

**SECURITY-Prüfung am 15.10.2004**

Name:

Matr.Nr.:

Kennzahl:

1.) Ein Sicherheitsmanagement in einem Unternehmen durchläuft mehrere Phasen mit einer üblichen Reihenfolge. Welche nachfolgend angegebenen Phasen sind in der Reihenfolge von oben nach unten richtig?

- a) Erstellung der Sicherheitspolitik
- b) Realisierung fehlender Maßnahmen
- c) Festlegung eines Sicherheitsmanagementteams
- d) Strukturanalyse (Erfassung der Komponenten und Anwendungen)
- e) Aufrechterhaltung im laufenden Betrieb
- f) Analyse (Soll-Ist-Vergleich etc.)
- g) Schutzbedarfsfeststellung

2.) Welche Aufgaben haben unter anderem Sicherheitszertifizierungen nach ITSEC oder Common Criteria und welche Angaben sind unten richtig:

- a) unabhängige Prüfung von realisierten Maßnahmen wie Identifikation, Authentifikation, Rechteverwaltung, Rechteprüfung etc.
- b) die Prüfung muss transparent und nachvollziehbar sein
- c) die Evaluierungen werden von akkreditierten Prüfstellen durchgeführt
- d) E1 (nach ITSEC) bzw. EAL2 (nach Common Criteria) sind sehr gute Ergebnisse
- e) E5 bzw. EAL 6 sind sehr gute Ergebnisse
- f) Der Prüfungsvorgang mit den entsprechenden Prüfkriterien ist aus Sicherheitsgründen geheim
- g) Hersteller von IT-Produkten erstellen Sicherheitszertifikate für ihre Produkte

3.) Was sind spezifische Eigenschaften der asymmetrischen Kryptografie?

- a) Der Ver- und Entschlüsselungsschlüssel sind identisch
- b) Der Schlüsselaustausch ist einfacher als bei der symmetrischen Kryptografie
- c) Die Schlüssel sind sehr lange (z.B. 1024 Bit)
- d) Der Ver- und Entschlüsselungsschlüssel sind verschieden
- e) Man kann sie für die Erzeugung der Digitalen Signatur verwenden
- f) Die Schlüssellänge wird häufig durch eine dreimalige Verwendung (Ver-/Ent-/Ver-Schlüsselung mit drei verschiedenen Schlüsseln) verdreifacht

4.) Welche nachfolgenden Angaben über biometrische Daten/Systeme im allgemeinen IT-Einsatz in Unternehmen sind richtig?

- a) ein System akzeptiert nur berechnigte Personen
- b) biometrische Systeme erreichen heute die aus erkennungsdienstlichen Anwendungen (z.B. Kriminalpolizei) bekannte Qualität
- c) Lebenderkennung ist kein Problem
- d) Biometrie kann eine Erhöhung des Komforts unter Wahrung des Sicherheitsniveaus bieten, wenn sie herkömmliche Methoden sinnvoll ergänzt
- e) heute werden sie vor allem in Identifikationsanwendungen eingesetzt
- f) im Hochsicherheitsbereich werden heute gerne DNA-Analysen eingesetzt
- g) die Vermessung der Handfläche mit gespreizten Fingern ist seit einiger Zeit vor allem im Zutrittsbereich im Einsatz
- h) ein System lehnt prinzipiell nur unberechnigte Personen ab

- 5.) Welche Eigenschaften / Vorsichtsmaßnahmen soll ein gutes (sicheres) Passwort aufweisen und was soll der Benutzer dabei berücksichtigen?
- a) es soll möglichst kurz sein, damit man es sich leichter merkt
  - b) mit der Passworteingabe gibt man eine Willenserklärung ab
  - c) es soll ein Tastaturmuster enthalten (z.B acht nebeneinander liegende Tasten auf der Tastatur als Passwort)
  - d) es soll nur Buchstaben oder Ziffern enthalten
  - e) es soll aus einer Kombination aus Straßenbezeichnung und Hausnummer des Büros bestehen
  - f) es soll monatlich geändert werden
  - g) es soll auf einem Notizzettel notiert werden, damit man es nicht vergessen kann
  - h) es soll in das Eingabegerät geschützt eingegeben werden
  - i) es soll nicht gelöscht werden, wenn der Benutzer seine Benutzungsberechtigung verliert
  - j) wenn bei einem Benutzer die Eingabe eines richtigen Passwortes abgelehnt wird, soll er es sofort wieder versuchen und wenn es dann angenommen wird, er ohne Reaktion weiterarbeiten
  - k) es soll vor jeder neuen Passworteingabe die letzte erfolgreiche Passworteingabe mit Uhrzeit und Datum angezeigt werden
  - l) bei einem Passwortwechsel soll nicht eines der letzten drei gewählt werden
  - m) es soll aus Ergebnissen des aktuellen Sports codiert werden (z.B. Name und Punkte des Drittplazierten der höchsten spanischen Fußballliga)
  - n) es soll geschützt zur Passwort prüfenden Stelle übertragen werden
  - o) es soll im IT-System, wo die Überprüfung stattfindet, im Klartext abgespeichert sein
- 6.) Welche angegebenen Schutzmethoden eignen sich für den Softwareschutz vor Raubkopien?
- a) ständige Darstellung des Namens des SW-Lizenznehmers am Bildschirm
  - b) Firewall
  - c) keine Hotline
  - d) Dongle
  - e) Anpassung der Software an den Kunden (z.B. durch Parametrisierung)
  - f) Zusendung von kostenlosen Updates an den Kunden
  - g) sehr günstige Preise
- 7.) Ein in Word verfasstes Dokument soll mit einer digitalen Signatur versehen und dann an den Empfänger übertragen werden. Welche unten angegebenen Schritte müssen dabei auf der Senderseite unter anderem durchgeführt werden? Bitte genaue Reihenfolge von oben nach unten beachten!!!
- a) das Dokument wird mit dem öffentlichen Schlüssel verschlüsselt
  - b) die digitale Signatur des Dokumentes wird mit dem öffentlichen Schlüssel verschlüsselt
  - c) die händische Unterschrift wird eingescannt
  - d) die eingescannte händische Unterschrift wird mit dem geheimen Schlüssel verschlüsselt
  - e) das Dokument wird mit einer Hashfunktion komprimiert
  - f) das Dokument wird mit einer Hashfunktion entkomprimiert
  - g) das Dokument wird mit dem geheimen Schlüssel verschlüsselt
  - h) das Zertifikat wird mit dem geheimen Schlüssel verschlüsselt

- i) das Ergebnis der Hashfunktion wird mit dem geheimen Schlüssel verschlüsselt
- j) das Ergebnis der Hashfunktion wird mit dem öffentlichen Schlüssel verschlüsselt
- k) aus dem Dokument und den Schlüsseln wird ein Zertifikat erzeugt
- l) das Zertifikat wird mit dem geheimen Schlüssel verschlüsselt
- m) die Digitale Signatur ist das Ergebnis aus d)
- n) die Digitale Signatur ist das Ergebnis aus g)
- o) die Digitale Signatur ist das Ergebnis aus h)
- p) die Digitale Signatur ist das Ergebnis aus i)
- q) die Digitale Signatur ist das Ergebnis aus j)
- r) die Digitale Signatur ist das Ergebnis aus l)

8.) Welche Daten werden von elektronischen Authentifikationssystemen zur Auswertung der Handschrift ausgewertet?

- a) Anpressdruck des Schreibstiftes auf die Unterlage
- b) die Geschwindigkeit und Beschleunigung des Schreibstiftes während des Schreibvorganges
- c) die Länge des Schreibstiftes
- d) die Farbe der Schrift
- e) Aussehen (Erscheinungsbild) der Handschrift

9.) Was sollte man bei der Entlassung eines Mitarbeiters tun?

- a) Sofortige Abgabe aller Zutrittsschlüssel
- b) Nach dem Austritt aus der Firma für eine Stellvertretung zu sorgen
- c) Aufbau einer sehr guten Firmenkultur, um eventuelle Frustrationen zu senken
- d) Austritt aus der Firma bei vollem Lohn während der Kündigungsfrist
- e) Sperre der Benutzerberechtigungen nach Ablauf der Kündigungsfrist

10.) Welche Aufgaben soll eine IT-Sicherheitspolitik erfüllen?

- a) Beschreibung des Aufsichtsrates eines Unternehmens
- b) Darstellung der Aufgabenbereiche der Geschäftsführung
- c) Auflistung aller Kunden (Referenzliste)
- d) Berechtigungskonzept für die IT-Nutzung
- e) Stellenwert der IT-Sicherheit im Unternehmen
- f) Durchführung eines Soll-Ist-Vergleiches aller IT-Komponenten

11.) Abstrahlung eines PCs:

Warum kann ein PC mit einem herkömmlichen Bildschirm (mit Kathodenstrahlröhre) mehrere Räume entfernt oder von der Straße aus mit einer relativ einfachen Ausrüstung abgehört werden?

- a) weil der Phosphor am abzuhörenden Bildschirm gut nachleuchtet
- b) weil das Bild am abzuhörenden Bildschirm mindestens 50 mal pro Sekunde am Bildschirm wiederholt dargestellt wird
- c) weil jedes am abzuhörenden Bildschirm dargestellte Zeichen aus vielen einzelnen Punkten aufgebaut ist
- d) weil der abzuhörende Bildschirm eine Strahlung abgibt, die auch bei ausreichender Entfernung einfach zu empfangen ist
- e) weil die Buchstaben, Ziffern und Zeichen aus 8 Bit codiert sind