3,4,7,10,13,14,15,16,17,18

Chapter 3

1. In general terms, what are four means of authenticating a user's identity?

Etwas, das der Einzelne **weiß**: Beispiele enthalten ein **Passwort**, eine persönliche Identifikationsnummer (**PIN**) oder **Antworten auf eine** verabredete Reihe von **Fragen**.
Etwas, das der Einzelne **besitzt**: Beispiele sind elektronische **Schlüssel-Karten, Chipkarten** und physische keys. Dieser Typ von Authentisierer ist als **Token** bezeichnet.
Etwas, das Einzelne **ist** (**statische Biometrie**): Beispiele dafür sind Erkennung durch **Fingerabdruck**, **Netzhaut** (Retina) und im **Gesicht**.
Etwas, das der Einzelne **tut** (**dynamische Biometrie**): Beispiele dafür sind **Erkennung durch Stimme,** Muster, **Handschrift** Eigenschaften, und **Schreibrhythmus**.

2. List and briefly describe the principal threats to the secrecy of passwords?

Offline-Wörterbuch-Angriff: Der Angreifer erhält das System-Passwort-Datei und vergleicht die Passwort-Hashes gegen Hashes der am häufigsten verwendeten Passwörter. Wenn eine Übereinstimmung gefunden wird, kann der Angreifer Zugang von diesem ID / Passwort-Kombination.
Bestimmtes Konto Angriff: Der Angreifer zielt auf ein bestimmtes Konto und legt Passwort Vermutungen vor, bis das richtige Passwort gefunden wird.
Beliebter Passwort Angriff: Eine Variation des vorhergehenden Angriff ist ein beliebtes Passwort zu verwenden und versuchen es gegen ein breites Spektrum von Benutzer-IDs zu benutzen.
Erraten von Passwörtern gegen einzelne Anwender: Der Angreifer versucht, das Wissen über den Kontoinhaber und System Passwort Police zu erhalten und nutzt dieses Wissen, um das Passwort zu erraten.
Workstation-Hijacking: Der Angreifer wartet bis eine angemeldete Workstation unbeaufsichtigt ist.
Ausnutzung Benutzerfehlern: Strict polices zwingen komplizierteres Passwort und der Benutzer ist wahrscheinlicher, es aufzuschreiben, weil es schwierig zu merken ist. Ein Angreifer kann den Benutzer oder einen Account Manager zur Preisgabe eines Passwortes täuschen (auch: vorkonfigurierte Passwörter für System-Administratoren sind eine Bedrohung)
Nutzung mehrerer Passwortbenutzung
Elektronische Überwachung: Wenn ein Passwort über ein Netzwerk kommuniziert wird um sich bei einem Remote-System anzumelden, ist es angreifbar für Lauschangriffe.

3. What are the two common techniques used to protect a password file?

Verwendung eines salt value. Dieses Salt wird in Klartext mit dem Hash aus (Salt + Passwort) gespeichert. **Password File Access Control.** Die Hash-Passwörter werden in einer separaten Datei aus dem Benutzer-IDs, bezogen auf **Shadow-Password-file**, gespeichert. Nur privilegierte Benutzer haben Zugriff auf diese Datei.

4. List and briefly describe four common techniques for selecting or assigning passwords.

– **User education**
– **Computer-generated passwords**
– **Reactive password checking**: Das System führt regelmäßig eigene Passwort-Cracker und benachrichtigt den Benutzer, wenn es in der Lage war sein Passwort zu knacken.
– **Proactive password checking**: Der Benutzer wählt sein Passwort auf Regeln, geben durch das System (zB mindestens acht Zeichen lang etc.)

5. Explain the difference between a simple memory card and a smart card.

Memory Card: Speichert, aber verarbeitet nicht Daten.
Smart Card: Hat einen Mikroprozessor, verschiedene Speicher, I / O-Ports, etc. können auch einen Krypto-Coprozessor und eine eingebettete Antenne haben.

6. List and briefly describe the principal characteristics used for biometric identification.

Facial characteristics, Fingerprints, Hand geometry, Retinal pattern, Iris, Signature, Voice

7. In the context of biometric user authentication, explain the terms, enrollment, verification, and identification.

Enrollment: Jede **Person**, die **in der Datenbank** der autorisierten Benutzer **aufgenommen** werden soll, muss zuerst in das System eingetragen werden.
Verification: Der Benutzer gibt einen **PIN und** verwendet auch einen **biometrischen Sensor.**
Identification: Die einzelnen verwendet die **biometrischen Sensor,** zeigt aber keine zusätzlichen Informationen

8. Define the terms *false match rate* and *false non-match rate,* and explain the use of a threshold in relationship to these two rates.

False match rate: Er misst den **Prozentsatz der ungültigen Eingaben,** die fälschlicherweise **akzeptiert** werden.
False non-match rate: Es misst den **Prozentsatz der gültigen Eingaben**, die fälschlicherweise **zurückgewiesen** werden.

Durch Bewegen des Schwellenwertes, kann die Wahrscheinlichkeiten verändert werden, aber bemerke, dass eine Abnahme der false match rate zwangsläufig zu einer Erhöhung der false non-match rate führt, und umgekehrt.

9. Describe the general concept of a challenge-response protocol.

Der Host erzeugt eine Zufallszahl **r** und sendet sie an den Benutzer (= **Challenge)**.
Darüber hinaus legt der Host zwei Funktionen an, ei**ne Hash-Funktion h (), und eine weitere Funktion f ()**, die in de r Antwort verwendet werden.
Der **Benutzer berechnet f(r', h(P'))**, wobei r'= r und P' das Benutzerpasswort ist. Wenn die Antwort ankommt, **vergleicht** der **Host** das eingehenden Ergebnis der berechneten **f(r, h(P))** und bei Übereinstimmung ist der Benutzer authentifiziert.
Vorteile: Nur die **Hashes der Kennwörter gespeichert** werden, und sie **müssen nicht direkt übertragen** werden, so kann ich während der Übertragung nicht erfasst werden.

Chapter 4

1. Briefly define the difference between DAC and MAC.

Discretionary (ermessen) access control: Steuert den Zugriff basierend auf der **Identität des Anfragenden** und **access rules gibt an was** Anforderer **tun oder nicht tun dürfen**.
Mandatory access control: Steuert den Zugriff basiernd auf den **Vergleich Sicherheitsetiketten mit security clearances.**

2. How does RBAC relate to DAC and MAC?

Role-based access control: Steuert den Zugriff auf den **Rollen**, die Benutzer haben **innerhalb des Systems** und **rules gibt an welche Zugriffe** von die Benutzer **in bestimmten Rollen** erlaubt sind.

3. List and define the three classes of subject in an access control system.

Owner: Dies kann der Ersteller einer Ressource, z. B. einer Datei sein.
Group: Zusätzlich zu den zugewiesenen Berechtigungen eines Besitzers, einer benannten Gruppe von Benutzern kann auch die gewährten Zugriffsrechte sein.
World: Die neueste Menge von Zugriff, die Benutzer gewährt wurde, die Lage sind in das System zugreifen zu können, aber nicht in den Kategorien Eigentümer und die Gruppe dieser Ressource enthalten sind.

4. In the context of access control, what is the difference between a subject and an object?

Ein **subject** ist eine **entity mit Zugriff auf Objekte** (zB Benutzer-, Anwendungs-, Prozess).
Ein **object** ist **Ressource, auf die der Zugriff kontrolliert wird.** Ein Objekt ist eine **entity,** die verwendet wird, um Informationen (zB Datensätze, Dateien, Verzeichnisse, Prozessoren, Kommunikations-Ports) zu enthalten.

5. What is an access right?

Ein Zugriffsrecht beschreibt **die Art**, in der ein **Subjekt auf** ein **Objekt zugreifen** kann. Eg. lesen, schreiben, ausführen, löschen.

6. What is the difference between an access control list and a capability ticket?

In der Praxis ist eine Zugangsmatrix Regel spärlich und durch Zersetzung in einer von zwei Weisen implementiert.
Die Matrix kann durch Spalten zerlegt werden, Gewinnung von **access control lists**. **Für jedes Objekt, ein ACL listet Benutzer und deren erlaubte Zugriffsrechte.**
Zersetzung durch Zeile gewinnt man **capability tickets** . **Eine capability tickets spezifiziert autorisierten Objekten und Operationen für einen bestimmten Benutzer.**

7. What is a protection domain?

Ein **Schutz-Domäne eine Gruppe von Gegenständen zusammen mit Zugriffsrechten für diese Objekte.** Im Hinblick auf die Zugangsmatrix definiert eine Zeile eine Schutzdomain. Obwohl in dem Schutzdomain Modell kann ein Benutzer Prozesse mit einer Teilmenge der Zugangsrechte des Benutzers erzeugen. Dies ist nützlich für Server um Prozesse für verschiedene Klassen von Benutzern zu erzeugen und für nicht voll vertrauenswürdigen Prozesse zur Reduzierung von ihren Zugriffsrechte auf ein sicheres Subset.

8. Briefly define the four RBAC models of Figure 4.9a.

RBAC0: enthält die minimale Funktionalität für ein RBAC-System.
RBAC1: umfasst die RBAC0 Funktionalität und fügt **Rolle Hierarchien**, die es einer **Rolle** ermöglichen **Berechtigungen von einer anderen Rolle zu erben.**
RBAC2: umfasst RBAC0 und fügt **constraints** (=Zwängen), die die Wege beschränken, auf denen die Komponenten eines RBAC System konfiguriert werden können.
RBAC3: enthält die **Funktionalität** von **allen anderen** drei **Modellen**.

9. List and define the four types of entities in a base model RBAC system.

User: Eine Person, die Zugriff auf dieses Computer System hat. Jedes Individuum hat eine zugeordnete Benutzer ID.
Role: Eine benannte Job-Funktion innerhalb der Organisation, die diese Computer-System steuert.
Permission: Eine Genehmigung eines bestimmten Modus mit Zugriff auf ein oder mehrere Objekte..
Session: Eine Mapping zwischen einem Benutzer und einem aktivierten Subset des Rollensets, auf dem der Benutzer zugewiesen ist.

10. Describe three types of role hierarchy constraints.

mutually exclusive roles: Das sind Rollen, so dass ein Benutzer **nur eine Rolle in dem Set zugeordnet werden** kann.
cardinality: Dies **bezieht sich auf eine maximale Anzahl in Bezug auf Rollen**. Eine solche Einschränkung ist eine maximale Anzahl von Benutzern, die zu einer gegebenen Rolle zugeordnet werden kann.
prerequisite roles: Kann diktieren, dass ein **Benutzer nur auf eine** bestimmte **Rolle zugewiesen werden kann, wenn** es **bereits** auf eine **andere** bestimmte **Rolle zugewiesen** wurde.

11. In the NIST RBAC model, what is the difference between SSD and DSD?

Static Separation of Duty Relations: **SSD** ermöglicht die Definition einer Reihe von **mutually exclusive roles** (sich gegenseitig ausschließenden Rollen). SSD kann eine **Kardinalität mit Einschränkung** für ein Rollenset platzieren.
Dynamic Separation of Duty Relations: **DSD** schränkt die Verfügbarkeit der Berechtigungen beim Platziern mit Einschränkung auf die Rollen, die innerhalb oder über einer user session aktiviert werden können.

Chapter 7

1. What is the role of compression in the operation of a virus?

Ein Virus kann Komprimierung so verwenden, dass das **infizierte Programm** genau der gleichen Länge wie ein uninfizierte Version ist.

2. What is the role of encryption in the operation of a virus?

Die **Mutation Engine erzeugt** einen **zufälligen** Verschlüsselungs**schlüssel** um den Rest des **Virus zu verschlüsseln**. Der **Schlüssel** wird **mit** dem **Virus gespeichert**, und die Mutation Engine selbst wird verändert. Wenn das **Virus sich kopiert**, wird ein **anderer Zufallsschlüssel ausgewählt**. **Da** der Großteil des **Virus** mit einem anderen Schlüssel für jede Instanz **verschlüsselter wird,** ist das **keine konsistente Bitpattern zu beobachten.**

3. What are the typical phases of operation of a virus or worm?

Dormant phase: Das Virus im Leerlauf ist, wird es schließlich durch ein Event aktiviert, wie ein Datum oder ein anderes Programm.
Propagation phase: Der Virus platziert eine Kopie von sich selbst in andere Programme oder in bestimmte Systembereiche auf der Festplatte
Triggering phase: Das Virus wird aktiviert, um die Funktion für die es bestimmt war durchzuführen. Wie bei der dormant phase kann die triggering phase durch eine Vielzahl von Systemereignisse verursacht werden.
Execution phase: Die Funktion wird ausgeführt. Die Funktion kann harmlos sein, wie eine Meldung auf dem Bildschirm, oder schädlich, wie die Zerstörung von Programmen und Dateien.

4. What is a digital immune system?

Dieses System bietet einen **general-purpose emulation** und **virus-detection system.** Ziel ist es, **schnelle Ansprechzeit anzubieten**, so dass Viren fast so schnell wie sie eingeführt werden abgestempelt werden. Wenn ein neues Virus eine Organisation eintritt, das **Immunsystem erfasst** ihn automatisch, **analysiert** ihn, **fügt detection and shielding hinzu** für ihn, entfernt ihn und **leitet Informationen** über diesen Virus an Systemen auf dem ein allgemeines Antivirenprogramm ausgeführt wird, so dass er erkannt werden kann, bevor es ihm erlaubt ist woanders zu laufen.

5. How does behavior-blocking software work?

Behavior-blocking software **integriert mit** dem **Betriebssystem** des Host-Computers und **überwacht das Verhalten des Programms** in Echtzeit für böswillige Aktionen. Das VBehavior-blocking software **blockiert** dann potenziell **schädliche Aktionen,** bevor sie eine Chance haben das System zu beeinflussen.

6. In general terms, how does a worm propagate?

- **Suche nach anderen Systemen** zu infizieren mithilfe der Prüfung von Host-Tabellen oder ähnlichen Repositories von Remote-System-Adressen
- **Herstellung** einer **Verbindung** mit einem Remote-System
- **Kopieren** sich selbst auf das Remote-System **und** verursachen, dass die Kopie **ausgeführt** wird.

7. Describe some worm countermeasures.

Signature-based worm scan filtering: Erzeugt eine Wurm Signatur, die dann verwendet wird, um Wurm Scans aus Betreten / Verlassen eines Netzwerk / Host zu verhindern.
Filter-based worm containment:Konzentriert sich eher auf den Inhalt des Werkes als auf eine Scan-Signatur. Der Filter überprüft eine Nachricht, um festzustellen, ob es Wurm-Code enthält.
Payload-classification based worm containment: Diese Netzwerk-basierte Techniken untersuchen Pakete, um zu sehen, ob sie einen Wurm enthalten.
Threshold random walk scan detection: TRW nutzt die Zufälligkeit in der Zielauswahl um zu verbinden als Mittel zur Feststellung, ob ein Scanner ist im Betrieb.
Rate limiting: Diese Klasse begrenzt die rate of scanlike traffic von einem infizierten Host.
Rate halting: Dieser Ansatz blockiert ausgehenden Datenverkehr, wenn ein Schwellenwert überschritten wird entweder in ausgehende Verbindungrate oder Vielfalt der Verbindungsversuche.

8. What is the difference between a bot and a rootkit?

Bot: Ein Bot ist ein **Programm**, **das** heimlich weitere Internet angeschlossenen **Computer übernimmt** und verwendet dann diesen Computer um **Angriffe zu starten**, **die nur schwer** zu den **Bot creator zurück zu verfolgen** sind.
Rootkit: Ein Rootkit ist **ein Set von Programmen**, die auf einem System installiert werden, um **Administrator-Zugriff** auf das System **zu erhalten**. Er **verändert** die **Host-**Standard-**Funktionalität in einer bösartigen** und verstohlenen **Art**. Rootkits verlassen sich nicht direkt auf Schwachstellen, um auf einem Computer zukommen.

Chapter 10

1. Explain the differences among the terms *security class*, *security level, security clearance* and *security classification*.

security class: jeder Gegenstand und jedes Objekt wird zu einer security class zugeordnet.
security level: im einfachsten Formulierung, security classes formen eine strenge Hierarchie und werden als security levels bezeichnet, wie *strategische> sensitive> vertrauliche> public.*
security clearance: ein *subject*, soll eine Sicherheitsüberprüfung einer bestimmten Ebene haben
security classification: Ein *object* soll einen Geheimhaltungsgrad haben

2. What are the three rules specified by the BLP model?

no read up – **simple security property**
no write down - ***-property**
ds-property: ein Individuum kann auf ein anderes Individuum Zugang zu einem Dokument basiernd auf Benutzerermessen gewähren, eingeschränkt durch die Mandatory Access Control (**MAC**) rules. So kann ein subject nur, Zugänge, für die sie die erforderliche Genehmigung hat,

und die, die MAC-Regeln erfüllen, ausführen.

3. How is discretionary access control incorporated into the BLP model?

Through the ds-property.

4. What is the principal difference between the BLP model and the Biba model?

Das BLP-Modell befasst sich mit der Vertraulichkeit und unbefugten Weitergabe von Informationen. Das **Biba-Modell** befasst sich mit **Integrität** und **unbefugte Änderung** von Daten.

5. What are the three rules specified by the Biba model?

Simple integrity: Ein subject kann ein object nur **ändern**, wenn das **Integrität Level** des subjects **dominiert** das Integrity Level des objects: I(S)> = I(O).
Integrity confinement: Ein subject kann ein object nur **lesen**, wenn das **Integrität Level** des subjects **niedriger** ist als der Integrity Level des objects.
Invocation property: Ein subject kann ein anderes subject nur **aufrufen**, wenn das Integrität Level der **ersten subjects beherrscht** das Integritäts Level des **zweiten** subjects:. I(S1) > = I(S2).

6. Explain the difference between certification rules and enforcement rules in the Clark-Wilson model.

certification rules: Sicherheitspolicy Beschränkungen auf das Verhalten der integrity verification procedures (IVPs) and transformation procedures (TPs).
enforcement rules: built-in-System Sicherheitsmechanismen, die die Ziele der Zertifizierung Regeln erreichen.

7. What is the meaning of the Term Chinese wall in the Chinese Wall Model?

Die Chinesische Mauer hat das Ziel, einen **Interessenkonflikt** zu vermeiden.

8. What are the two rules that a reference monitor enforces?

no read up, no write down

9. What properties are required of a reference monitor?

complete mediation, isolation, verifiability

10. In general terms, how can MLS be implemented in an RBAC system?

Constraint on users, Constraint on permissions, Definitions, Constraints on UA.

11. Describe each of the possible degrees of granularity possible with an MLS database system.

entire database, individual tables, individual columns, individual rows, individual elements

12. What is polyinstantiation?

Write Access in DB systems: Ein niedriger privilegierten Benutzer versucht, eine Zeile in eine Tabelle einzufügen mit einem Primärschlüssel, der bereits existiert. Der Schlüssel wurde von einem höheren privilegierten Benutzer hinzugefügt und ist vertraulich. **Polyinstantiation vermeidet Inferenz und Probleme mit der Integrität** und ermöglicht dem Benutzer die Zeile einzufügen. Dieser erstellt eine Datenbank mit widersprüchlichen Einträgen.

13. Briefly describe the three basic services provided by a Trusted Platform Modules (TPMs).

authenticated boot: Der authentifizierte Boot-Service ist für das Booteing das gesamte Betriebssystem in Stufen verwantwortlich und stellt sicher, dass jeder Teil des OS, wie es geladen wird, eine Version ist, die zur Verwendung genehmigt ist. Dies wird durch Verifizieren einer digitalen Signatur verbunden mit der Software.
certification: Das TPM kann ein digitales Zertifikat mit der Unterzeichnung eines formatierten Beschreibung der Konfigurationinformation unter Verwendung des TPM privaten Schlüssel zu erzeugen. So kann ein anderer Benutzer sicher sein, dass eine unveränderte Konfiguration in Gebrauch ist.
encryption: Die Verschlüsselungs-Service ermöglicht die Verschlüsselung von Daten in der Weise, dass die Daten **nur** von einer bestimmten Maschine entschlüsselt werden können, und nur, wenn diese Maschine in einer bestimmten Konfiguration ist.

14. What is the aim of evaluating an IT product against a trusted computer evaluation standard?

Das Ziel dieser Standards ist es, **mehr Vertrauen in die Sicherheit von IT-Produkten** zu gewährleisten.

15. What is the difference between *security assurance* and *security functionality* as used in trusted computing evaluation standards?

Funktionale Anforderungen definieren gewünschtes Verhalten.
Assurance Anforderungen sind die Grundlage für Vertrauen gewinnen, dass die geforderten Sicherheitsmaßnahmen wirksam sind und korrekt implementiert sind.

16. Who are the parties typically involved in a security evaluation process?

Sponsor, Developer, Evaluator, Certifier

17. What are the three main stages in an evaluation of an IT product against a trusted computing standard, such a the Common Criteria?

Preparation, Conduct of evaluation, Conclusion

Chapter 13

1. What are the principal concerns with respect to inappropriate temperature and humidity?

Computer sind entworfen, um innerhalb eines **bestimmten Temperaturbereichs** (meist zwischen **10-32°C**) zu arbeiten. **Außerhalb** dieses Bereiches könnten Ressourcen weiterhin arbeiten, aber erzeugen **unerwünschte Ergebnisse** und **Komponenten** könnten **beschädigt** werden. Ein weiteres Problem ist die Innentemperatur vom Gerät, die deutlich höher als die Raumtemperatur ist. Die **Kühlmechanismen verlassen sich auf**, oder werden beeinflusst von**, äußere Bedingungen**.
Die relative **Luftfeuchtigkeit** sollte zwischen **40% und 60%** gehalten werden. Zu h**ohe Luftfeuchtigkeit** kann zu **Korrosion, Kondensation** (Bedrohung für magnetische und optische Speicherung sowie Leiterplatten) **führen**. Zu **niedrige Luftfeuchtigkeit** kann dazu führen, das einige **Materialien** ihre **Form zu ändern** und **statische Elektrizität wird zum Risiko**.

2. What are the direct and indirect threats posed by fire?

Die Bedrohung kommt nicht nur von der **direkten Flamme,** sondern auch von der **Hitze**, Freisetzung von **giftigen Dämpfen, Wasser**schäden von Feuerunterdrückung und **Rauchschäden**. Ferner Feuer kann **die Versorgung stören**, insbesondere **Strom**.

3. What are the threats posed by loss of electrical power?

3 Gruppen von Energieversorgungsproblemen: *Unterspannung, Überspannung, Lärm.*
Unterspannung events reichen von vorübergehenden Einbrüche der Spannungsversorgung zu **Spannungsabfälle**, zu**Stromausfälle**. Grundsätzlich ist kein Schaden angerichtet, aber der Service ist unterbrochen.
Ein Anstieg der **Überspannung durch** eine Versorgung **Anomalie**, einige interner **Verkabelungsfehler** oder **Blitzschlag** können elektrische **Bauteile zerstören**.
Lärm kann mit Signalen im Inneren elektronische Geräte zerstören, was **logische Fehler verurascht.**

4. List and describe some measures for dealing with inappropriate temperature and humidity.

Für den Umgang mit dieser Sache ist es erforderlich, **environmental-control equipment** und eine geeignete **Sensoren** zu haben, die **warnen**, falls der Schwellenwerte überschritten wird.

5. List and describe some measures for dealing with fire.

Wahl des Standorts um die Wahrscheinlichkeit von Katastrophen zu **minimieren**, **Klimaanlage sollten designed sein,** so dass sich das Feuer nicht ausbreitetet, **Positionierung von Geräten** um Schäden zu minimieren, **Brennbares sollte nicht in den IS-Bereich aufbewahrt werden**, **handbetriebenen Feuerlöscher** leicht erreichbar und regelmäßig getestet, **Automatische Feuerlöscher, Power-Off-Schalter, Notfallmaßnahmen** ausgehängt, die Sicherheit des Personals, **Aufzeichnungen für Datei-Rekonstruktion benötig werden, werden außerhalb des Betriebes gelagert.**

6. List and describe some measures for dealing with water damage.

Kenntnisse über die Gliederung der Wasserzuleitungen ist entscheidend für sinnvolle Geräteanordnung. Die Lage aller **Absperrventile muss deutlich sichtbar** sein oder zumindest deutlich dokumentiert und verantwortliches Personal sollte die Notfallmaßnahmen kennen. **Wasser-Sensoren** sind von entscheidender Bedeutung, **um mit Sanitär-Lecks** umzugehen und andere Quellen von Wasser und sollte sich **auf dem Boden der EDV-Räume befinden.**

7. List and describe some measures for dealing with power loss.

Um mit kurzen Stromunterbrechungen umzugehen, sollte eine **unterbrechungsfreie Stromversorgung** (uninterruptible power supply **UPS =** Backup-Batterie-Einheit) für kritische Geräte eingesetzt werden. Eine UPS kann als ein **Überspannungsschutz**, **power noise filter** und **automatic shutdown device** funktionieren, wenn die Batterie zur Neige geht. Für **längere Stromausfälle** kann eine Notstromquelle wie **Generator** installiert werden.

Chapter 14

1. What are the benefits of a security awareness, training, and education program for an organization?

- **Verbesserung** der Mitarbeiter-**Verhalten**
- Steigerung der Fähigkeit **Mitarbeiter** für ihre Handlungen **verantwortlich machen**
- **Schadensbegrenzende Haftung der Organisation** für ein Mitarbeiterverhalten
- **Einhaltung von Vorschriften** und vertraglichen Verpflichtungen

2. What is the difference between security awareness and security training?

Ein **Security Awareness Programm** versucht, zu **informieren und** zu **konzentrieren** eines Mitarbeiters **Aufmerksamkeit auf Themen betreffend der Sicherheit** innerhalb der Organisation. Die Ziele sind: Mitarbeiter sind in Kenntniss über ihre **Verantwortung für** die Aufrechterhaltung der

Sicherheit, Benutzer **verstehen** auf die **Wichtigkeit** von Sicherheit, sie **lernen über** die **Sanktionen** und Disziplinarmaßnahmen wegen Verstößen verhängt werden.
Ein **Security Training-Programm** wurde **entwickelt**, um Menschen beizubringen, die Fähigkeiten, um **IS-Aufgaben sicherer** durchzuführen. Zum Beispiel: Der **Schutz der physischen Bereich und Anlagen** und **schützen Passwörter oder andere Authentifizierungs-Daten oder Token,** die **Meldung** sicherheitsrelevanter Verletzungen oder **Vorfälle**. Programmierer und System-Betreuer erfordern spezialisierte oder Weiterbildung.

3. What is an organizational security policy?

Eine **security policy** ist eine **formelle Erklärung zu den Regeln**, nach denen **Menschen, die Zugang zu** einer Organisation **technologie haben** und Informationkapital **aufrechthalten müssen**. Es macht deutlich, **was geschützt wird und warum, artikuliert Sicherheitsverfahren, heißt** die **Verantwortung** für diesen Schutz, **bietet eine Grundlage zur Lösung späterer Konflikte,** die entstehen können.

4. Who should be involved in developing the organization's security policy and its security policy document?

Site security administrator, information technology staff, **supervisors of large user groups** (eg. business divisions), **security incident response team**, **representatives of the user groups affected by the security policy,** responsible **management.**

5. What is the ISO 17799?

Die ISO 17799 ist ein umfassendes **Set von Kontrollen** miteingeschlossen die Best Practices im Bereich der **Informationssicherheit**. Es ist im Wesentlichen eine international anerkannte **allgemeine Informationssicherheitsstandard.**

6. What principles should be followed in designing personnel security policies?

Before employment: **Background checks and screening** (früheren Arbeitgeber fragen, frage die mögliche Mitarbeiter für so viele Details wie möglich über Beschäftigungs-und Bildungs-Geschichte, die es immer schwieriger, zu lügen macht, sorgen für erfahrene Mitarbeiter zu interviewen Kandidaten, etc.), **Beschäftigungsvereinbarung**.
During employment: **Least Privileg, Trennung von Aufgaben, begrenzte Abhängigkeit von schlüsselmitarbeitern.**
Termination of employment: **Entfernen den Namen der Person aus allen Listen der autorisierten Zugriff**, informieren Wachen, **ändern** Sperrekombinationen und **Zugang Kartensysteme, wieder alle Vermögenswerte** wie ID, Datenträger, Unterlagen und equipment.

7. Why is an e-mail and Internet use policy needed?

- Erhebliche Arbeitszeit kann durch Aktivitäten auf der Web konsumiert werden und wichtige Ressourcen können unnötig verbraucht werden.
- Übermäßiger Einsatz des Internet und E-Mail unnötig erhöht das Risiko der Einschleppung von bösartiger Software in der Organisation ist die Umwelt.
- Die nicht-arbeitsbezogenen Mitarbeiter Aktivität könnte in gefährlich für anderen Individuen werden, wodurch eine Haftung für die Organisation entsteht
- E-Mail und das Internet als Werkzeug der Belästigung von einem Mitarbeiter gegen eine andere verwendet werden.
- Unangemessene Online-Verhalten kann der Reputation des Unternehmens beschädigen.

Chapter 15

1. Explain the difference between a security audit message and a security alarm.

Die Logik eingebettet in die Software (=**event discriminator**) des Systems die Systemaktivitäten überwacht, **sendet Audit-Einträge zum Audit Recorder für jedes Ereignis,** das entdeckt worden ist. **Einige** der entdeckten Ereignisse **werden** definiert, um **Alarmereignisse** zu sein. Für solche Ereignisse **wird** ein **Alarm** an einen **Alarm-Prozessor ausgegeben**, der eine Aktionen nimmt basierend auf der Alarm.

2. List and briefly describe the elements of a security audit and alarms model.

Event discriminator: erkennt sicherheitsrelevante Ereignisse
Audit recorder: zeichnet die Ereignisse auf, die vom Diskriminator gegeben werden
Alarm processor: ergreift Maßnahmen, wenn eine Alarmmeldung ausgegeben wird
Security audit trail: das Audit-Recorder erzeugt eine formatierte record für jedes event und speichert es in der Security Audit Trail
Audit analyzer: analysiert, dass trail und kann eine neues überwachbares Ereignis basierend auf den observed patterns erstellen
Audit archiver: speichert alle audits dauerhaft im **Archiv**
Audit provider: Eine application oder user interface für den Audit-Trail
Audit trail examiner: Eine application oder ein Benutzer, der das Audit-Trail und Archive für die historische Trends, Computer forensische Zwecke und für andere Analysen untersucht
Security reports: erstellt vom audit trail examiner in human-readable form.

3. List and briefly describe the principal security auditing functions.

Data generation: Audit data generation, User identity association
Event selection: Ermöglicht dem System auf verschiedenen Ebenen der Granularität konfiguriert werden
Event storage: Erstellung und Pflege von security audit trail.
Automatic response: Definiert Reaktionen getroffen anschließend Erkennung von Ereignissen
Audit analysis: Mögliche Verletzung Analyse und Angriff Heuristiken via automatisierte Mechanismen
Audit review: Verfügbar für den Menschen zum unterstützen in der Audit-Data-Review.

4. In what areas (categories of data) should audit data be collected?

Ereignisse im Zusammenhang mit der **Verwendung der Auditing-Software oder Security-Mechanismen** auf dem System, **Ereignisse, die für die Nutzung durch die verschiedenen Sicherheits-Erkennung und Verhinderung von Mechanismen gesammelt werden, System Calls,** Anwendungs**zugriff für ausgewählte Anwendungen, Remote-Zugriff.**

5. List and explain the differences among four different categories of audit trails.

System-Level: sollte erfassen Daten wie **Login-Versuche**, beide erfolgreiche und erfolglose, **devices used** and **OS functions performed**; andere Daten können aufgenommen werden wie zB **system operation** und **network performance indicators**
Application-Level: Kann verwendet werden, um **Verletzungen der Sicherheit innerhalb einer Anwendung** oder **Mängel in der Anwendung Interaktion mit dem System** zu **erkennen** , zB. eine E-Mail-Anwendung aufzeichnen können Absender, Empfänger, Nachrichtengröße und Arten von Anhängen.
User-Level: **Spuren die Aktivität der einzelnen Nutzer** im Laufe der Zeit wie zB **Befehle erteilt, Identifizierung und Authentifizierung Versuche und Dateien und Ressourcen eingesehen**. Nützlich zu **halten** einen **Benutzer die Verantwortung** für seine Handlungen **oder** als **Eingang zu einem Analyse-Programm** in den normalen oder anormalen Verhalten zu definieren.
...

...Physical Access: Record physischen Zugriff Ereignisse. Beispiele sind **Karten schlüsselfertige Systeme** oder Alarmanlagen. Es sollte protokolliert, wenn eine Person Zugriff auf das Gebäude etc. werden

6. What are the main elements of a UNIX syslog facility?

Ein **API (syslog ())** verfügbar für Anwendungsprogramme, einem **Befehl (Logger)** verwendet, um Single-**Line-Einträge** in der System-Log hinzuzufügen, einer **Konfigurationsdatei** und das **System-Daemon (syslogd)** zum Empfangen und Streckennetz log Ereignisse.
Zusätzliche Features / Pakete sind verfügbar: Robust Filterung, Log-Analyse, Event Antwort, Alternative-Nachrichtenformate, Log-Datei-Verschlüsselung, Datenbank-Storage für logs, Rate Limiting

7. Explain how an interposable library can be used for application-level auditing.

Mit Bibliothek Interpolation wird eine spezielle **interposable library konstruiert,** so dass bei der Ladenzeit, **Programm verlinkt zu** dem interposable library anstelle der gemeinsamen Bibliothek. Die zwischengeschaltet **Modul kann jede auditing-bezogenen Funktion durchführen**, wie die **recording the fact of the call**,die **Parameter bestanden** und kehrten zurück, die Absenderadresse in das aufrufende Programm **usw**.

8. Explain the difference between audit review and audit analysis.

Eine **audit review** ermöglicht einen **Administrator Informationen aus ausgewählten Audit-Protokolle zu lesen**. Audit review **kann** auf Datensätze, die mit bestimmten Attribute übereinstimmen, fokussiert werden, wie z. B. Benutzer oder Gruppe, Zeitfenster, Art der Aufzeichnung usw.
Die einfachste der Analyse ist für die Software **einen Hinweis, dass ein besonders interessantes Ereignis aufgetreten ist (= alerting) zu geben.** Ein weiterer Teil ist **Baselining**. Es ist der Prozess des **Definierens normalen gegenüber ungewöhnliches Ereignis und Mustern.** Eg. eine starke Zunahme des FTP-Verkehrs könnte hindeuten, dass Ihr FTP-Server kompromittiert wurde. **Korrelation** ist eine Art von Analyse, die **nach Beziehungen zwischen Ereignissen** sucht.

9. What is a security information and event management (SIEM) system?

SIEM-Software ist ein **Logging-Software-Paket** ähnlich wie syslog. SIEM-Systeme **bieten ein** zentralisiertes, einheitliches **Audit-Trail-Storage facility und** eine Reihe von **Audit-Daten-Analyse-Programme.** Sie sind in der Lage, **eine Vielzahl von Log-Formate**, Sicherheitssoftware und Applikationsservern zu erkennen. Normalerweise sind sie mit **GUI**, ein **Sicherheits-Wissensbasis** und **Incident-Tracking-und Reporting-capabilities.**

Chapter 16

1. Define *IT security management*.

Ein Verfahren benutzt zur Erreichung und Aufrechterhaltung eines angemessenen Levels der **Vertraulichkeit, Integrität, Verfügbarkeit, Verantwortung, Authentizität und Zuverlässigkeit.**

2. List the three fundamental questions IT security tries to address.

Welche Vermögenswerte müssen wir schützen?
Wie werden diese Vermögenswerte bedroht?
Was können wir tun, um den Bedrohungen entgegen zu halten?

3. List the steps in the process used to address the three fundamental questions.

Ermitteln Sie zunächst, eine **klare Sicht einer Organisation der IT-Sicherheit objektive** und allgemeine Risikoprofil. Als Nächstes wird ein **IT-Sicherheit Risikobewertung für jedes Vermögen** in der Organisation, die den Schutz erfordert, benötigt. Diese Einschätzung **liefert die notwendigen Informationen, um zu entscheiden, welche Ressourcen benötigt** werden, zu reduzieren oder zu eliminieren die Risiken.

4. List some of the key national and international standards that provide guidance on IT security management and risk assessment.

ISO27000-ISO27005 and *ISO13335*

5. List and briefly define the four steps in the iterative security management process.

Plan: Schaffung eines Gemeinwesens, Ziele usw. für das Risikomanagement
Do: Umsetzung und in Betriebnahme der Sicherheitspolitik
Check: Beurteilung und Messung der Leistung
Act: Ergreifung Korrektur-und Vorbeugungsmaßnahmen

6. Organizational security objectives identify what IT security outcomes are desired, based in part on the role and importance of the IT systems in the organization. List some questions that help clarify these issues.

Welche wichtigen Aspekte der Organisation, die IT-Unterstützung erfordern?
Welche Aufgaben können nur mit IT-Unterstützung durchgeführt werden?
Welche Daten erstellt, verwaltet, bearbeitet und gespeicherte durch das IT-System brauchen Schutz?
Was sind die Folgen eines Sicherheitsfehlers?

7. List and briefly define the four approaches to identifying and migration IT risks.

Baseline approach: Zielt auf eine **grundlegende allgemeine Niveau der Sicherheit**skontrollen mit **Baseline Dokumente, Verhaltenskodizes** und I**ndustrie Best Practices** zu implementieren.
Vorteil: erfordert nicht die Ausgaben von zusätzlichen Ressourcen in der Risikobewertung.
Nachteil: **keine besondere Beachtung** wird, **um Variationen** in der Organisation Risiko gegeben.
Die Baseline-Ansatz ist **nur für kleine Organisationen empfohlen.**
Informal approach:Umfasst die Durchführung irgendeine Form von **informellen, pragmatische Risikoanalyse** und basiert auf dem Wissen von i**nternen Experten oder Beratern,** die die Durchführung der Analyse beruhen. Dieser Ansatz kann sich auf mehr Aspekte als die Baseline approach, sondern weil ein förmliches Verfahren nicht verwendet wird, **einige Risiken können nicht berücksichtigt werden.**
Detailed risk analysis: Eine detaillierte Risikobewertung, unter Verwendung eines f**ormalen strukturierten Prozess,** bietet **größtmögliche Sicherheit**, dass alle Risiken erkannt. **Erhebliche Kosten** an Zeit und Ressourcen.
Combined approach: kombiniert Elemente aus den anderen Ansätzen

8. Which of the four approaches for identifying and migrating IT risks does [ISO13335] suggest in the most cost effective for most organizations?

The **combined approach**.

9. List the steps in the detailed security risk analysis process.

System Charakterisierung, Threat Identifikation, Schwachstellen Identifikation, Control analysis Likelihood determination, Impact-Analyse, Risk determination, Control recommendations, Ergebnisse Dokumentationen.

10. Define *asset, control, threat, vulnerability* and *risk.*

Asset: alles, was einen Wert für die Organisation hat
Threat: eine mögliche Ursache für eine unerwünschte Ereignis, das zu einem Schaden für die Organisation führen kann
Vulnerability: eine Schwäche in einem Vermögenswert, der durch eine Bedrohung ausgenutzt werden kann.
Risk: die Möglichkeit, dass eine bestimmte Bedrohung Schwachstellen eines Vermögenswertes ausnutzen wird um den Verlust oder die Beschädigung der Anlage führen.

11. State the two key questions answered to help identify threats and risks for an asset. Briefly indicate how these questions are answered.

- Wer oder was könnte der Anlage schaden?
Eine Bedrohung kann entweder **natürlich** oder **von Menschen gemacht** sein und kann **versehentliche oder absichtliche** sein. Alles, was einen **Vermögenswert verhindert die Bereitstellung** geeigneter Ebenen der **Vertraulichkeit, Integrität oder Verfügbarkeit** ist eine Bedrohung.

- Wie konnte das geschehen?
Beantwortung dieser, beinhaltet die **Ermittlung Mängel oder Schwächen in den Organisationen IT-Systeme** dass könnte durch eine Bedrohung ausgenutzt werden.

12. Define *likelihood* and *consequence.*

Likelihood ist die Wahrscheinlichkeit eines Ereignisses stattfindet. Die Wahrscheinlichkeit für eine Bedrohung auftreten wird typischerweise qualitativ mit Worten wie selten - unwahrscheinlich - möglich – wahrscheinlich – fast sicher beschrieben.
Consequence: Der Analytiker muss dann die Folgen durch das Eintreten einer spezifischen Bedrohung spezifizieren und die entsprechenden Reaktionen in Betracht ziehen; minor - moderate - major - katastrophale

13. What is the simple equation for determining risk? Why is this equation not commonly used in practice?

Risiko = (Wahrscheinlichkeit, dass Bedrohung eintritt) x **(Organisatiokosten)**
In Wirklichkeit ist es oft schwer, genaue Wahrscheinlichkeiten, realistische Kosten Konsequenzen oder beide zu bestimmen. Somit sind die meisten Risikoanalysen verwenden qualitative Bewertungen für diese beiden Elemente.
low – medium – high – extreme

14. What are the items specified in the risk register for each asset/threat identified?

Existing Controls, Likelihood, Consequence, Level of risk, Risk priority

15. List and briefly define the five alternatives for treating identified risks.

Risk acceptance
Risk avoidance (nicht fortfahren mit der Tätigkeit, die dieses Risiko erstellt)
Risk transferal (Teilung der Verantwortung für das Risiko mit einem Dritten, zB. Versicherung)
Reduce the consequence (Veränderung der Struktur, um Auswirkungen zu verringern, zB. Off-site Backup, Disaster Recovery Plan)
Reduce the likelihood (Umsetzung geeigneter Kontrollen, zB. Einsatz Firewalls und Zugangs-Token)

Chapter 17

1. Define *security control* and *safeguard*.

Safeguards oder security control sind Praktiken, **Verfahren** oder Mechanismen, die **gegen** eine **Bedrohung zu schützen,** die **Schwachstellen verringern, begrenze die Auswirkung** eines unerwünschten Ereignisses, erkennen unerwünschte Zwischenfälle und **erleichtern Wiederherstellung.**

2. List and briefly define the three broad classes of controls and the three categories each can include.

Management control: **Fokus auf** Sicherheitsrichtlinien, **Planung und** Standards, die die **Auswahl von operativen und technischen Kontrolle**n beeinflussen. Deren Kontrollen beziehen sich auf Issues Management muss angesprochen werden.
Operational: Adresse die **korrekte Umsetzung** und Anwendung von Sicherheitsrichtlinien.
Technical controls: Beziehen Sie die korrekte **Verwendung von Hardware und Software Sicherheitsfunktionen** in Systemen.

3. List a specific example of each of the three broad *classes of controls* from those given in Table 17.3.

Management control: Risk Assessment, Planning, System and Services Acquisition, Security Assessments.
Operational: Personnel Security, Physical Protection, Contingency Planning, Maintenance, Incident Response, Awareness and Training
Technical: Identification and Authentication, Access Control, Audit, System and Communications Protection

4. List the steps [NIST02] specifies for selecting and implementing controls.

Prioritize Actions, Evaluate Recommended Control Options, Conduct Cost-Benefit Analysis, Select Controls, Assign Responsibility, Develop Safeguard Implementation Plan, Implement Selected Controls

5. List three ways that implementing a new or enhanced control can reduce the residual level of risk.

Es kann das Restrisiko reduzieren:
- **Verringerung** der Anzahl der **Mängel oder Fehler**
- **Hinzufügen** einer gezielten **Steuerung**
- **Verringerung** der Stärke des **Anschlags**

6. List the items that should be included in an IT security implementation plan.

- **Risiken** (assets / threats / Schwachstelle Kombination)
- **Empfohlene Kontrollen** (aus der Risikobewertung)
- **Action Priorität für jedes Risiko**
- **Ausgewählte Kontrollen** (auf der Grundlage der Kosten / Nutzen-Analyse)
- **Die benötigten Ressourcen f**ür die Umsetzung der ausgewählten Steuerelemente
- **Verantwortlich Personal**
- **Target Start-und Enddatum für die Umsetzung**
- **Wartungsaufwand** und andere Kommentare

7. List and briefly define the elements from the **implementation of controls** phase of IT security management.

Implementierung von Security Plan (kann Systemkonfiguration Änderungen, Upgrades, neue System-Installation, Entwicklung neuer Verfahren zu dokumentieren Praktiken erfordern)
Security Training (für Personal verantwortlich)
Security Awareness (allgemeines Sicherheitstraining für alle Mitarbeiter, einschließlich Workshops etc., um die Notwendigkeit für die Sicherheit und das Bewusstsein zu erklären)

8. List and briefly define the elements from the implementation of follow-up phase of IT security management.

Maintenance of security controls (sicherstellen, dass die Kontrollen, wie vorgesehen weiterlaufen)
Security Compliance Checking (Überprüfung der Einhaltung der Sicherheits-Plan)
Change und Configuration Management (zur vorgeschlagenen Änderungen des Systems überprüfen)
Incident Handling (Entwicklung von Verfahren verwendet um auf Sicherheitsvorfälle zu reagieren)

9. What are the benefits of developing an incident response team.

Das Antwortteam muss **kritische Entscheidungen über wesentliche Maßnahmen treffen**. Die Politik sollte festlegen **wie man die Verantwortlichen kontaktiert**. Eg. Wenn ein E-Mail-Wurm in der Firma ist, kann die E-Mail-Server heruntergefahren werden. Dies kann die Ausbreitung des Wurms stoppen, sondern auch einen großen Verlust der Systeme Funktionalität verursachen .

10. List the broad categories of security incidents.

- Ablehnung von Service-Attacken
- **Bösartiger Code**, der einen Host infiziert
- Unberechtigter Zugriff auf ein System
- Unangemessene Nutzung eines Systems
- Multi-Komponenten-Vorfälle zwei oder mehr der oben genannten Kategorien sind involviert

11. List some types of tools used to detect and respond to incidents.

System integrity verification tools, Log analysis tools, Network and host intrusion detection systems, Intrusion prevention systems

12. What should occur following the handling of an incident with regard to the overall IT security management process?

Identifizieren Sie, welche Schwachstelle führte zum Eintritt des Ereignisses und **wie** sich dies angesprochen, um den Vorfall **in der Zukunft zu verhindern**. Dies beinhaltet typischerweise **Fütterung der** gesammelte **Information** als Ergebnis des **Vorfalls zurück zu einer früheren Phase des IT-Sicherheits-Management-Prozess**.

Chapter 18

1. Describe a classification of computer crime based on the role that the computer plays in the criminal activity.

Computer als Ziele: zB. **Erschließung von Informationen** auf einem Computer gespeichert sind, um das **Zielsystem** (jeweils ohne Erlaubnis) zu **steuern** oder um die **Integrität der Daten zu ändern,** oder die **Zusammenarbeit mit der Verfügbarkeit** des Computers.
Computer als Speichergeräte: zB. **gestohlen Passwort-Listen speichern, Kreditkartennummern**, pornographische Bilddateien, warez.
Computer als Kommunikationsmittel: Verbrechen, die online begangen worden sind wie illegalen Verkauf von verschreibungspflichtigen Medikamenten, die geregelte Stoffe, Waffen; Betrug, Glücksspiel usw.

2. Define three types of property.

Immobilien (Grundstücke und Dinge an Land: Bäume, Gebäude)
Persönliches Eigentum (bewegliche Sachen wie Autos, Bankkonten, Versicherungen, Haustiere)
Geistiges Eigentum (alle immateriellen Vermögenswertes, der menschlichen Wissen und Ideen besteht: Software, Daten, Tonaufnahmen, die Gestaltung eines neuen Mausefalle, ein Heilmittel für eine Krankheit)

3. Define three types of intellectual property.

Urheberrecht: Das Urheberrecht schützt die **materielle oder festen Ausdruck einer Idee.**
Trademarks: Eine Marke ist ein Wort, einen Namen oder ein Symbol, im Handel mit Gütern verwendet wird, um die Herkunft der Waren zu kennzeichnen und sie von den Waren anderer zu unterscheiden.
Markenrechte können verwendet werden, um andere von der Nutzung eines ähnlichen Marke zu verhindern.
Patente: ist die Gewährung eines Rechts auf Eigentum an den Erfinder. **Das Recht, anderen die Herstellung, Gebrauch, Anbieten zum Verkauf oder Verkauf der Erfindung auszuschließen.**

4. What are the basic conditions the must be fulfilled to claim a copyright?

- Die vorgeschlagene Arbeit ist ein Original.
- Der Schöpfer hat diese Idee in eine konkrete Form, wie Hardcopy (Papier), Software oder multimediale Form zu bringen.

5. What rights does a copyright confer?

Reproduction right, **Modification** right **Distribution** right
Public-performance right
Public-display right

6. Briefly describe the Digital Millennium Copyright Act.

Der DMCA **stärkt den Schutz von urheberrechtlich geschütztem Material in digitaler Form.** Es fördert Urheberrechtsinhaber auf technische Maßnahmen, um urheberrechtlich geschützte Werke zu schützen.
2-Maßnahmen, um **Zugang** zum Arbeitsbereich zu **verhindern**, um zu **verhindern**, das **Kopieren** der Arbeit. Umgehung dieser Maßnahmen wird auch durch das Gesetz verboten.

7. What is the digital rights management?

Er bezieht sich auf Systeme, die gewährleisten, dass die **Inhaber von digitalen Rechte eindeutig identifiziert und erhalten** ihre Bezahlung für ihre Werke. Das System **kann weitere Beschränkungen** wie das Verbot weitere Verbreitung. Das Hauptziel ist es, **konsistente Inhalte Schutz vor unbefugtem Zugang zu digitalen Inhalten zu geben.** Es gibt keine einzelne DRM-Standard.

8. Describe the principal categories of users of digital rights managements systems.

Content-Provider: Hält die digitalen Rechte an den Inhalten, zB. ein Musik Label.
Distributor: bietet Vertriebskanäle, wie zum Beispiel einen Online-Shop
Consumer: nutzt das System, um die digitalen Inhalte durch Abrufen herunterladbare Inhalte über den Vertriebskanal zugreifen und dann die Zahlung für die digitale Lizenz.
Clearinghouse: Behandelt das Finanzgeschäft für die Erteilung der digitale Lizenz an den Kunden und zahlt den Content-Provider sowie die Händler.

9. What are the key principles embodies in the EU Directive on Data Protection?

Hinweis: Organisationen mitteilen muss, welche persönlichen Daten sie sammeln und warum Consent: Der Einzelne muss in der Lage sein zu entscheiden, ob und wie ihre persönlichen Daten verwendet wird, oder offenbart, Dritte.
Konsistenz: Organisationen können persönliche Informationen nur in der Weise durch den Gegenstand erlaubt ist.
Access: Individuelle müssen Zugang zu ihren Informationen und die Möglichkeit, ihn zu ändern haben.
Security: Unternehmen müssen geeignete Sicherheit.
Onward transfer: Dritte muss auch das gleiche Maß an Sicherheit.
Durchsetzung: Die Richtlinie gewährt eine private Klagerecht für Einzelpersonen, wenn Organisationen folgen nicht dem Gesetz.

10. What functions can a professional code of conduct serve to fulfill?

inspirierend Funktionen, Bildungs-, Unterstützung für eine professionelle **Entscheidung, ein Mittel der Abschreckung und Disziplin** sein kann**, kann verbessern die Berufe in der Öffentlichkeit**

(inspirational functions, educational, provide support for a professional decision, can be a means of deterrence and discipline, can enhance the profession's public image)