Übungsaufgaben zur IT-Sicherheit

Übungsaufgaben zu Grundlagen und Zusammenhänge

1. Suchen Sie Beispiele für Maßnahmen/Mechanismen für
   - die der Security dienen, jedoch nicht oder kaum der Safety dienen
   - die der Safety dienen, jedoch nicht oder kaum der Security dienen
   - die sowohl der Safety als auch der Security dienen.

Gehen Sie hierzu typische Sicherheitsmaßnahmen im Bereich der IT(Netzsicherheit, Übertragungssicherheit, physikalische Sicherheit) aber auch in anderen Bereichen durch.

2. Firma X stellt bestimmte hochtechnologische Produkte automatisiert her. Folgende Geschäftsbereiche werden unterschieden:
   - Auftragsbearbeitung (Auftragsannahme, Ablaufkontrolle, Rechnungsstellung, etc.)
   - Produktionssteuerung (inkl. Datenaufbereitung für die Produktion)
   - Entwicklung (Forschung, Weiterentwicklung der Produkte)
   - Personalverwaltung (Mitarbeiter, Löhne, Gehälter, etc.)
   - Des Weiteren gibt es ein Mitarbeiterinformationssystem, das von den Bereichen gemeinsam zur Informationsbereitstellung für die Mitarbeiter genutzt wird.

   a) Jeder der Bereiche nutzt IT. Weisen Sie den Bereichen sinnvolle Schutzbedarfe (gering, mittel, hoch) zu den Grundwerten Vertraulichkeit, Integrität und Verfügbarkeit zu. Begründen Sie Ihre Zuweisungen.

   b) Die Firma X verfügt lediglich über ein zentrales IT-System, auf dem sämtliche Bereiche (z. B. über Arbeitsplatzterminals) arbeiten. Welchen Schutzbedarf hat dieses IT-System?

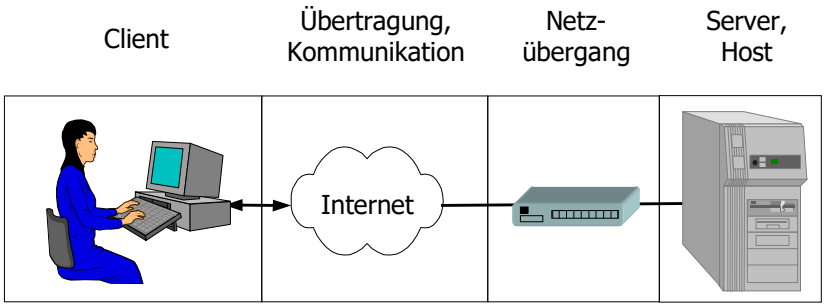
   c) Sie haben als CIO des Unternehmens die Möglichkeit, die Aufgaben auf zwei IT-Systeme zu verteilen. Wie verteilen Sie die Aufgabenbereiche auf die IT-Systeme?

   d) Zusätzlich wird ein IT-System für einen Web-Auftritt der Firma eingerichtet, über das Informationen zu den Produkten bereitgestellt werden. Welchen Schutzbedarf ordnen Sie diesem System zu?

   e) Der Web-Auftritt wird jetzt so erweitert, dass registrierte Kunden über die Web-Schnittstelle Aufträge eingeben können und den Status der Bearbeitung ihres Auftrags bis zur Rechnungsstellung mitverfolgen können. Was ändert sich am Schutzbedarf? Welche weiteren Probleme treten auf?

3. Nennen Sie mindestens 4 von der Art her verschiedene Beispiele jeweils für
   - Bedrohungen der Verfügbarkeit,
   - Bedrohungen der Integrität und
   - Bedrohungen der Vertraulichkeit.

4. Betrachten Sie die folgende Kommunikationskette:



Nennen Sie für jedes der Kettenglieder jeweils 2-3 Beispiele für technische, organisatorische, personelle und physische Sicherheitsmaßnahmen.

5. Der Zugang zu einem RZ erfolgt über eine Sicherheitstür mit einem elektronischen Schloss. Wie sollte sich diese Tür (bzw. das Schloss) bei Stromausfall verhalten?

   a) um der Safety zu genügen

   b) um der Security zu genügen

   c) der Safety und Security zu genügen

6. Unternehmen JOGHURT plant die Einführung des zusätzlichen internen Systems KIRSCHE, das sicherheitskritischer ist, als die bisher eingesetzten Systeme, jedoch eine Anbindung an das Internet erfordert. Die bisherige Firewall (FW) zum Internet ist aufgrund vieler Kommunikationsanforderungen löcherig wie ein Schweizer Käse. Daher soll über eine Risikoanalyse ermittelt werden, ob die Einrichtung einer dedizierten FW für das neue System sinnvoll ist. Folgende Daten liegen vor:
   - Für die neue FW werden Beschaffungskosten von € 100.000, Integrationskosten von € 50.000 , Wartungskosten (in den Folgejahren) in Höhe von 20% der Beschaffungskosten und ein Betriebsaufwand von 2 Personentagen pro Monat eines Systemadministrators kalkuliert.
   - Ein Systemadministrator kostet dem Unternehmen rund 300€ pro Tag.
   - Die Sicherheitsexperten rechnen damit, dass mit der bisherigen FW 70% der erfolgreichen Angriffe keinen Schaden verursachen, da sie rechtzeitig abgewehrt werden können oder harmlos sind. Bei 25% der erfolgreichen Angriffe wird für KIRSCHE mit einem mittleren Schaden von € 40.000 gerechnet. In den verbleibenden 5% der Fälle wird der Schaden inkl. Folgeschäden auf € 1.000.000 geschätzt.
   - Des Weiteren rechnen die Experten damit, durch den Aufbau der neuen FW die Sicherheit um 80% zu erhöhen, d. h. die Wahrscheinlichkeit erfolgreicher Angriffe auf 20% gegenüber bisher zu verringern.
   - Laut Firmenstatistik gab es in den letzten 5 Jahren 8 Ereignisse eines erfolgreichen Angriffs Unbefugter aus dem Internet. Mit einem Rückgang ist nicht zu rechnen.

Als Chief Information Officer von JOGHURT sollen Sie jetzt entscheiden, ob eine neue FW für KIRSCHE eingesetzt wird.

Falls Sie sich für den Einsatz einer neuen FW entscheiden, möchte der Vorstand genau wissen, nach welcher Zeit (Jahre, Monate) sich das neue System bezahlt gemacht hat.

7. Schadenshöhe und Eintrittswahrscheinlichkeit seien für ein mittelständiges Unternehmen folgendermaßen festgelegt:

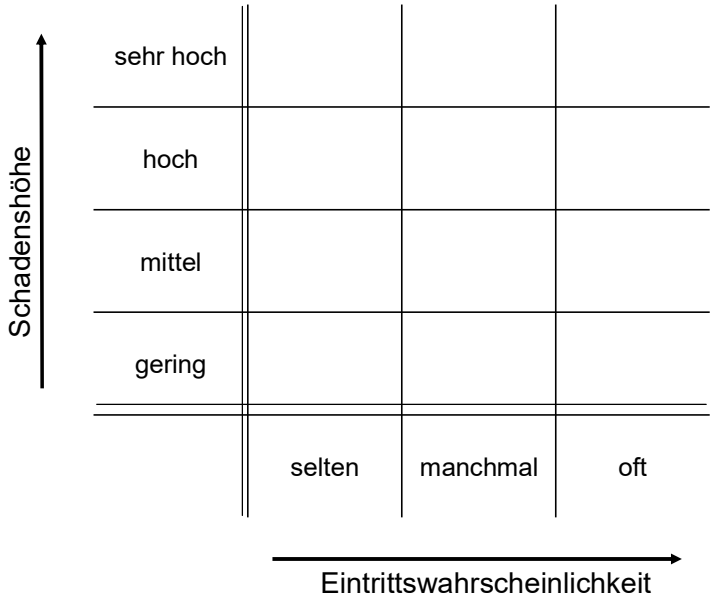
Schadenshöhen	
S <1000€	gering
1000€ < S < 10.000€	mittel
10 T€ < S < 100 T€	hoch
S > 100T€	sehr hoch

Eintrittswahrscheinlichkeit	
ca. alle 5 Jahre	selten
ca. jährlich	manchmal
ca.monatlich	oft

Die Risiken werden gemäß der folgenden Tabelle skaliert:

geringes Risiko	Risiko < 5000 € Schaden pro Jahr
mittleres Risiko	5000€/Jahr < Risiko < 20.000 €/Jahr
Hohes Risiko	Risiko > 20.000€/Jahr

Geben Sie die genauen Risiken und Risikostufen in folgender Tabelle an:



Übungsaufgaben zum Thema Kryptologie

1. Ein deutscher Text (nur Großbuchstaben) wird mit einem Schlüssel k $\in$ {0,1,2,...,25} dadurch verschlüsselt, dass jedes Zeichen durch das Zeichen ersetzt wird, das k Stellen weiter hinten im Alphabet steht:

Beispiele: Verschlüsselung von ABC mit k=1 ergibt BCD

Verschlüsselung von UNS mit k=2 ergibt: WPU

a) Known-Plaintext Angriff: Sie wissen, dass B zu X verschlüsselt wird. Berechnen Sie den Schlüssel und entschlüsseln Sie den Text PNWQI.

b) Skizzieren Sie eine Ciphertext-Only Angriff auf die Verschlüsselung.

c) Sie wollen von verschiedenen vorliegenden entschlüsselten Texten automatisch beurteilen, bei welchem es sich um den korrekten deutschen Klartext handelt. Wie gehen Sie vor?

2. Berechnen Sie die Additions- und Multiplikationstabelle modulo 7. (Nutzen Sie die Kommutativität von Addition und Multiplikation aus.)

+	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

.	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

3. Generatoren, Diskreter Logratihmus und Diffie-Hellman

a) Prüfen Sie, ob 2 eine Primitivwurzel/Generator modulo 13 ist.

b) Berechnen Sie den diskreten Logarithmus von 3 zur Basis 2 modulo 13.

c) Bei einem Diffie-Hellmann Schlüsselaustausch zwischen Alice und Bob über $Z_{13}\backslash\{0\}$ mit dem Generator 2 werden die Nachrichten 5 und 12 abgehört. Bestimmen Sie den vereinbarten Schlüssel.

4. RSA Verfahren: Gegeben sei der RSA-Modul m=55.

a) Verschlüsseln Sie die Zahl 3 mit dem öffentlichen Exponenten e=7

b) Welche der Zahlen 10,11,12,13 sind zulässige öffentliche Exponenten?

c) Berechnen Sie den zu e=7 gehörenden geheimen Exponenten d.

d) Entschlüsseln Sie die Zahl 12 durch Potenzierung mit dem geheimen Exponenten. Beschreiben Sie genau Ihren Berechnungsweg!

5. Betriebsmodi von Blockchiffren: In der Vorlesung wurde für die Betriebsarten von Blockchiffren jeweils die Verschlüsselung dargestellt.

a) Geben Sie zu den Modes ECB, CBC und OFB das zugehörige Entschlüsselungsverfahren an. Abbildungen sind dabei hilfreich!

b Für einen ausgewählten Schlüssel k sei die Blockchiffre E(k,m) mit der Blocklänge 4 Bit (Hexadezimal codiert) durch die folgende Tabelle gegeben.

m	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
E(k,m)	8	7	6	5	1	2	3	4	F	E	D	C	8	9	A	B

Verschlüsseln Sie den hexadezimalen Klartext „1A2B“ mit der Blockchiffre E im CBC Mode mit dem IV = „0“ und dem Schlüssel k.

6. Hybride Verschlüsselung: Alice will dieselbe Nachricht M unter Nutzung der hybriden Verschlüsselung gleichzeitig an die n Empfänger B(i), i=1,...,n verteilen. Dabei sei (PE,PD) das asymmetrische Kryptosystem, (E,D) das symmetrische Kryptosystem und (PubK-B(i), PrivK-B(i)) das Schlüsselpaar des Empfängers B(i).

a) Wie oft muss Alice hierzu symmetrisch und asymmetrisch verschlüsseln?

b) Alice will genau eine (verschlüsselte) Nachricht erzeugen und diese an Empfänger verteilen. D. h. jeder Empfänger erhält die gleichen Daten von Alice. Wie sieht die verschlüsselte Gesamtnachricht aus?

c) Alice will jetzt zusätzlich noch eine digitale Signatur der Ausgangsnachricht M mitschicken. Was ändert sich? Wie sieht die verschlüsselte Gesamtnachricht aus?

7. Nachrichtenauthentisierung: Sei CRC ein Cyclic Redundancy Check, H eine kryptographisch sichere Hashfunktion und E_K eine sichere symmetrische Blockchiffre (z.B. Advanced Encryption Standard im CBC-Mode).

   Beurteilen Sie, welche der folgenden Nachrichten zur Übertragung und Authentisierung der Nachricht M geeignet sind. Begründen Sie ihre Ergebnisse.

   a) M, CRC(M)

   b) M, H(M)

   c) E_K(M | CRC(M))

   d) M, CRC(K, M))

   Beachten Sie, dass ein CRC eine lineare Funktion ist: CRC(M) ist eine Linearkombination der Bits von M

8. Wieso ist es beim Senden von verschlüsselten und digital signierten Nachrichten sinnvoll, erst die Nachricht zu signieren und dann zu verschlüsseln anstatt umgekehrt?

Übungsaufgaben zum Thema Public Key Infrastrukturen

1. Rückwirkende Sperrungen und kompromittierte Zeitstempel

a) Diskutieren Sie, ob es sinnvoll ist, Sperrungen rückwirkend zu erlauben: „Ich habe vor 3 Tagen meine Signaturkarte verloren, bitte Sperren Sie meinen Schlüssel rückwirkend ab diesem Datum."

b) Der Schlüssel, den eine Zertifizierungsstelle zur Anfertigung von Zeitstempeln einsetzt, wird geknackt. Welchen Zustand haben ehemals mit dem Schlüssel ausgestellte Zeitstempel.

2. In der EU-Richtlinie zur elektronischen Signatur heißt es:

*„(1) Die Mitgliedstaaten tragen dafür Sorge, daß **fortgeschrittene elektronische Signaturen**, die auf einem **qualifizierten Zertifikat** beruhen und die von einer **sicheren Signaturerstellungseinheit** erstellt werden, ...*

... in Gerichtsverfahren als Beweismittel zugelassen sind"

In dem ersten Satzteil stecken 3 Bedingungen (fett gedruckt), die vorliegen müssen sind, damit Signaturen rechtskräftig sind. Erläutern Sie zu jeder der 3 Bedingungen:

a) Welche (ein oder mehrere) *grundlegenden* Anforderungen stecken hinter der Bedingung und wer oder was hat diese Anforderungen einzuhalten?
(Eine Nennung von Detailanforderungen ist nicht erforderlich!)

b) Nennen Sie jeweils ein Gegenbeispiel, bei dem die Anforderungen (und damit die jeweilige Bedingung) nicht erfüllt sind.

3. Zur Erstellung digitaler Signaturen werden üblicherweise Chipkarten mit eigenem Prozessor eingesetzt.

a) Welche sicherheitstechnischen Vorteile hat der Einsatz solcher Chipkarten gegenüber der Nutzung einer reinen Softwarelösung? Welche sonst möglichen Angriffe werden verhindert?

b) Manche Chipkartenleser sind zusätzlich mit einer Tastatur ausgestattet. Welche Sicherheitsvorteile ergeben sich zusätzlich hieraus? Welche sonst möglichen Angriffe werden verhindert?

c) Manche Chipkartenleser sind zusätzlich mit einem Display ausgestattet. Welche Sicherheitsvorteile ergeben sich zusätzlich hieraus? Welche sonst möglichen Angriffe werden verhindert?

Übungsaufgaben zum Thema IPSec und SSL/TLS

1. Zwei Filialen eines Unternehmens sind über angemietete Standleitungen an die Zentrale angebunden. Zwei weitere Filialen sollen jetzt zusätzlich angebunden werden. Dabei wird überlegt, anstelle der Standleitungen ein VPN über das Internet einzusetzen.

   Die Standleitungen sind bei einem Network-Provider für 15T€ pro Standleitung pro Jahr angemietet. Die Verträge für die Standleitungen laufen noch zwei Jahre. Der Provider bietet für die zusätzlichen Standleitungen einen Rabatt von 30% an.

   Nach Marktsichtung stellt sich heraus, dass ein VPN-Gateway (GW) für die Zentrale 20T€ kostet und in den Filialen VPN-GW für jeweils 10T€ eingesetzt werden können. Als externe Projektkosten für die Einrichtung der GW sind zentral 6 Personentage (PT) und pro Filiale 2 PT zu je 1000€ anzusetzen. Hinzu kommen interne Projektaufwände von dem halben Zeitaufwand. Interne Tage werden mit 500€/PT verrechnet.

   Die Wartungkosten für die GW betragen ab dem 2. Jahr jährlich 20% des Kaufpreises. Hinzu kommt ein interner Betriebs- und Pflegeaufwand von 2PT pro Monat für die VPN-Infrastruktur, unabhängig von der Anzahl der GW.

a) Berechnen Sie die entstehenden Kosten für die ersten 5 Jahre
   - bei sofortigen Aufbau der VPNs (Einrichtungszeit wird vernachlässigt)
   - bei Zukauf der zusätzlichen Standleitungen

b) Welche Handlungsstrategie schlagen Sie dem IT-Leiter vor?

c) Nach welcher Zeit hat sich der Aufbau des VPNs amortisiert (Break-Even-Point)

2. Im Next Header Feld eines ESP-Headers ist TCP angegeben. Was für ein IPSec-Modus wurde genutzt?

3. Warum erfolgt die Sequenznummernprüfung vor der MAC-Prüfung?

4. Warum erfolgt die MAC-Prüfung vor der Verschiebung des Replay-Fensters?

5. Welche Funktionalität bietet der gleichzeitige Einsatz von AH und ESP über den Einsatz von ESP hinaus?

6. Zwei Endsysteme kommunizieren ESP-geschützt (verschlüsselt und authentisiert) im Transportmodus.

a) Weshalb ist hierbei die Authentizität von Sender und Empfänger nicht sichergestellt?

b) Erläutern Sie zwei IPSec-Möglichkeiten, wie zusätzlich zur Verschlüsselung auch die Authentizität von Sender und Empfänger sichergestellt werden kann.

   Stellen Sie jeweils die resultierende Paketstruktur dar und erläutern Sie, wie beim Empfang die Authentizität von Initiator bzw. Responder geprüft wird.

   Für die Darstellung der Paketstruktur ist dabei eine blockweise Darstellung unter Nutzung folgender Blöcke ausreichend: IP-Header, AH-Header, ESP-Header und Payload. (D. h. diese Blöcke brauchen nicht weiter inhaltlich aufgeschlüsselt zu werden. ESP-Trailer braucht der Übersichtlichkeit halber nicht mit angegeben zu werden). Für die IP-Header sind IP-Adressen zu berücksichtigen.

7. Ein Firmennetz und eine Filiale sind über Router, die auch als IPSec-Gateways dienen, an das Internet angebunden. Zwischen den Gateways werden die Daten ESP geschützt übertragen. Darüber hinaus wird für die Übertragung zwischen Endsystemen in der Filiale und Servern im Firmennetz zusätzlich AH verwendet.

a) Welche Kombinationsarten von Transport- und Tunnelmodus sind erlaubt?

b) Stellen Sie für die erlaubten Kombinationsarten von Transport- und Tunnelmodus ausgehend von einem normalen IP-Paket dar, wie das Paket für die Übertragung erweitert und verändert wird.

   Für die Darstellung der Paketstruktur ist dabei eine blockweise Darstellung unter Nutzung folgender Blöcke ausreichend: IP-Header, AH-Header, ESP-Header und Payload. (D. h. diese Blöcke brauchen nicht weiter inhaltlich aufgeschlüsselt zu werden. ESP-Trailer braucht der Übersichtlichkeit halber nicht mit angegeben zu werden). Für die IP-Header sind IP-Adressen zu berücksichtigen.

8. Sichere Einsatz von TLS: Betrachten Sie das Szenario einer SSL-geschützten Homebanking Anwendung. Welche eher organisatorischen Maßnahmen sind beim Einsatz von TLS vom Benutzer und von der Bank einzuhalten, damit die erwünschte Sicherheitsfunktionalität (Verschlüsselung, Serverauthentisierung) erreicht wird?

Übungsaufgaben zum Thema Firewalling

1. Zählen Sie Gefährdungen auf, gegen die eine Firewall keinen Schutz bietet.

2. FTP Konfiguration eines Paketfilters.

Ports und Funktionsweise von FTP:

- FTP benötigt eine TCP-Kontrollverbindung (kurz KV) und eine TCP-Datenverbindung (kurz DV).
- Der FTP-Client baut die KV auf (TCP-Zielport 21 (Server), Quellport >1023 (Client)). Der FTP-Server baut daraufhin die DV auf (Quellport 20 (Server), Zielport >1023 (Client)).

An einem Paketfilter mit drei Netzinterfaces NIC1, NIC2 und NIC3 sind folgende Netze angebunden:

- NIC1: Extranet mit FTP-Servern und FTP-Clients anderer Unternehmen (IP-Adressmaske „extern“)
- NIC2: FTP-Server des Unternehmens (IP-Adresse „ftpServ“)
- NIC3: Internes Netz mit FTP-Clients (IP-Adressmaske „intern“)

Folgende Kommunikationsbeziehungen sollen ermöglicht werden:

- Interne Clients dürfen auf den eigenen FTP-Server und auf FTP-Server im Extranet zugreifen.
- Externe Clients dürfen auf den FTP-Server des Unternehmens zugreifen.

a) Erstellen Sie ein Netzstrukturdiagramm mit den notwendigen Datenflüssen und Richtungen der Verbindungsinitiierung.

b) Konfigurieren Sie die Paketfilterregeln für an den NICs eingehende Pakete in Form einer Tabelle:

NR	NIC	IP-Src	IP-Dest	Prot	SrcPort	DestPort	ACK	Action
1								
2								
3								
..								

c) In der Vorlesung wurde die Arbeitsweise eines dynamischen Paketfilters für FTP erläutert:

- Die Client-Portnummer für die Datenverbindung wird beim Aufbau der Kontrollverbindung vom Client an den Server übertragen
- Der Paketfilter erkennt diese und generiert temporäre Regeln für die Datenverbindung und für die Rückrichtung der Kontrollverbindung
- Die Regeln werden mit dem Abbau der Kontrollverbindung wieder gelöscht.

Welche Regeln aus der Konfiguration aus Teilaufgabe b) entfallen, da sie jetzt dynamisch generiert werden?

In wie weit hat sich die Sicherheit verbessert?

4. Sie sind Administrator eines Firewall-Systems in einem großen Unternehmen.

In der Vorlesung wurden die hiermit verbundenen organisatorischen Aufgaben kurz angesprochen.

- Freischalten neuer Dienste/Kommunikationsbeziehungen am Netzübergang
- Sperren bestehender Dienste/Kommunikationsbeziehungen
- Regelmäßig Überprüfung, ob alle Freischaltungen notwendig sind
- Regelmäßige Auswertung von Protokolldateien

a) Beschreiben Sie einen organisatorischen Prozess für die Freischaltung neuer Dienste/Kommunikationsbeziehungen am Firewall-System.

b) Skizzieren Sie verschiedene Möglichkeiten, um sicherzustellen, dass nur die Dienste/ Kommunikationsbeziehungen freigeschaltet sind, die auch tatsächlich benötigt werden.

   Wie kann eine regelmäßige Überprüfung erfolgen? Beschreiben Sie den zugehörigen organisatorischen Prozess. Welche Dokumentation ist erforderlich?

Übungsaufgaben zum Thema Zugriffskontrolle und Authentisierung

1. In der Vorlesung wurden 5 Hierarchieebenen für die Zugriffskontrolle vorgestellt. Überlegen Sie für jede Ebene, welche Funktionen des „AAA“ realisiert sind und in welcher Weise (Beispiele) sie realisiert sein können.

2. Die Authentisierung zu einer Client-Server-Anwendung erfolgt passwortbasiert, wobei die Passworte z.B. mit dem AES verschlüsselt werden. Hierzu teilt sich jeder Client mit dem Server einen spezifischen Schlüssel K und ein Passwort PW. Zur Authentisierung sendet der Client das verschlüsselte Passwort AES_K(Passwort) an den Server. Der Server berechnet seinerseits AES_K(Passwort) und prüft auf Übereinstimmung mit dem empfangenen Wert.

a) Wieso ist das Verfahren nicht sicher? Wie heißt die Art des Angriffs?

b) Ist eine TLS-geschützte Clientauthentisierung per Passwort sicher?

3. OpenAuthorization: Angenommen, die User-Authentisierung erfolgt passwortbasiert.

a) An welcher Stelle / welchem Schritt besteht bei der Berechtigungsvergabe an Dritte die Gefahr eines Phishings?

b) Welche Auswirkungen hätte ein erfolgreiches Phishing?

4. In Unternehmen werden Mitarbeiter durch die *Personalabteilung* verwaltet:

   a. Einstellung, b. interne Versetzung, c. Ausscheiden bzw. Kündigung

   Die IT-bezogene Benutzer- und Berechtigungsverwaltung erfolgt durch den *IT-Betrieb*.

a) Was ist zu beachten, damit das Berechtigungsmanagement ordentlich funktioniert? Was hat der IT-Betrieb in den Fällen a.-c. jeweils zu tun?

b) Welche Konsequenzen ergeben sich, wenn die Schnittstelle zwischen Personalabteilung und IT-Betrieb nicht funktioniert? Betrachten Sie wieder a.-c. einzeln!

5. Passwort-Sicherheit:

a) Es gibt immer noch Service-Provider, die Kundenpasswörter unverschlüsselt speichern. Was ist daher bei der Nutzung von Passwörtern im Internet besonders wichtig?

b) Selbst wenn Service-Provider Passwörter verschlüsselt speichern: Oftmals werden die Server gehackt und die Dateien mit den Passwort-Hashes abgezogen. Nennen Sie 3 Maßnahmen, um das „Knacken“ solcher Dateien mit PW-Hashes zu erschweren.

c) Welche Problematik besteht beim PW-Reset per E-Mail.

d) Oft wird der PW-Reset durch ein organisatorisches „Challenge-Response“ geschützt. Wodurch kann dabei Sicherheit gegenüber Social-Engineering erhöht werden?

Übungsaufgaben zum Thema Verfügbarkeit und Notfallvorsorge

1. Vergleichen Sie für die Vollsicherung, die differenzielle und die inkrementelle Sicherung jeweils
   - Zeit bzw. Aufwand, den eine Datensicherung erfordert,
   - Zeit bzw. Aufwand, die eine Wiederherstellung erfordert
   - den Verbrauch an Speichermedien

2. a) Ein Dienst habe eine MTBF von 2 Jahren. Wie hoch darf die MTTR maximal sein, um eine Verfügbarkeit von „4 Nines“ zu erreichen?

   b) Ein Dienst habe eine Verfügbarkeit von 99%. Berechnen Sie die zu erwartende Ausfallzeit pro Jahr, pro Woche und pro Tag.

   c) Weshalb ist für einen IT-ler eine MTBF aussagekräftiger als eine Verfügbarkeit?

3. In der Vorlesung wurde das Großvater (monatlich) – Vater (wöchentlich) – Sohn (täglich) Generationenprinzip erläutert. Der Einfachheit halber nehmen wir an, dass für jede Datensicherung (egal ob voll oder inkrementell) ein Datenträger benötigt wird. Wieviel Datenträger benötigen Sie insgesamt, wenn Sie gemäß dem Generationenprinzip Datensicherungen der letzten 6 Monate vorhalten wollen?

4. Gegeben Sei ein Plattensystem mit einer MTBF (mean time between failure) von 364 Tage. Die MTTR (mean time to repair) ist (a) bei Herstellerwartung 3 Tage, (b) bei vorhandenen Ersatzplatten 0,5 Tage

a) Berechnen Sie für ein einzelnes Plattensystem: Wie hoch ist die Verfügbarkeit in Prozent? Wie hoch ist die theoretische mittlere Downtime pro Jahr?

b) Berechnen Sie die Größen für ein Striping über 3 Platten.

c) Berechnen Sie die Größen für eine Plattenspiegelung über 2 Platten.

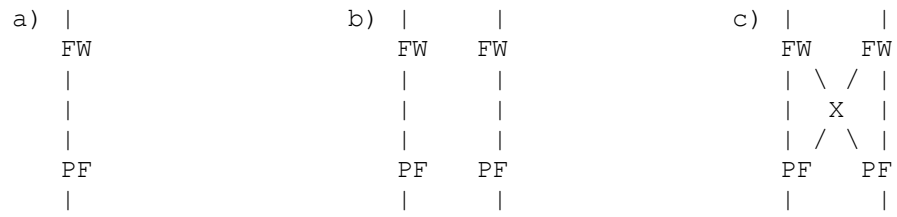
d) Berechnen Sie die Größen für RAID5 über 3 Platten

5. Zur Absicherung eines Internet-Übergangs werden Proxies (FW) und Paketfilter (PF) eingesetzt. Der Proxy hat eine Ausfallwahrscheinlichkeit von A_{FW}=1%, der PF eine von A_{PF}=0,5%. Berechnen Sie die Ausfallwahrscheinlichkeit

a) … der einfachen Reihenschaltung von FW und PF

b) … einer doppelten Reihenschaltung von FW und PF.

c) … einer doppelten Reihenschaltung von FW und PF mit Kreuzung.



d) In den Berechnungen wird davon ausgegangen, dass die Ereignisse statistisch unabhängig sind. Ist das realistisch?

Übungsaufgaben zur Organisation

1. Fernwartung

In einer Firma wird ein System mit vertraulichen internen Daten betrieben. Das System wir von einem Service-Dienstleister über das Internet gewartet (remote administration).

a) Nennen Sie einige relevante Sicherheitsanforderungen (auch org.) für das Szenario.

b) Sie arbeiten in der Revision des Unternehmens und sollen die Sicherheit der Fernwartung prüfen. Geben Sie zu jeder der drei Prüfebenen der sicherheitstechnischen Revision kurz mögliche Prüfungen zu den unter a) genannten Maßnahmen an.