

SECURITY-Prüfung am 14.1.2005

Name: _____ Matr.Nr.: _____ Kennzahl: _____

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

- a) Der Prüfungsvorgang mit den entsprechenden Prüfkriterien ist aus Sicherheitsgründen geheim
- b) die Prüfung muss transparent und nachvollziehbar sein
- c) die Evaluierungen werden von akkreditierten Prüfstellen durchgeführt
- d) Hersteller von IT-Produkten erstellen Sicherheitszertifikate für ihre Produkte
- e) E2 (nach ITSEC) bzw. EAL3 (nach Common Criteria) sind sehr gute Ergebnisse
- f) unabhängige Prüfung von realisierten Maßnahmen wie Identifikation, Authentifikation, Rechteverwaltung, Rechteprüfung etc.

2.) Was sind spezifische Eigenschaften der symmetrischen Kryptografie?

- a) Der Ver- und Entschlüsselungsschlüssel sind verschieden
- b) Der Schlüsselaustausch ist einfacher als bei der asymmetrischen Kryptografie
- c) Die Schlüssel sind sehr lange (z.B. 1024 Bit)
- d) Der Ver- und Entschlüsselungsschlüssel sind gleich
- e) Man kann sie für die Erzeugung der Digitalen Signatur verwenden
- f) Durch ein Verfahren wie ECB (Electronic Codebook), das direkt die Datenblöcke verschlüsselt ohne Rückkopplung, können symmetrische Verfahren sicherer gemacht werden

3.) Welche Methoden / Maßnahmen sind für Passwörter aus Sicherheitsgründen ungeeignet?

- a) Eliminierung mehrerer Buchstaben eines längeren Wortes als Passwort
- b) Aushützung von Tastaturmustern als Passwort
- c) Notieren des Passwortes auf einem Notizzettel
- d) Ergänzung eines Passwortes mit Zufallszeichen
- e) Kombination aus Straßenbezeichnung und Hausnummer des Büros als Passwort
- f) Einbau von Rechtschreibfehlern in ein Passwort
- g) bei einem Passwortwechsel eines der letzten drei verwendeten auszuwählen
- h) Codierung von Ergebnissen des aktuellen Sports (z.B. Name und Punkte des Drittplatzierten der höchsten italienischen Fußballliga) als Passwort
- i) Implementierung eines Frage-Antwort-Systems als Passwortsystem

4.) Welche angegebenen Schutzmethoden eignen sich für den Softwareschutz vor Raubkopien?

- a) niedrige Preise
- b) ständige Darstellung des Namens des SW-Lizenznehmers am Bildschirm
- c) Dongle
- d) keine Hotline
- e) Firewall
- f) Anpassung der Software an den Kunden (z.B. durch Parametrisierung)

5.) Sicherheitseigenschaften sind (1) Authentizität (Authenticity), (2) Integrität (Integrity), (3) Vertraulichkeit (Confidentiality), (4) Verfügbarkeit (Availability), (5) Verbindlichkeit (Non-repudiation) und (6) Abrechenbarkeit (Accountability). Welche Sicherheitseigenschaften werden von jedem nachfolgend angegebenen Mechanismus/Verfahren sehr gut erfüllt? Bitte tragen sie maximal 2 geeignete Nummern ein.

- Symmetrische Verschlüsselung
- Digitale Signatur
- Passwort
- Protokollierung
- Biometriesystem
- RSA-Algorithmus

6.) 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.)

7.) Was sind Angriffspunkte für eine Konkurrenzspionage gegen Unternehmen?

- a) Feriapraktikanten
- b) Besucher, die sich frei im Unternehmen bewegen dürfen
- c) Die kompromittierende Abstrahlung von Desktop-PCs
- d) Kommunikation mit einer Zweigstelle mit sicher verschlüsselten Daten
- e) In Sicherheitsfragen gut geschultes Personal
- f) Kommunikation mit einer Zweigstelle mit sicher digital signierten Daten

8.) Welche Angaben über die Gesichtserkennung zur elektronischen Authentifikation sind falsch?

- a) Gesicht ist gut geeignet, weil es ein primäres Erkennungsmerkmal ist
- b) sie ist unaufdringlich und berührungslos
- c) es sind auch enge Verwandte einfach unterscheidbar
- d) bei einem der vielen verschiedenen Verfahren werden geometrische Informationen (Abstände, Radien, Winkeln) von Nase, Mund, Kinn etc. berechnet
- e) sie ist unabhängig von der Beleuchtung
- f) sie garantiert hohe Hygiene (weil keine Berührung)
- g) Verdeckungen wie Brillen und andere Frisur spielen keine Rolle

9.) Welche Angaben über Versicherungen sind richtig?

- a) Die Informationsverlust- und Datenträger-Versicherung versichert Datenträger und die auf diesen befindlichen Daten, falls sie nicht wiederbeschaffbar sind
- b) Die Computer-Missbrauchsversicherung hilft z.B. bei vorsätzlicher rechtswidriger Bereicherung an Vermögenswerten oder Schädigung des Versicherungsnehmers
- c) Die Betriebsunterbrechungsversicherung ersetzt für einen bestimmten Zeitraum unter anderem die laufenden Kosten (Gehälter, Miete)

10.) Welche Aussagen sind richtig über die ISO Norm 17799?

- a) Sammlung von Empfehlungen, die sich bewährt haben (Best Practices)
- b) Es enthält konkrete Sicherheitslösungen
- c) Sie bietet Orientierungshilfen und Richtlinien
- d) Anwendbar nur für große Unternehmen
- e) Leistet eine umfangreiche Hilfe bei der Bewertung von Sicherheitsmaßnahmen
- f) Beschäftigt sich auch mit der Sicherheitspolitik

11. Ein in Word verfasstes Dokument wurde mit einer digitalen Signatur versehen und an den Empfänger per Internet übertragen. Der Empfänger überprüft nun die Signatur. Welche Schritte werden dabei auf Empfängerseite unter anderem durchgeführt. Welche unten angegebenen Schritte sind dabei richtig?

- a) das Dokument wird mit dem geheimen Schlüssel entschlüsselt
- b) das Dokument wird mit dem öffentlichen Schlüssel entschlüsselt
- c) das Dokument wird mit einer Hashfunktion entkomprimiert
- d) das Dokument wird mit einer Hashfunktion komprimiert
- e) das Dokument wird verschlüsselt
- f) die mitübertragene Signatur wird mit dem öffentlichen Schlüssel entschlüsselt
- g) die mitübertragene Signatur wird mit dem geheimen Schlüssel entschlüsselt
- h) das Ergebnis der Hashfunktion wird mit dem öffentlichen Schlüssel entschlüsselt
- i) das Ergebnis der Hashfunktion wird mit dem geheimen Schlüssel entschlüsselt
- j) zuletzt werden zwei der oben angegebenen Ergebnisse verglichen

12.) Welche Ziele soll ein Risikomanagement in einem Unternehmen NICHT haben?

- a) Risikopolitik in die Unternehmenspolitik integrieren
- b) Sicherung des Fortbestands des Unternehmens
- c) Reduktion des Unternehmenswertes
- d) Risikobewusstsein bei Mitarbeitern erhöhen
- e) Erhöhung des Risikos
- f) Frühwarnung als frühzeitige Ortung von Bedrohungen