n) der Schritte 1 und 3 (2 Punkte).

1: Threat Analysis / Bedrohungsanalyse

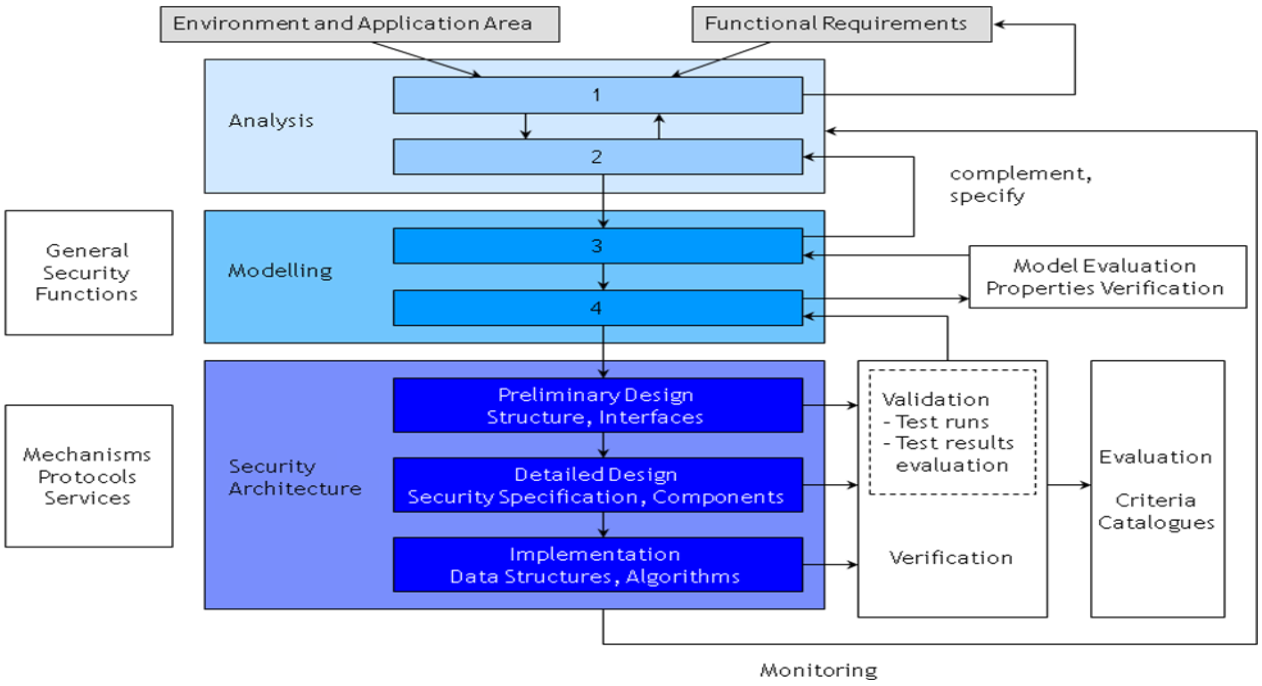
Aufgabe(n): Untersuchung von System Schwächen/Verletzlichkeiten/Verwundbarkeiten hinsichtlich bekannter Bedrohungsquellen zur Bestimmung existierender Bedrohungen für ein definiertes System in seiner spezifischen Einsatzumgebung.

2: Risk Analysis / Risikoanalyse

3: Security Policy / Sicherheitsleitlinie

Aufgabe(n): Modellierung abstrakter Sicherheitsanforderungen, Abbildung Beziehungen zwischen konkreten Sicherheitsleitlinienelementen und Basis Sicherheitsfunktionen

4: Security Model / Sicherheitsmodell



b) Wie ist ein „Attack Tree“ (Angriffsbaum) aufgebaut (3 Punkte) und wofür verwendet man ihn (1 Punkt)?

Aufbau:

- Wurzel: symbolisiert das Angriffsziel
- Folgende Ebene(n): beinhalten als Knotendargestellte Zwischenziele die erreicht werden müssen, damit das Angriffsziel erreicht wird.

UND-Knoten müssen gemeinschaftlich erreicht/erfüllt werden, ODER-Knoten hingegen alternativ.

- Blätter: stellen möglich Angriffswege zur Erreichung des Angriffszieles dar

Verwendung:

- *System Bedrohungen* können als Angriffsbäume dargestellt werden außerdem dienen als *Hilfsmittel zur Risikoanalyse*.

c) Sie sollen eine Risikoanalyse durchführen. Welche Herangehensweisen für die Durchführung kennen Sie und wie unterscheiden sich diese (2 Punkte)?

Quantitativ Analyse

- Versucht realistische Zahlenwerte allen Elementen des Risikoanalyseprozesses zuzuordnen.
- Jedes Element wird quantifiziert und in Berechnungen zur Ermittlung des Restrisikos eingesetzt.
- Eine rein quantitative Risikoanalyse ist nicht möglich, da die Methode versucht qualitativen Werten Zahlenwerte zu zuordnen was immer mit Unschärfe/subjektiver Bewertung verbunden ist.

Qualitative Analyse

- Risiken werden in der Regel auf eine zwei bis vier stufigen Skala qualitativ bewertet (niedrig, mittel, hoch, katastrophal).

d) Was ist UMLsec (1 Punkte)?

Eine Erweiterung der UML zur Unterstützung sicherer Softwareentwicklung.

e) Nennen Sie einen Vorteil von UMLsec (1 Punkte).

- Evaluate UML specifications for weaknesses in design.
- Zusammenfassen etablierter Regeln zum sicheren entwickeln in Checklisten.
- Sicherheitsüberlegungen werden für Entwickler ohne entsprechende Spezialisierung verfügbar gemacht.
- Berücksichtigung von Sicherheitsanforderungen im Systemkontext schon in frühen Entwicklungsphasen.
- Unterstützung für kosteneffektive Zertifizierung.

Aufgabe 9: Security Management (8 Punkte)

a) Nennen Sie zwei Aufgaben des IT-Security Managements (2 Punkt).
- Notwendige Prozesse implementieren (Get relevant Processes in place).
- Entwickeln einer verbindlichen Organisationsstruktur (Create a responsible organizational structure).
- Sicherheit zum Unternehmensziel machen. (Make IT-Security a Business objective).

b) Skizzieren Sie den aus vier Schritten bestehenden Lebenszyklus eines ISMS (2 Punkte). Beschreiben Sie stichwortartig, was in jedem den einzelnen Schritten passiert (4 Punkte).