IT-Sicherheit
Verständnisaufgaben

Fragen zu Grundlagen und Zusammenhänge

Welches sind die Grundwerte der IT-Sicherheit?

Was ist der Unterschied zwischen Security und Safety?

Geben Sie eine Definition des Begriffs IT-Sicherheit an!

Was versteht man unter dem Begriff Schutzbedarf?

Aus was leitet sich der Schutzbedarf von IT-Systemen ab?

Was ist der Unterschied zwischen Schutzbedarf und Risiko?

Wann sind Sicherheitsmaßnahmen nicht angemessen?

Was ist der Unterschied zwischen präventiven und reaktiven Sicherheitsmaßnahmen?

Wie werden Schäden und Eintrittswahrscheinlichkeiten i.d.R. skaliert?

Welche 3 Stufen von Maßnahmen unterscheidet der IT-Grundschutz?

Wann kann beim IT-Grundschutz auf eine Risikoanalyse verzichtet werden?

Was versteht man beim IT-Grundschutz unter Modellierung?

Wie erhält man beim IT-Grundschutz die Liste umzusetzender Anforderungen?

Erläutern Sie die Dreiecksbeziehung zwischen Funktionalität, Kosten und IT-Sicherheit.

Erläutern Sie die Problematik der Sicherstellung *umfassender* IT-Sicherheit.

Fragen zu Kryptologie

Was ist der Unterschied zwischen Blockchiffren und Stromchiffren?

Was besagt das Kerckhoffsche Prinzip?

Welche Schlüssellängen weist der AES auf?

Welche Hashwertlänge sollte eine aktuell sichere kryptographische Hashfunktion mindestens aufweisen?

Sichere kryptographische Hashfunktionen sollen kollisionsresistent sein. Was heißt das?

Was versteht man unter *Authenticated Encryption*?

Welche Schlüssellänge sollte für einen sicheren Einsatz des RSA-Verfahrens aktuell mindestens verwendet werden?

Auf welchem zahlentheoretischen Problem beruht die Sicherheit des DH-Verfahrens?

Welche Auswirkung hätte die Existenz hinreichend großer Quantencomputer auf die Sicherheit aktuell verwendeter asymmetrischer und symmetrischer Verfahren?

Welche Schlüssel werden bei asymmetrischen Kryptoverfahren wozu verwendet?

1. Öffentlicher Schlüssel Sender	a) Verschlüsselung
2. Privater Schlüssel Sender	b) Entschlüsselung
3. Öffentlicher Schlüssel Empfänger	c) Signierung (Signatur-Berechnung)
4. Privater Schlüssel Empfänger	d) Signaturprüfung

Was ist der zentrale Vorteil von Verfahren über Elliptischen Kurven im Vergleich zum RSA und DH-Verfahren modulo großer Primzahlen?

Welche Schlüssellänge muss ein EC-Verfahren aufweisen um eine Sicherheit zu bieten vergleichbar mit einer 128 Bit symmetrischen Verschlüsselung?

Erläutern Sie die Vor- und Nachteile von symmetrischer und asymmetrischer Verschlüsselung.

Erläutern Sie, wie die hybride Verschlüsselung die Vorteile der symmetrischen und asymmetrischen Verschlüsselung kombiniert.

Erläutern Sie den Begriff Forward Secrecy.

Weshalb weist der Schlüsselaustausch per DH die Eigenschaft Forward Secrecy auf, der RSA-Schlüsselaustausch jedoch nicht?

Erläutern Sie die Funktionsweise von Message-Authentication-Codes (= kryptografischer Prüfsummen).

Ordnen Sie den Sicherheitsfunktionen die Grundwerte der IT-Sicherheit zu, denen Sie dienen:

Sicherheitsfunktion	Grundwert(e)
Verschlüsselung	
Kryptographische Prüfsummen	
Digitale Signaturen	

Wofür stehen die Abkürzungen ECDH und ECDSA?

Fragen zu PKI

Wozu dienen Public-Key-Zertifikate?

Nach welchem Standard sind im Internet verwendete Public-Key Zertifikate aufgebaut?

Nennen Sie wichtige Informationen, die in einem Zertifikat enthalten sind.

Zertifikats-Extensions können kritisch und unkritisch sein. Was bedeutet das?

Was besagt die Extension Key-Usage?

Was bedeutet die Abkürzung CRL und was ist in einer CRL gespeichert?

Durch welche Angaben in einem Zertifikat ist das nächsthöhere Zertifikat im Zertifizierungspfad eindeutig bestimmt?

Wie heißt der standardisierte Dienst zur Zertifikatsprüfung?

Welche 3 Prüfungen sind bei der Prüfung eines Zertifikats durchzuführen?

Nennen Sie die 3 im Internet verwendeten Zertifikatsklassen.

Sie sind auf einer Firmen-Webseite, die sich mit einem *Let's encrypt* Zertifikat ausweist. Im Impressum der Webseite sind Name und Anschrift der Firma angegeben. Können Sie sicher sein, dass Sie auf der Webseite der angegebenen Firma sind?

Erläutern Sie die Anforderungen „Sichere Darstellung" und „Sichere PIN-Eingabe" in Bezug auf digitale Signaturen.

Wie heißt die EU-Verordnung, die den rechtsverbindlichen Einsatz digitaler Signaturen regelt?

Was ist der zentrale Unterschied zwischen dem *Web of Trust* und einer hierarchischen PKI?

Fragen zur Kommunikationssicherheit (VPN, IPsec, SSL/TLS)

Erläutern Sie die Begriffe Sniffing, Spoofing, Replay und MITM.

Welche nach ihrem Einsatzzweck unterschiedenen VPN-Arten gibt es?

Wozu dienen bei IPsec Security Policies?

Wozu dienen bei IPsec Security Associations?

Mit welchem Protokoll werden Security Associations ausgehandelt?

Wodurch ist bei IPsec sichergestellt, dass grundlegende IPsec-Standards bei der Anpassung kryptographischer Verfahren nicht geändert werden müssen?

Wann darf bei IPsec der Tunnel-Modus und wann der Transport-Modus eingesetzt werden?

Welche Sicherheitsfunktionen bietet IPsec? Welche davon werden beim Einsatz von ESP und welche bei AH erreicht?

In welcher Weise bietet IPsec einen Basisschutz gegen DoS-Angriffe?

Welche Sicherungsfunktionen bietet TLS?

Skizzieren Sie den Ablauf des TLSv1.2-Handshakes für einen Schlüsselaustausch per RSA und einen Schlüsselaustausch per DH.

Wodurch erfolgt beim RSA-Schlüsselaustausch eine Authentifizierung des Servers?

Wie erfolgt beim DH-Schlüsselaustausch eine Authentifizierung des Servers?

Welche wesentlichen Unterschiede gibt es zwischen TLS Version 1.2 und 1.3?

Gegeben seien folgende TLS Ciphersuites:

1. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
2. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
3. TLS_RSA_WITH_AES_256_CBC_SHA256
4. TLS_AES_256_GCM_SHA384

- Welche der Ciphtersuites gehört zu TLS 1.2 und welche zu TLS 1.3?
- Bei welchen der Ciphersuites erfolgt der Schlüsselaustausch per RSA (hybride Verschlüsselung) und bei welchen per DH?
- Wozu dient das ECDSA-Verfahren in der 1. Ciphersuite?
- Wozu dient das RSA-Verfahren in der 2. Ciphersuite?

- Wozu dient das RSA-Verfahren in der 3. Ciphersuite?
- Was bedeutet das GCM in den Ciphersuites 1,2 und 4?
  (Es ist nicht nach der Auflösung der Abkürzung gefragt.)

Fragen zur Absicherung von Netzübergängen

Was ist ein Firewall-System (Definition)?

Beschreiben Sie unterschiedliche Firewall-Typen und Grenzen Sie diese gegeneinander ab.

Was ist ein wichtiger Grundsatz bei der Konfiguration von Paketfiltern?

Auf Basis welcher Informationen entscheidet ein Paketfilter i.d.R. ob ein Paket durchgelassen (permit) oder blockiert (deny/drop) wird?

Wie „lernt“ ein dynamischer Paketfilter (stateful inspection) temporäre Regeln?

Wieso bieten die dynamisch erzeugten Regeln eine höhere Sicherheit als statische Regeln?

Welchen weiteren Vorteil hinsichtlich Sicherheit hat ein dynamischer Paketfilter gegenüber einem statischem?

Was ist eine DMZ? Welche Systeme werden in einer DMZ betrieben?

Eine DMZ kann 1-stufig oder 2-stufig ausgelegt sein. Skizzieren Sie die Topologien des Netzübergangs.

Welche Vorteile hat ein 2-stufiges Firewallsystem gegenüber einem 1-stufigen?

Was verbirgt sich hinter dem Begriff „Zoning“ des internen Netzes.

Nennen sie flankierende organisatorische Prozesse beim Betrieb eines Firewallsystems.

Welche Komponenten gehören zu einem IDS?

Nennen Sie einige Vor-/Nachteile von Netzsensoren und Hostsensoren.

Welche zwei grundsätzlich unterschiedlichen Erkennungsmethoden für Angriffe gibt es?

Welche Problematik ergibt sich beim Einsatz von IDS und gleichzeitiger Nutzung von Verschlüsselungen (https, smtps, …)?

Fragen zu Schadsoftware, Cybercrime und SVM

Weshalb ist die Erkennung und Filterung von Schadsoftware heute nur noch begrenzt möglich?

Was versteht man unter den Begriffen Schwachstelle (Vulnerability), Exploit, Botnet und Ransomware, Phishing?

Nennen Sie einige typische Infektionswege für Schadsoftware.

Weshalb ist die regelmäßige Aktualisierung von Software eine wichtige Sicherheits-maßnahme?

Was ist Aufgabe/Ziel des SVM und welches sind damit verbundene typische Probleme in Unternehmen?

Fragen zu AAA

Wofür steht die Abkürzung AAA?

Wie werden Passwörter (PW) i.d.R. serverseitig gespeichert? Wie wird dabei erreicht, das gleiche PW nicht zu dem gleichen serverseitig gespeicherten Wert führen?

Wieso hat für die Nutzung von Passwörtern im Internet der Zugriffsschutz auf E-Mails eine besonders hohe Bedeutung?

Erläutern Sie das Grundprinzip einer Challenge-Response Authentisierung.

Nennen Sie drei grundsätzlich verschiedene Arten von „Faktoren“ bei der Authentisierung.

Beschreiben Sie den Ablauf einer 2FA bei der Nutzung einer Authenticator-App auf dem Smartphone. Was bedeutet dabei der Begriff TOFU?

Erläutern Sie, wie eine 2FA gegen Phishing schützt.

Charakterisieren Sie kurz die 4 verschiedenen Zugriffskontrollmodelle.

- Wer legt beim DAC die Zugriffsrechte auf Objekte fest?

- Was versteht man beim RBAC unter dem Begriff der „Rolle“?

- In welchem der Zugriffskontrollmodelle gibt es Sicherheitskennungen (security labels)?

Wozu dienen SAML und OAuth?

Welche Idee steckt hinter der Fido-Authentisierung?

Wie gelingt es Fido die Sicherheit der Authentisierung zu erhöhen und gleichzeitig die Bequemlichkeit zu verbessern?

Beschreiben Sie die Abwägung von Anforderungen hinsichtlich der „3 A’s“ für das Szenario Fernwartung.

Beschreiben Sie die Abwägung von Anforderungen hinsichtlich der „3 A’s“ für das Szenario Gäste-WLAN.

Fragen zu Verfügbarkeit, BCM

Erläutern und diskutieren Sie die Backup-Varianten full, differential und incremental backup.

Erläutern Sie die Funktionsweisen der Raid-Level 0, 1 und 5.

Wie wirken sich die Raid-Level 0, 1 und 5 auf die Verfügbarkeit aus und wie auf die Schreib-/Leseperformance?

Berechnen Sie für eine gegebene Verfügbarkeit *V* einzelner Platten die Verfügbarkeit eines Raid-0 und Raid-1 mit 3 Platten und eines Raid-5 mit 4 Platten.

Erläutern Sie die Begriffe Cold-/Hot-Standby und Lastverteilung.

Ein System habe eine MTBF von einem Jahr. Welche MTTR darf das System maximal haben um eine Verfügbarkeit von „5 Nines“ zu erreichen?

Wofür steht die Abkürzung BIA und was ist das Ergebnis einer BIA?

Wie kann organisatorisch sichergestellt werden, dass die Notfallvorsorge angemessen berücksichtigt wird und stets auf einem aktuellen Stand bleibt (z.B. bei der Einführung neuer IT-Systeme oder Anwendungen)?

Fragen zu Recht und Datenschutz

Welches Gesetz definiert IT-Sicherheitsvorgaben für Betreiber kritischer Infrastrukturen?

Um den Schutz welcher Daten geht es beim „Datenschutz“?

Wie heißt die europäische Regelung/das Gesetz zum Datenschutz?

Nennen Sie die 3 zusätzlichen Grundwerte des Datenschutzes.

Nennen und erläutern Sie einige Grundsätze des Datenschutzes.

Gegen welchen Grundsatz würde verstoßen, wenn die Hochschule ihre Studierendendaten an Werbeunternehmen verkauft?

Im Lernraum wird ein Klausurergebnis per Liste mit Matrikelnummern und Noten bereitgestellt. Die Matrikelnummern sind dabei die _____?

Fragen zu Web-Applikations-Sicherheit

Erläutern Sie kurz die Funktionsweise des Angriffs Cross-Site-Scripting (XSS)?

Erläutern Sie kurz die Funktionsweise des Angriffs SQL-Injection?

Erläutern Sie kurz die Funktionsweise des Angriffs Cross-Site-Request-Forgery (CSRF)?

Bietet https Schutz gegen Web-Applikations-Angriffe?

Wieso ist der Übergang von der Entwicklung zum Live-Betrieb bei Web-Applikationen sicherheitskritisch? Was ist zu beachten?

Wo finden Sie im Internet wichtige Hinweise zu Risiken und der sicheren Entwicklung von Web-Applikationen?

Wie kann ein Web-FW-Proxy gegen eine nutzerseitige Manipulation von Cookies (Cookie-Poisoning) schützen?

Wie kann ein Web-FW-Proxy dafür sorgen, dass nur über eine Homepage verlinkte Seiten aus dem Internet zugreifbar sind?

Fragen zu ISMS und Organisation

Welches ist der internationale normative Standard zum Informationssicherheitsmanagement (ISM)?

Welches ist ein für kleine- und mittlere Unternehmen sinnvolles Vorgehen zur Einführung eines ISMS?

Nennen Sie die Schritte zur Schaffung angemessener IT-Sicherheit in Unternehmen.

Weshalb ist ein Prozess „Aufrechterhaltung angemessener IT-Sicherheit“ erforderlich?

Was sind Zweck und Ziel einer Corporate IT-Security Policy?

Beschreiben Sie die allgemeine Vorgehensweise zur Erstellung von Sicherheitskonzepten und erläutern Sie kurz die einzelnen Schritte.

Beschreiben Sie die Grundschutz-Vorgehensweise zur Erstellung von Sicherheitskonzepten und erläutern Sie kurz die einzelnen Schritte.

(Weitere Fragen zum Grundschutz siehe vorne Fragen Grundlagen und Zusammenhänge)

Organisatorische Prinzipien und Prozesse:

- Was besagt das Prinzip der Funktionstrennung?
  Erläutern Sie das Prinzip der Funktionstrennung an einem Beispiel.
- Wieso wird durch „Standardisierung“ die Sicherheit erhöht?
- Wieso wird durch „Einfachheit“ die Sicherheit erhöht?
- Wie wird durch das „Owner-Prinzip“ die Sicherheit erhöht?

Erläutern Sie, weshalb das Änderungsmanagement (Change-Management) im Unternehmen ein sicherheitsrelevanter Prozess ist.

Nennen Sie die 3 Ebenen der sicherheitstechnischen Revision!

Wieso gilt „nicht dokumentierte Sicherheit ist keine Sicherheit“?

Wie erfolgt i.d.R. die Kontrolle der Umsetzung?

Wie erfolgt häufig die Kontrolle der Wirksamkeit?

Geben Sie Beispiele für Prüfungsfragen zu den 3 Ebenen am Beispiel Notfallvorsorge/BCM an.

Geben Sie Beispiele für Prüfungsfragen zu den 3 Ebenen am Beispiel des Szenarios „Fernwartung“ an.

Was versteht man unter Fail-Safe / Fail Secure? Geben Sie Beispiele entsprechender Maßnahmen an.