Nennen Sie die Grundfunktionen vertrauenswürdiger Systeme. (5 Punkte)

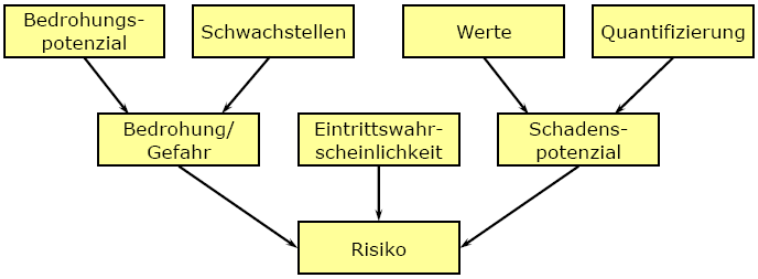
Kapitel 6, S. 2

- **Identifikation**: Bestimmung der Identität eines Subjektes
- **Authentisierung**: Nachweis einer angegebenen Identität oder Gruppenzugehörigkeit eines Subjektes
- **Rechteverwaltung**: Verwaltung der Rechtebeziehung zwischen Subjekten und Objekten
- **Rechteprüfung**: Überprüfung ob ein bestimmtes Subjekt die Berechtigung hat, in der beabsichtigten Art auf das gewünschte Objekt zuzugreifen
- **Beweissicherung**: Verstöße gegen die Sicherheitspolitik sollten zumindest nachträglich nachgewiesen werden können

Erläutern Sie was unter dem Risiko einer Bedrohung zu verstehen ist. (6 Punkte)

Kapitel 2, S. 6

Unter dem Risiko einer Bedrohung verstehen wir die Wahrscheinlichkeit des Eintritts eines Schadensereignisses und die Höhe des potentiellen Schadens, der dadurch hervorgerufen werden kann.



Erläutern Sie die Probleme symmetrischer Verschlüsselungssysteme. (6 Punkte)

Kapitel 4, S. 13f

- Wurde der Schlüssel aufgedeckt, können alle verfügbaren Nachrichten durch nicht autorisierte Personen entschlüsselt werden, bzw. ungültige Nachrichten produziert werden.
- Die Verteilung eines neuen Schlüssels muss unter maximalen Sicherheitsvorkehrungen geschehen (sicherer Kanal).
- Jeder Teilnehmer kann sowohl ver- als auch entschlüsseln. Er könnte sich daher unter dem Namen seines Partners eine fingierte Nachricht schicken. Dieser hat keine Möglichkeit zu beweisen, dass die Nachricht nicht von ihm stammt. Umgekehrt kann ein Sender nicht beweisen, dass er eine Nachricht abgeschickt hat.
- Da zwischen allen Personen, welche verschlüsselte Informationen austauschen wollen, eigene Schlüssel existieren müssen, wächst die Anzahl der Schlüssel rapide mit der Anzahl der Personen, welche Nachrichten austauschen.

Digitale Signaturen sind das elektronische Analogon zur eigenhändigen Unterschrift. Welche Funktionen besitzen eigenhändige Unterschriften? Nennen und erläutern Sie diese kurz. (15 Punkte)

Kapitel 4, S. 32

- Die **Echtheitsfunktion** besagt, dass das unterzeichnete Dokument dem Aussteller vorgelegen hat und von ihm anerkannt wurde.
- Die **Identitätsfunktion** besagt, dass die Unterschrift durch ihre Personenabhängigkeit die Identität des Ausstellers der Urkunde deutlich macht.
- Die **Abschlussfunktion** liegt darin, dass sie den Abschluss bzw. die Vollendung der Erklärung zum Ausdruck bringt und vom bloßen Entwurf abhebt.
- Die **Warnfunktion** hat den Schutz des Unterzeichners vor Übereilung zum Inhalt. Sie soll dem Unterzeichner die Relevanz des Unterschreibens bewusst machen.
- Die **Beweisfunktion** soll dem Träger der Beweislast in einem evtl. folgenden Streitfall die Beweisführung über das Vereinbarte erleichtern.

Warum hängt die Risikobewertung sehr stark von dem zugrunde liegenden Angreifermodell ab? (7 Punkte)

Kapitel 8, Teil 1, S. 30f

- Eintrittswahrscheinlichkeit ergibt sich aus
  - geschätztem Aufwand für den Angreifer
  - Einschätzung des möglichen Nutzens für den Angreifer bei erfolgreichem Angriff
  - Einschätzung der möglichen Motive eines Angreifers
- Risikobewertung hängt sehr stark von dem zugrundeliegenden Angreifermodell ab
- Angreifermodell enthält u.a.
  - Angreifertyp (Skript Kidie, Hacker, Mitarbeiter, Wirtschaftsspion)
  - das zur Verfügung stehende Finanzbudget
  - Kenntnisse (nicht vorhandene – Insider Wissen)
  - Ziele (z.B. Neugier, reines Gewinnstreben, Rache)

Welche Angaben enthält ein Zertifikat für die Zertifizierung des öffentlichen Schlüssels bei Digitalen Signaturen? (10 Punkte)

Kapitel 4, S. 41

- Name des Zertifikatsinhabers
- Öffentlicher Schlüssel des Zertifikatinahbers
- Authentifikationsalgorithmus des Zertifikatinhabers
- Name der Zertifizierungsinstanz
- Gültigkeitszeitraum

Erläutern Sie die Aufgabe eines Datenschutzbeauftragten im Unternehmen. (6 Punkte)

Kapitel 9, Teil 2, S. 45

Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriten über den Datenschutz hin. Er hat insbesondere

- die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen.
- die bei der Verwendung personenbezogenen Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

Security Engineering. Nennen Sie die allgemeinen Konstruktionsprinzipien und erläutern Sie zwei davon. (12 Punkte)

Kapitel 8, Teil 1, S. 5

- Erlaubnisprinzip: grundsätzlich ist verboten was nicht erlaubt ist
- Vollständigkeit: jeder Zugriff ist auf seine Zulässigkeit zu prüfen
- Need-to-know: Prinzip der minimalen Rechte
- Akzeptanz: Benutzerakzeptanz
- Offener Entwurf: no security through obscurity
- Sicherheitskern

Erläutern Sie folgende Begriffe: Vertraulichkeit, Verfügbarkeit. (6 Punkte)

Kapitel 2, S. 5

- Vertraulichkeit: nur autorisierte Benutzer dürfen lesenden Zugriff auf das Sicherheitsobjekt erlangen
- Verfügbarkeit: jedes dazu berechtigte Subjekt kann in vorgegebener Art und Weise und zu jedem vorgesehenen Zeitpunkt das Objekt benutzen

Erläutern Sie die Begriffe Integrität und Anonymität. (6 Punkte)

Kapitel 2, S. 5

- Integrität: das Sicherheitsobjekt darf nur von dazu berechtigten Subjekten in vorgegebener Weise verändert werden
- Anonymität: die wahre Identität des Objekts bleibt verborgen

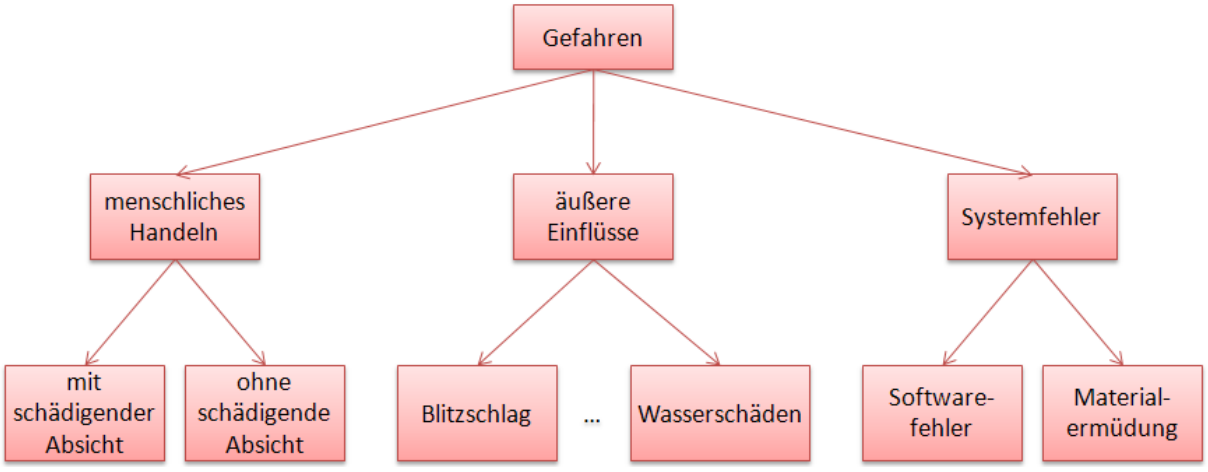
Eine Grundfunktion vertrauenswürdiger Systeme ist die Beweissicherung. Erläutern Sie diese und gehen Sie dabei insbesondere auf die Problematik der Körnung der Subjekte und Objekte ein! (12 Punkte)

Kapitel 6, S. 25ff

- Protokolle der Beweissicherung enthalten Informationen darüber, welche Subjekte zu welchem Zeitpunkt auf welche Art und Weise auf welche Objekte zugegriffen haben bzw. zuzugreifen versucht haben
  - Ergebnisprotokolle: enthalten Aufzeichnungen der betroffenen Daten vor und nach dem Zugriff
  - Ereignisprotokolle: enthalten Aufzeichnungen der Aktionen, die auf Daten ausgeführt werden, sowie Parameter dieser Aktionen
- Protokollinhalte (Fragen die zu beantworten sind)
  - Zugriffsart: befugte und unbefugte Zugriffe / nur unbefugte Zugriffe
  - Aktionen: alle Aktionen / ausgewählte (z.B. nur schreibende) Aktionen
  - Schutzobjekte: alle Datenobjekte / nur ausgewählte Datenobjekte
  - Subjekte: alle Subjekte / priviligierte Subjekte / Stichproben
  - Zeitpunkt des Zugriffs: Datum / Datum + Uhrzeit
  - Login: erfolgreiche Versuche / fehlgeschlagene Versuche / erfolgreiche Versuche nach wievielen fehlgeschlagenen Versuchen (auf keinen Fall dürfen Paswörter und andere Authentifikationsmittel mitprotokolliert werden)
  - Protokollierung: automatisch / ständig / manuell zuschaltbar (durch wen?) / automatisch zuschaltbar beim Eintritt bestimmter Ereignisse
  - Archivierung der Protokolldaten

Welche Gefahrenquellen unterscheidet man bei Betrachtung der Sicherheit von IT-Systemen? Nennen und erläutern Sie diese! (9 Punkte)

Kapitel 2, S. 2



Erläutern Sie detailliert das Vorgehen bei der vertraulichen elektronischen Verwendung der asymmetrischen Verschlüsselung! Erläutern Sie dabei auch, warum die digitale Signierung vor der Verschlüsselung auf Grund der Gewährleistung der Vertraulichkeit erfolgt? (20 Punkte)

Kapitel 4, S. 15

- Jeder Benutzer hat einen Schlüssel (public key), den er der Öffentlichkeit zur Verfügung stellt und einen geheimen Schlüssel (private key).
- Der Benutzer kann mit seinem privaten Schlüssel Nachrichten entschlüsseln, welche von einem anderen mit dem public key verschlüsselt wurden. Wird der public key mit k_{pub} und der private key mit k_{priv} bezeichnet, dann gilt: $P = D(k_{priv}, E(k_{pub}, P))$. Damit werden für jeden Benutzer nur noch zwei Schlüssel benötigt.
- Verschickt Benutzer A eine Nachricht mit seinem privaten Schlüssel, so kann die Nachricht von anderen Benutzern mit seinem öffentlichen Schlüssel entschlüsselt werden: $P = D(k_{pub}, E(k_{priv}, P))$.

Kapitel 4, S. 37ff

- durch asymmetrische Verschlüsselungsverfahren lassen sich die folgenden Funktionen erfüllen:
  - Vertraulichkeit der Nachricht (optional bei digitaler Signatur)
    - A verschlüsselt Dokument mit öffentlichem Schlüssel von B
    - zum Entschlüsseln wird der private Schlüssel von B benötigt
    - nur B kann Dokument entschlüsseln
    - *Vertraulichkeit* durch Einzigartigkeit des privaten Schlüssels
  - Authentizität des Senders (zwingend bei digitaler Signatur)
    - A signiert Dokument mit seinem privaten Schlüssel
    - zum Entschlüsseln wird der öffentliche Schlüssel von A benötigt
    - jeder kann entschlüsseln, aber A ist der einzige, der signieren konnte
    - Authentizität durch Einzigartigkeit des privaten Schlüssels

Nennen Sie den Unterschied zwischen deutschen und europäischen Datenschutzrichtlinien! (6 Punkte)

Kapitel 9, Teil 2

Die europäischen Datenschutzrichtlinien legen die Rahmenbedingungen für alle Mitlgiedsländer der EU fest. Die einzelnen Länder konretisieren diese in eigenen, länderspezifischen Datenschutzrichtlinien. Diese sind konkreter und richten sich zusätzlich an die Anforderungen in den entsprechenden Ländern.

Was muss man tun, um die Vertrauenswürdigkeit eines IT-Produktes oder IT-Systems prüfen oder bescheinigen lassen will? (5 Punkte)

Kapitel 7, S. 1f

- ein Anwender, der ein sicheres IT-Produkt oder –System einsetzen will, hat folgende Möglichkeiten:
  - er glaubt und vertraut den Beteuerungen und Versprechen der Hersteller (Vorsicht!)
  - er prüft die Sicherheit der zur Auswahl stehenden IT-Produkte und –Systeme selbst (erhebliche Kosten, Fachwissen)
  - Prüfung (Evaluation) und Bescheinigung (Zertifikation) von Sicherheitseigenschaften durch eine (oder mehrere) unabhängige Drittinstanz(en) → ausgestelltes Zertifikat stellt eine Beglaubigung von Sicherheitseigenschaften dar, wodurch auch ohne Preisgabe von vertraulichen Informationen Vertrauen beim Anwender geschaffen werden kann
- zur Prüfung und Bescheinigung der Vertrauenswürdigkeit eines IT-Produkts werden entsprechende Sicherheitskriterien (security criteria) als objektive Bewertungsgrundlage benötigt, welche üblicherweise in Form von Kriterienkatalogen publiziert werden

Erläutern Sie den Unterschied zwischen den Ausübungsformen Hauptamtlicher, Nebenamtlicher und Externe Datenschutzbeauftragter. (9 Punkte)

Kapitel 9, Teil 2, S. 46

- hauptamtlicher Datenschutzbeauftragter
  - Vorteile: hohe Fachkunde, keine Interessenskollision, hoher innerbetrieblicher Bekanntheitsgrad, informelle Organisation ist bekannt
  - Nachteile: nur ab bestimmter Größe der Institution wirtschaftlich vertretber
- Nebenamtlicher Datenschutzbeauftragter
  - Vorteile: wirtschaftlich günstige Lösung, in der Regel innerbetrieblich bekannt, informelle Organisation ist bekannt
  - Nachteile: in der Regel geringe bis keine Fachkunde, in der Regel besteht Zeitmangel, kann zu Interessenskonflikten kommen, problematischer Kündigungsschutz, langfristige Bindung
- Externer Datenschutzbeauftrager
  - Vorteile: sehr hohe Fachkunde, Praxiserfahrung auch aus Randgebieten, kein Kündigungsschutz, kurzfristig verfügbar, schwerpunktmäßig einsetzbar, Kosten sind kalkulierbar da Budgetierung, keine Nebenkosten für z.B. Weiterbildung
  - Nachteile: zunächst innerbetrieblich nicht bekannt, zunächst informelle Organisation nicht bekannt

Erklären Sie eine von drei Sicherheitspolitiken MAC, DAC oder RBAC (6 Punkte)

Kapitel 6, S. 4

- Diskrete Sicherheitspolitik (Discretionary Access Control, DAC)
  - für jedes Paar (Subjekt, Objekt) ist definiert, ob das Subjekt ein Zugriffsrecht auf das Objekt besitzt und welcher Art ein eventuelles Recht (Privileg) ist
  - die Speicherung erfolgt häufig in Form einer Zugriffskontrollmatrix

Kapitel 6, S. 17

- Politik der Schutzklassen (Mandatory Access Control, MAC)
  - Objekte und Subjekte sind mit Sicherheitsstufen ausgestattet
  - ein Subjekt darf auf ein Objekt zugreifen, wenn die Freigabe des Subjektes die Klassifikation der referenzierten Objekte dominiert: $clear(S) \geq class(O)$

Kapitel 6, S. 23

- Role-Based Access Control (RBAC)
  - Berechtigungen werden direkt an Rollen (und damit an Aufgaben) geknüpft
  - RBAC-Sicherheitsmodell legt fest, welche Subjekte welche Aufgaben durchführen, d.h. in welchen Rollen agieren
  - hierarchische, rollenbasierte Modelle

Erläutern Sie die Begriffe Authentisierung und Authentifizierungstechnik. (6 Punkte)

Kapitel 6, S. 2ff

- Eine Authentisierung meint den Prozess des Prüfens einer Identität. Hierbei soll geprüft werden ob das jeweilige Subjekt die Identität besitzt die es vorgibt zu haben. Im Sinne der Authentizität darf es sich hierbei (im Gegensatz zur Originalität) um eine Kopie handeln.
- Authentifizierungstechniken sind Verfahren anhand derer eine Authentizität nachgewiesen werden kann. In der Regel können sich Subjekte anhand 3 verschiedener Arten authentifizieren:
  - durch Wissen (z.B. durch Eingabe eines Passwortes)
  - durch Besitz (z.B. durch Eingabe einer Chipkarte)
  - durch persönliche Eigenschaften (z.B. durch Eingabe des Fingerabdrucks)
- Typische Authentifizierungstechniken sind: Passwortverfahren, Challenge-Response Verfahren, Zero-Knowledge-Verfahren, Public-Key-Verfahren, Besitzbasierende Verfahren, Biometrische Verfahren.

Erläutern Sie das Prinzip der Ver- und Entschlüsselung. (8 Punkte)

Kapitel 4, S. 4f

- Das System besteht aus einem Verschlüsselungsalgorithmus (Chiffrieralgorithmus), der die Transformation der ursprünglichen Nachricht (Klartext, plaintext) in eine für Unbefugte nicht verständliche Nachricht (Ciphertext, Chiffrat) vornimmt.
- Diese Transformation (Chiffrierung, encryption) kann genau wie der umgekehrte Vorgang (Dechiffrierung, decryption) von einem Parameter (Chiffrierschlüssel, Dechiffrierschlüssel) gesteuert werden.
- für die Darstellung in Formeln werden im allgemeinen die Abkürzungen der englischen Begriffe verwendet:
  - E für Encryption
  - D für Decryption
  - P für Plaintext
  - C für Ciphertext
  - K für Key
- manche Chiffriersysteme unterscheiden zwischen Chiffrierschlüssel (KE) und Dechiffrierschlüssel (KD)
- Wird der Klartext P unter dem Schlüssel K chiffriert, so stellt sich das Resultat als $C = E_K(P)$ dar. Der Klartext ergibt sich aus der Dechiffrierung von C: $P = D_K(C)$.

Was ist ein Zertifikat im Zusammenhang mit der digitalen Signatur und was sagt es aus? (4 Punkte)

Kapitel 4, S. 41

- Zertifikat = „digitaler Ausweis“
- stellt den Zusammenhang zwischen dem öffentlichen Schlüssel und einer bestimmten natürlichen oder juristischen Person dar
- beinhaltet Angaben über
  - Name des Zertifikatinhabers
  - öffentlicher Schlüssel des Zertifikatinhabers
  - Authentifikationsalgorithmus des Zertifikatinhabers
  - Name der Zertifizierungsinstanz
  - Gültigkeitszeitraum …
- signiert mit dem privaten Schlüssel der Zertifizierungsstelle

Erläutern Sie die Schutzbedarfsermittlung nach BSI. (6 Punkte)

Kapitel 7, S. 9ff

- Zuordnung von Schutzkategorien mittels Schadensszenarien (was wäre wenn…)
- Schutzkategorien:
  - niedrig bis mittel: Schadensauswirkungen sind begrenzt und überschaubar
  - hoch: können beträchtlich sein
  - sehr hoch: können existenziell bedrohliches, katastrophales Ausmaß annehmen
- Schadensszenarien:
  - Schadensszenario 1: Verstoß gegen Gesetze / Vorschriften / Verträge
  - Schadensszenario 2: Beeinträchtigung der informationellen Selbstbestimmung
  - Schadensszenario 3: Beeinträchtigung der persönlichen Unversehrtheit
  - Schadensszenario 4: Beeinträchtigung der Aufgabenerfüllung
  - Schadensszenario 5: negative Auswirkungen
  - Schadensszenario 6: finanzielle Auswirkungen

Erläutern Sie die Role-Based Acces Control. (12 Punkte)

Kapitel 6, S. 23

- Berechtigungen werden direkt an Rollen (und damit an Aufgaben) geknüpft.
- RBAC-Sicherheitsmodell legt fest, welche Subjekte welche Aufgaben durchführen, d.h. in welchen Rollen sie agieren