

Skills Card Nr	DEMO-Test	Bestanden	<input type="checkbox"/> JA <input type="checkbox"/> NEIN	SC-Demo
Vorname		Punkte	[erforderlich 75%, d.h. 27 von 36]	
Name		Beurteiler/in		
Testdatum		Unterschrift		

## OCG

## IT-Security

Bei Multiple-Choice-Fragen kann eine Antwort korrekt sein oder mehrere (Achten Sie auf die Fragestellung). Kreuzen Sie den Buchstaben der richtigen bzw. alle richtigen Antworten an.

Bei offenen Fragen genügt eine kurze Antwort in Schlagworten.

1. Was versteht man unter der Informationsklassifikation **confidential**: 1
  - A Unautorisierte Offenlegung könnte schwerwiegende Auswirkungen auf das Unternehmen haben
  - B Offenlegung ist nicht erwünscht, würde sich aber nicht nachteilig auswirken
  - C Offenlegung würde die Privatsphäre eines Mitarbeiters verletzen
  - D Die nationale Sicherheit würde durch Offenlegung der Daten gefährdet sein
  
2. Was versteht man unter Risikoverlagerung? 1

.....

.....

.....
  
3. Das vollständige und unveränderte Übertragen von Daten zwischen einem Absender und einem Empfänger sichert die: 1
  - A Vertraulichkeit
  - B Integrität
  - C Verfügbarkeit
  - D Nicht-Abstreitbarkeit
  
4. Was wird benötigt um mit Hilfe einer digitalen Signatur eine Nachricht NICHT abstreitbar zu machen? (Bitte alle richtigen ankreuzen) 1
  - A Ein weiterer Signierungsvorgang
  - B Eine dritte vertrauenswürdige Instanz (Certification Authority)
  - C Eine sichere (verschlüsselte) Verbindung zwischen Absender und Empfänger
  - D Ein schriftliches Protokoll der Kommunikation
  
5. Welche der folgenden Bedrohungen für den Serverraum ist der Kategorie höherer Gewalt zuzuschreiben? 1
  - A Wasser
  - B Ausfall der Stromversorgung
  - C Diebstahl
  - D Manipulation an Daten oder Software

Name	<<vorname>> <<nachname>>	SC-Demo
------	--------------------------	---------

6. Nennen Sie 3 vorsätzliche Fehlhandlungen, durch die Bedrohungen für Daten durch interne Personen entstehen können: 1
- .....
- .....
- .....
7. Nennen Sie 3 Bedrohungen für den Serverraum: 1
- .....
- .....
- .....
8. Was ist ein mögliches Sicherheitsproblem beim Löschen von Office Dokumenten? 1
- A Office Dokumente sind standardmäßig schreibgeschützt und können daher nicht gelöscht werden
  - B Die Dateien verbleiben auch nach dem Löschen der eigentlichen Datei als temporäre Dateien erhalten
  - C Wenn die Dateien zu groß sind können sie nicht in den Papierkorb verschoben werden
  - D Dateien werden zentral beim Hersteller gespeichert
9. Was beschreibt **Spoofing** am besten? 1
- A Abhören eines Kommunikationskanals
  - B Das Durcharbeiten einer Wortliste
  - C Session Hijacking
  - D Die Vorgabe einer fremden Identität
10. Welche der folgenden Aussagen ist, in Bezug auf Malicious Code, richtig? 1  
(Bitte alle richtigen ankreuzen)
- A Virensignaturen müssen laufend aktualisiert werden, um ausreichend Schutz zu bieten
  - B Prüfsummen verhindern auf jeden Fall das Manipulieren von Dateien
  - C Trojanische Pferde sind Programme, die unbemerkt in anderen Programmen versteckt sind
  - D Mein Virens scanner erkennt alle Viren, ich bin absolut sicher
11. Welche Aussage über Geheimtext ist wahr? 1
- A Geheimtext wird erzeugt durch Klartext, Schlüssel und kryptographischer Methode
  - B Geheimtext ist verständlich lesbar
  - C Die Form des Geheimtextes hängt nicht von der gewählten kryptographischen Methode ab
  - D Geheimtext darf nie in die Hände einer unautorisierten Person gelangen

Name	<<vorname>> <<nachname>>	SC-Demo
------	--------------------------	---------

12. Worauf sollte man im Umgang mit sensiblen Daten achten? (Bitte alle richtigen ankreuzen) 1
- A Es genügt, wenn ich Dokumente zerreiße, wenn bevor ich sie entsorge
  - B Sensible Dokumente sollten geschreddert werden
  - C Namen und Geburtsdaten sind keine sensiblen Daten
  - D E-Mail Adressen sollten grundsätzlich nicht frei zugänglich sein
13. In welchen Abständen sind, nach gegebenen Standards, Passwörter zu wechseln? 1
- .....
- .....
- .....
14. Welche Aussagen treffen bei IP zu? (Bitte alle richtigen ankreuzen) 1
- A Jeder Computer im Internet hat eine eindeutige IP-Adresse
  - B Eine IP-Adresse kann von mehreren Computern verwendet werden
  - C Bei IPv4 werden Hexadezimalzahlen verwendet
  - D IP-Adressen werden normalerweise in der **dotted decimal notation** angegeben
15. Was versteht man unter netzwerk-basierter Sicherheit? 1
- Bei diesem Konzept geht es um die Absicherung eines (heterogenen) Verbundes aus Computersystemen vor einem anderen Netzwerk. Dies geschieht unter anderem durch den Einsatz einer Firewall. Netzwerk-basierte Sicherheitslösungen dienen als Ergänzung zur Absicherung des individuellen Rechners, sollten jedoch nie diese ersetzen
16. Ist ActiveX als absolut unsicher zu betrachten? 1
- A Nein, es bietet nur Funktionalitäten von denen keine Gefahr ausgeht
  - B Ja, ActiveX wurde als Techdemo geschrieben um Schwächen in Browsern und dem Betriebssystem zu demonstrieren
  - C Nein, solange ich nur signierte Elemente erlaube da eine Signierung die Funktionalität auf Sicherheitsaspekte überprüft
  - D Ja, weil es in keiner Sandbox läuft sondern sich lokal installiert und mit den Rechten des angemeldeten Benutzers läuft
17. Was verwendet ein Virens Scanner um Viren zu identifizieren? 1
- A Den Dateinamen
  - B Die Dateigröße
  - C Eine Virensignatur
  - D Den Lempel-Ziv-Welch Algorithmus
18. Was versteht man unter einem **Manuellen Scanner**? 1
- .....
- .....
- .....

19. Zum symmetrischen Verschlüsseln wird die Nachricht mit dem... 1
- A öffentlichen Schlüssel ver- und mit dem privaten Schlüssel entschlüsselt
  - B privaten Schlüssel ver- und mit dem öffentlichen Schlüssel entschlüsselt
  - C privaten Schlüssel ver- und mit dem privaten Schlüssel entschlüsselt
  - D öffentlichen Schlüssel ver- und mit dem öffentlichen Schlüssel entschlüsselt
20. Sie erhalten ein E-Mail Ihres Arbeitgebers, das sie im Zuge eines Gewinnspiels um Eingabe von Name, Adresse und Windows-Benutzername auffordert. Wieso handelt es sich hierbei vermutlich um eine Phishing-Attacke? 1
- A Weil das Unternehmen diese Daten bereits besitzt und sie nicht abfragen muss
  - B Weil auch das Geburtsdatum und die Telefonnummer abgefragt werden müsste
  - C Weil das E-Mail von einem unternehmensinternen Absender stammt
  - D Weil neben dem Benutzernamen auch das Passwort abgefragt werden müsste
21. Wie könnte man sich effektiv gegen Cross Site Scripting-Attacken schützen? 1
- A Es sollte nicht möglich sein, die eigenen Webseiten aus dem Firmennetzwerk zu erreichen
  - B Sämtliche Benutzereingaben sollten gefiltert werden
  - C Die zugrunde liegende Datenbank sollte stets auf dem aktuellsten Stand gehalten werden
  - D Das zugrunde liegende Betriebssystem muss stets gepatcht werden
22. SSL (Secure Socket Layer) sichert die Datenübertragung zwischen zwei Kommunikationspartnern folgendermaßen: 1
- A Mittels einer SmartCard wird ein asymmetrischer Schlüssel ausgetauscht, der für die eigentliche Kommunikation verwendet wird
  - B Mittels Username und Passwort wird ein Token generiert, das für die eigentliche Kommunikation verwendet wird
  - C Mittels eines gültigen Zertifikates einer Certificate Authority wird ein symmetrischer Schlüssel ausgetauscht, der für die eigentliche Kommunikation verwendet wird
  - D Mittels einer signierten E-Mail einer Certificate Authority wird ein asymmetrischer Schlüssel ausgetauscht, der für die eigentliche Kommunikation verwendet wird
23. Warum würden Sie Ihre Kreditkartendaten NICHT per E-Mail bzw. eines Instant-Messengers versenden? 1
- .....
- .....
- .....
24. Welcher Zahlungsart ist bei Online-Versteigerungen zu bevorzugen? 1
- A Vorkasse
  - B Treuhandservice
  - C Kreditkarte
  - D Überweisung

Name	<<vorname>> <<nachname>>	SC-Demo
------	--------------------------	---------

25. Welche Methode kennen Sie um die Nicht-Abstreitbarkeit und Integrität von E-Mails zu gewährleisten? 1
- A Anforderung einer Bestätigung über den Erhalt der E-Mail
  - B Verschlüsselung des Inhalts
  - C Verschlüsselte Übertragung
  - D Elektronische Signatur
26. Welche WLAN Verschlüsselung ist als unsicher eingestuft? 1
- A WPA
  - B WPA2
  - C WEP
  - D WPP
27. Wired Equivalent Privacy ist ein Verfahren zur ... 1
- A Datenverschlüsselung und Authentifizierung in Wireless LANs
  - B Datenübertragung in Wireless LANs
  - C Datenverschlüsselung und Authentifizierung in Wired LANs
  - D Datenübertragung in Wired LANs
28. Welche Sicherheitsstufe der Internet-Zone ist standardmäßig im IE7 eingestellt? 1
- A Hoch
  - B Mittelhoch
  - C Mittel
  - D Niedrig
29. Welche Authentifizierungsmethoden kann es bei VPNs geben? 1  
(Bitte alle richtigen ankreuzen)
- A User/Passwort
  - B Tokens
  - C Smart Cards
  - D Zertifikate
30. Bietet ein nicht konfigurierter Router mit Firewall Funktion genügend Schutz vor Viren und anderen Angriffen? 1
- A Ja, ich bin ausreichend geschützt falls eine solche Funktion vorhanden ist
  - B Ja, allerdings nur wenn die Firmware des Routers auf aktuellem Stand ist
  - C Nein, ein Router mit Firewall Funktion bietet mir keinerlei Schutz
  - D Nein, er verhindert bei Verwendung von NAT nur die direkte Erreichbarkeit der angeschlossenen Rechner
31. Eine inkrementelle Sicherung sichert...? 1
- A Sichert den Gesamtbestand aller Daten zum Sicherungszeitpunkt
  - B Sichert alle Daten, die seit der letzten Sicherung neu erzeugt wurden, oder sich verändert haben
  - C Sichert alle Daten, die seit der letzten Sicherung unverändert geblieben sind
  - D Sichert nur System- und Statusinformationen des Servers

Name	<<vorname>> <<nachname>>	SC-Demo
------	--------------------------	---------

32. In welcher Situation ist ein Wachmann die geeignete Wahl zur physischen Zutrittskontrolle? 1
- A Wenn ein kontextspezifisches Urteil über die Zutrittserlaubnis erforderlich ist
  - B Wenn Intrusion Detection erforderlich ist
  - C Wenn das Sicherheitsbudget gering ist
  - D Wenn weitere Zutrittskontrollsysteme implementiert sind
33. Welche der folgenden Aussagen trifft NICHT zu? 1
- A Der Zugriff auf den Backup-Datenträger sollte nur Befugten Personen möglich sein
  - B Ein schneller Zugriff auf den Backup-Datenträger muss gewährleistet sein
  - C Die räumliche Trennung von Backup-Datenträger und Rechner muss gewährleistet sein
  - D Der Backup-Datenträger sollte schnell auffindbar auf dem Schreibtisch des Administrators liegen
34. Welche der folgenden Techniken eignen sich zur physischen Zerstörung von Daten auf Festplatten? (Bitte alle richtigen ankreuzen) 1
- A Säure
  - B Abrasion
  - C Verbrennen
  - D Tiefrieren
35. Wo kann ein mittels Windows Sicherungsprogramm erstelltes Backup auf Korrektheit überprüft werden? (Bitte alle richtigen ankreuzen) 1
- A In der Microsoft Management Console
  - B Bei zyklisch geplanten Backups kann der Status und das letzte Ergebnis bei den geplanten Tasks verifiziert werden
  - C Mittels der generierten SFV-Datei
  - D Bei der Erstellung des Sicherungsauftrages kann eine Überprüfung der Daten nach der Sicherung konfiguriert werden
36. Welche Richtlinie muss eine externe Firma für die Datenvernichtung erfüllen? 1
- A Der Internet Auftritt muss überzeugend sein
  - B Die externe Firma muss als Auftragsdatenverarbeitung bei der Aufsichtsbehörde gemeldet sein
  - C Der Preis muss die Leistung rechtfertigen
  - D Zur Datenvernichtung wird ausschließlich die Verbrennung angewendet