Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 4. Übung im SoSe 2011:
IT-Sicherheit (1)

4.1 Beispiele für Bedrohungen der IT-Sicherheit

Aufgabe:

- Die mehrseitige IT-Sicherheit bestimmt sich anhand der Einhaltung der Sicherheitsziele:
  - ° Verfügbarkeit
  - ° Integrität
  - ° Vertraulichkeit
  - ° Zurechenbarkeit (im Sinne von Authentizität)
  - ° Rechtsverbindlichkeit (im Sinne von Nachweisbarkeit)

  Konstruieren Sie je ein Beispiel für eine Bedrohung der einzelnen Sicherheitsziele und begründen Sie, warum die von Ihnen angegebene Bedrohung für die Gewährleistung des betreffenden Sicherheitszieles gefährlich ist!

4.1 Beispiele für Bedrohungen der IT-Sicherheit (1)

Bedrohung der Verfügbarkeit:

- **Denial-of-Service-Angriff** kann IT-System zur Überlastung bringen, so dass der auszuführende Dienst nicht mehr seiner eigentlichen Funktion nachkommen kann

Bedrohung der Integrität:

- **Virenangriff** kann dazu führen, dass beim Aufruf eines Files Daten verändert werden, so dass die gespeicherten Daten nicht mehr originalgetreu und unverfälscht sind

Bedrohung der Vertraulichkeit:

- Network Analyzer (**Sniffing**) können dazu genutzt werden, dass eingehender Datenverkehr unbefugt mitprotokolliert wird, so dass die gespeicherten Daten für Dritte nicht mehr geheim sind

4.1 Beispiele für Bedrohungen der IT-Sicherheit (2)

Bedrohung der Zurechenbarkeit (Authentizität):

- **Session Hijacking** kann dazu führen, dass ein Angreifer eine bestehende Verbindung übernimmt und unbemerkt einen Kommunikationspartner ersetzt, so dass der Kommunikationspartner nicht korrekt erkannt wird

Bedrohung der Rechtsverbindlichkeit:

- **Web-Defacing** kann dazu führen, dass einem Angreifer unbefugt Zugriffsrechte zugebilligt werden, da der Nutzer optisch den Eindruck hat, die korrekte Web-Site geladen zu haben, so dass tatsächlich die Identität eines Kommunikationspartners nicht sicher festgestellt werden kann

4.2 Beispiele für Verwundbarkeiten von IT-Systemen

Aufgabe:

- Geben Sie für ein frei gewähltes IT-System eine potentielle Verwundbarkeit an, über die die unter 4.1 angegebene Bedrohung jeweils zu einer erfolgreichen Schädigung des IT-Systems bzw. der dort gespeicherten Daten führen kann.

4.2 Beispiele für Verwundbarkeiten von IT-Systemen (1)

Anmerkung:

***IT-System** = systematisch verbundene informationstechnische Komponenten*

*Für die Lösung wurde ein **Web-Server** als IT-System gewählt*

- Eine DoS-Attacke kann z.B. bei einem Web-Server zum Erfolg führen, wenn dieser ohne Firewall betrieben wird (oder diese keine sinnvollen Regeln aufweist) → **mangelhafter Firewall-Schutz** oder die Verbindung zum Web-Server nicht hochverfügbar ausgelegt ist → **fehlende Hochverfügbarkeit** oder kein adäquates Berechtigungskonzept auf dem Web-Server eingerichtet wurde, indem z.B. noch Default-Passwörter vorhanden sind → **schlechtes Passwort-Management**

4.2 Beispiele für Verwundbarkeiten von IT-Systemen (2)

- Ein Virenangriff kann z.B. bei einem Web-Server zum Erfolg führen, wenn dieser ohne wirksamen Virenschutz betrieben wird (z.B. keine automatisierte tägliche Aktualisierung) → **unzureichender Virenschutz** oder der Web-Server nicht vom LAN abgeschottet ist oder auf dem Web-Server selbst andere Tätigkeiten (z.B. Bearbeitung eingegangener Mails) ausgeführt werden → **unzureichende Netzwerksegregation**
- Sniffing kann z.B. bei einem Web-Server zum Erfolg führen, wenn vertraulicher Datenverkehr unverschlüsselt oder nur mäßig verschlüsselt übertragen wird → **unzureichende Transportverschlüsselung** oder der Raum, in dem der Web-Server steht, nicht wirksam unterbindet, dass man sich dort einstöpseln kann → **unzureichender Zutrittsschutz**

4.2 Beispiele für Verwundbarkeiten von IT-Systemen (3)

- Ein Session Hijacking kann z.B. bei einem Web-Server zum Erfolg führen, wenn beim Verbindungsaufbau via TCP kein Pseudozufallszahlengenerator verwendet wird → **schwache Authentifizierung** oder eine Session unbegrenzt ablaufen kann → **fehlende Timeout-Funktion**
- Ein **Website-Defacing** kann z.B. bei einem Web-Server zum Erfolg führen, wenn ein Web-Server z.B. mittels Speicherüberlauf übernommen werden konnte → **Buffer-Overflow** oder ein Web-Seiten-Aufruf gezielt umgeleitet wurde → **DNS-Cache-Poisoning** (Anm.: i.d.R. zu aufwändig für Angreifer, da in vielen Fällen bereits eine Phishing-Mail ausreicht, dass auf eine manipulierte Adresse geklickt wird)

4.3 Empfohlene Gegen-maßnahmen für Security

Aufgabe:

- Welche Maßnahme(n) würden Sie dem IT-Leiter empfehlen, der den von Ihnen unter 4.1 angegebenen Bedrohungen unter Beachtung der von Ihnen angegebenen Verwund-barkeit aus 4.2 angemessen zu begegnen hat?

4.3 Empfohlene Gegen-maßnahmen für Security (1)

Maßnahmen gegen Bedrohungen der Verfügbarkeit:

- Denial-of-Service-Angriff durch mangelhaften Firewall-Schutz → Web-Server in DMZ ansiedeln & Firewall-Regeln nach Stand der Technik formulieren
- Denial-of-Service-Angriff durch fehlende Hochverfügbarkeit → Aufbau redundanter und parallelisierter Technik, die sich vorzugsweise in getrennten Räumen befindet
- Denial-of-Service-Angriff durch schlechtes Passwortmanagement → Dienstanweisung erstellen, dass voreingestellte Start-Kennwörter stets abgeändert werden und dabei die Komplexitätsanforderungen erfüllt werden

4.3 Empfohlene Gegen-maßnahmen für Security (2)

Maßnahmen gegen Bedrohungen der Integrität:

- Virenangriff durch unzureichenden Virenschutz
  → Einsatz eines mindestens tagesaktuellen Virenscanners, der automatisch vorhandene Updates von nachgewiesen vertrauenswürdigen Webseiten herunterlädt
- Virenangriff durch unzureichende Netzwerksegregation
  → Einrichtung separierter Schutzzonen, die nicht durch Regellücken in Firewalls (oder aus Bequemlichkeit) umgangen werden können

4.3 Empfohlene Gegen-maßnahmen für Security (3)

Maßnahmen gegen Bedrohungen der Vertraulichkeit:

- Sniffing durch unzureichende Transportverschlüsselung
  → Versand vertraulicher Dokumente ausschließlich unter Ausnutzung einer Verschlüsselung nach dem Stand der Technik
- Sniffing durch unzureichenden Zutrittsschutz
  → Einrichtung einer Schutzzone für den Serverraum (und die jeweiligen Verteilerkästen/Patchschränke), so dass sichergestellt ist, dass lediglich befugte Personen Zutritt erlangen können

4.3 Empfohlene Gegen-maßnahmen für Security (4)

Maßnahmen gegen Bedrohungen der Zurechenbarkeit:

- Session Hijacking durch schwache Authentifizierung
  → Sicherstellung, dass ein echter Pseudozufallszahlengenerator verwendet wird
- Session Hijacking durch fehlende Timeout-Funktion
  → Einrichtung einer Timeout-Funktion in der genutzten Web-Applikation

4.3 Empfohlene Gegen-maßnahmen für Security (5)

Maßnahmen gegen Bedrohungen der Rechtsverbindlichkeit:

- Web-Defacing durch Buffer-Overflow
  → Abfangen von Steuerungssymbolen bei Befehlsabarbeitung und Verwendung stabiler Bibliotheksfunktionen, die nicht durch längen-bedingte Angaben zu einem Überschreiben unvorherbestimmter Speicherblöcken führen
- Web-Defacing durch DNS-Cache-Poisoning
  → den eigenen DNS-Server als Secure Proxy (statt als Cache Proxy) konfiguieren

4.4 IT-Grundschutz Web-Server (1)

Schicht	Baustein	Maßnahme
Übergeordnete Aspekte	B 1.3 Notfallmanagement	M 6.111 Leitlinie zum Notfallmanagement und Übernahme der Gesamtverantwortung durch die Leitungsebene
		M 6.112 Aufbau einer geeigneten Organisationsstruktur für das Notfallmanagement
		M 6.114 Erstellung eines Notfallkonzepts
		M 6.118 Überprüfung und Aufrechterhaltung der Notfallmaßnahmen

4.4 IT-Grundschutz Web-Server (2)

Schicht	Baustein	Maßnahme
Übergeordnete Aspekte	B 1.4 Datensicherungs-konzept	M 6.36 Festlegung des Minimaldatensicherungs-konzeptes
		M 2.137 Beschaffung eines geeigneten Daten-sicherungssystems
		M 2.41 Verpflichtung der Mitarbeiter zur Daten-sicherung
		M 6.37 Dokumentation der Datensicherung
		M 6.20 Geeignete Aufbe-wahrung der Backup-Datenträger

4.4 IT-Grundschutz Web-Server (3)

Schicht	Baustein	Maßnahme
Übergeordnete Aspekte	B 1.4 Datensicherungs-konzept	M 6.22 Sporadische Über-prüfung auf Wiederher-stellbarkeit von Daten-sicherungen
		M 6.32 Regelmäßige Datensicherung
		M 6.41 Übungen zur Datenrekonstruktion
	B 1.8 Behandlung von Sicherheitsvorfällen	M 6.58 Etablierung einer Vorgehensweise zur Behandlung von Sicher-heitsvorfällen
		M 6.121 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen

4.4 IT-Grundschutz Web-Server (4)

Schicht	Baustein	Maßnahme
Übergeordnete Aspekte	B 1.8 Behandlung von Sicherheitsvorfällen	M 6.59 Festlegung von Verantwortlichkeiten bei Sicherheitsvorfällen
		M 6.60 Festlegung von Meldewegen für Sicherheitsvorfälle
		M 6.125 Einrichtung einer zentralen Kontaktstelle für die Meldung von Sicherheitsvorfällen
		M 6.64 Behebung von Sicherheitsvorfällen
		M 6.65 Benachrichtigung betroffener Stellen bei Sicherheitsvorfällen

4.4 IT-Grundschutz Web-Server (5)

Schicht	Baustein	Maßnahme
Übergeordnete Aspekte	B 1.8 Behandlung von Sicherheitsvorfällen	M 6.130 Erkennen und Erfassen von Sicherheitsvorfällen
		M 6.131 Qualifizieren und Bewerten von Sicherheitsvorfällen
		M 6.132 Eindämmen der Auswirkung von Sicherheitsvorfällen
		M 6.133 Wiederherstellung der Betriebsumgebung nach Sicherheitsvorfällen

4.4 IT-Grundschutz Web-Server (6)

Schicht	Baustein	Maßnahme
Infrastruktur	B 2.3 Büroraum	M 2.17 Zutrittsregelung und -kontrolle
		M 1.15 Geschlossene Fenster und Türen
		M 1.23 Abgeschlossene Türen
		M 1.46 Einsatz von Diebstahl-Sicherungen
	B 2.7 Schutzschränke	M 1.7 Handfeuerlöscher
		M 2.311 Planung von Schutzschränken
		M 2.95 Beschaffung geeigneter Schutzschränke

4.4 IT-Grundschutz Web-Server (7)

Schicht	Baustein	Maßnahme
Infrastruktur	B 2.7 Schutzschränke	M 1.40 Geeignete Aufstellung von Schutzschränken
		M 2.17 Zutrittsregelung und -kontrolle
		M 2.21 Rauchverbot
		M 3.20 Einweisung in die Bedienung von Schutzschränken
		M 1.15 Gechlossene Fenster und Türen
		M 2.96 Verschluss von Schutzschränken
		M 2.97 Korrekter Umgang mit Codeschlössern

4.4 IT-Grundschutz Web-Server (8)

Schicht	Baustein	Maßnahme
Infrastruktur	B 2.12 IT-Verkabelung	M 1.20 Auswahl geeigneter Kabeltypen unter physikalisch-mechanischer Sicht
		M 1.21 Ausreichende Trassendimensionierung
		M 2.395 Anforderungsanalyse für die IT-Verkabelung
		M 5.2 Auswahl einer geeigneten Netz-Topologie
		M 5.3 Auswahl geeigneter Kabeltypen unter kommunikationstechnischer Sicht

4.4 IT-Grundschutz Web-Server (9)

Schicht	Baustein	Maßnahme
Infrastruktur	B 2.12 IT-Verkabelung	M 1.9 Brandabschottung von Trassen
		M 1.68 Fachgerechte Installation
		M 5.4 Dokumentation und Kennzeichnung der Verkabelung
		M 5.5 Schadensminimierende Kabelführung
		M 5.1 Entfernen oder Deaktivieren nicht benötigter Leitungen

4.4 IT-Grundschutz Web-Server (10)

Schicht	Baustein	Maßnahme
IT-Systeme	B 3.101 Allgemeiner Server	M 2.315 Planung des Servereinsatzes
		M 2.316 Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server
		M 5.10 Restriktive Rechtevergabe
		M 2.204 Verhinderung ungesicherter Netzzugänge
		M 2.318 Sichere Installation eines Servers
		M 4.7 Änderung voreingestellter Passwörter
		M 4.15 Gesichertes Login

4.4 IT-Grundschutz Web-Server (11)

Schicht	Baustein	Maßnahme
IT-Systeme	B 3.101 Allgemeiner Server	M 4.16 Zugangsbeschränkungen für Accounts und / oder Terminals
		M 4.17 Sperren und Löschen nicht benötigter Accounts und Terminals
		M 4.237 Sichere Grundkonfiguration eines IT-Systems
		M 2.22 Hinterlegen des Passwortes
		M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

4.4 IT-Grundschutz Web-Server (12)

Schicht	Baustein	Maßnahme
IT-Systeme	B 3.101 Allgemeiner Server	M 4.24 Sicherstellung einer konsistenten Systemverwaltung
		M 4.238 Einsatz eines lokalen Paketfilters
		M 4.239 Sicherer Betrieb eines Servers
		M 2.320 Geregelte Außerbetriebnahme eines Servers
		M 6.24 Erstellen eines Notfall-Bootmediums
		M 6.96 Notfallvorsorge für einen Server

4.4 IT-Grundschutz Web-Server (13)

Schicht	Baustein	Maßnahme
IT-Systeme	B 3.201 Allgemeiner Client	M 2.321 Planung des Einsatzes von Client-Server-Netzen
		M 2.322 Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz
		M 4.237 Sichere Grundkonfiguration eines IT-Systems
		M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates
		M 3.18 Verpflichtung der Benutzer zum Abmelden nach Aufgabenerfüllung

4.4 IT-Grundschutz Web-Server (14)

Schicht	Baustein	Maßnahme
IT-Systeme	B 3.201 Allgemeiner Client	M 4.2 Bildschirmsperre
		M 4.3 Einsatz von Viren-Schutzprogrammen
		M 4.238 Einsatz eines lokalen Paketfilters
		M 4.241 Sicherer Betrieb von Clients
		M 2.323 Geregelte Außer-betriebnahme eines Clients
		M 6.24 Erstellen eines Notfall-Bootmediums
		M 6.32 Regelmäßige Datensicherung

4.4 IT-Grundschutz Web-Server (15)

Schicht	Baustein	Maßnahme
IT-Systeme	B 3.301 Sicherheitsgate-way (Firewall)	M 2.70 Entwicklung eines Konzepts für Sicherheits-gateways
		M 2.71 Festlegung einer Policy für ein Sicherheits-gateway
		M 2.73 Auswahl geeigne-ter Grundstrukturen für Sicherheitsgateways
		M 2.74 Geeignete Aus-wahl eines Paketfilters
		M 2.75 Geeignete Aus-wahl eines Application-Level-Gateways

4.4 IT-Grundschutz Web-Server (16)

Schicht	Baustein	Maßnahme
IT-Systeme	B 3.301 Sicherheitsgate-way (Firewall)	M 2.299 Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway
		M 2.76 Auswahl und Ein-richtung geeigneter Filter-regeln
		M 2.77 Integration von Servern in das Sicher-heitsgateway
		M 2.78 Sicherer Betrieb eines Sicherheitsgateways
		M 4.47 Protokollierung der Sicherheitsgateway-Akti-vitäten

4.4 IT-Grundschutz Web-Server (17)

Schicht	Baustein	Maßnahme
IT-Systeme	B 3.301 Sicherheitsgate-way (Firewall)	M 5.39 Sicherer Einsatz der Protokolle und Dienste
		M 5.46 Einsatz von Stand-alone-Systemen zur Nut-zung des Internets
		M 5.59 Schutz vor DNS-Spoofing
		M 5.70 Adressumsetzung – NAT (Network Address Translation)
		M 5.120 Behandlung von ICMP am Sicherheitsgate-way

4.4 IT-Grundschutz Web-Server (18)

Schicht	Baustein	Maßnahme
Netze	B 4.1 Heterogene Netze	M 2.139 Ist-Aufnahme der aktuellen Netzsituation
		M 4.79 Sichere Zugriffs-mechanismen bei lokaler Administration
		M 5.2 Auswahl einer geeigneten Netz-Topologie
		M 5.13 Geeigneter Einsatz von Elementen zur Netzkoppelung
		M 5.60 Auswahl einer geeigneten Backbone-Technologie
		M 5.61 Geeignete physikalische Segmentierung

4.4 IT-Grundschutz Web-Server (19)

Schicht	Baustein	Maßnahme
Netze	B 4.1 Heterogene Netze	*M 4.7 Änderung voreingestellter Passwörter*
		M 4.82 Sichere Konfiguration der aktiven Netzkomponenten
		M 5.7 Netzverwaltung
		M 6.52 Regelmäßige Sicherung der Konfigurationsdaten aktiver Netzkomponenten

4.4 IT-Grundschutz Web-Server (20)

Schicht	Baustein	Maßnahme
Anwendungen	B 5.4 Webserver	M 2.172 Entwicklung eines Konzeptes für die Web-Nutzung
		M 2.173 Festlegung einer Web-Sicherheitsstrategie
		M 2.175 Aufbau eines Webservers
		M 2.271 Festlegung einer Sicherheitsstrategie für den WWW-Zugang
		M 2.272 Einrichtung eines WWW-Redaktionsteams
		M 5.69 Schutz vor aktiven Inhalten

4.4 IT-Grundschutz Web-Server (21)

Schicht	Baustein	Maßnahme
Anwendungen	B 5.4 Webserver	M 4.94 Schutz der WWW-Dateien
		M 4.95 Minimales Betriebssystem
		M 4.98 Kommunikation durch Paketfilter auf Minimum bechränken
		M 2.174 Sicherer Betrieb eines Webservers
		M 2.273 Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates

4.4 IT-Grundschutz Web-Server (22)

Schicht	Baustein	Maßnahme
Anwendungen	B 5.4 Webserver	M 4.33 Einsatz eines Viren-Suchprogramms bei Datenträgeraustausch und Datenübertragung
		M 4.78 Sorgfältige Durchführung von Konfigurationsänderungen
		M 5.59 Schutz vor DNS-Spoofing

Anmerkung: *kursiv* gedruckte Maßnahmen wurden bereits an vorangegangener Stelle aufgelistet. Diese werden also mehrfach (mit verschiedenem Blickwinkel!) berücksichtigt.

4.5 Verfügbarkeitsberechnung

Aufgabe:

- Die **Verfügbarkeit** eines IT-Systems kann als das Produkt der Verfügbarkeiten ihrer jeweiligen Komponenten verstanden werden, sofern diese Komponenten seriell miteinander verbunden sind. Diese werden unter Berücksichtigung etwaiger Ausfallzeiten in % gegenüber der vereinbarten Servicezeit berechnet:
  $$\text{Verfügbarkeit einer IT-Komponente} = \frac{(\text{vereinbarte Servicezeit} - \text{Ausfallzeit})}{\text{vereinbarte Servicezeit}} \; [\text{in } \%]$$
- Wenn hingegen Komponenten eines IT-Systems parallel betrieben werden, erhöht sich die Verfügbarkeit für diesen technisch redundanten Cluster in Abhängigkeit zur Anzahl der technisch redundant ausgelegten IT-Komponenten auf:
  $$\text{Redundanz-Verfügbarkeit} = 1 - (1 - \text{Verfügbarkeit}_{\text{normal}})^{\text{Anzahl}}$$
- A) Das zu betrachtende IT-System bestehe aus einem Server, der während der Betriebszeit zu 8 Stunden pro Jahr ausfällt, einem Client, der dabei zu 16 Stunden pro Jahr ausfällt, und einer Vernetzungskomponente, die während des Betriebs zu 24 Stunden pro Jahr ausfällt. Als Servicezeit sei ein 12-Stunden-Betrieb von Montag bis Freitag vereinbart worden. Wie hoch ist die Verfügbarkeit jeder einzelnen Komponente und des gesamten IT-Systems?
- B) Wie wirkt sich es sich auf die Verfügbarkeit des gesamten IT-Systems aus, wenn die Vernetzungskomponente mit einer identisch konfigurierten weiteren geclustert wird? Die Prozentangaben sind dabei auf drei Nachkommastellen anzugeben (also 12,345%).

4.5 Verfügbarkeitsberechnung

Teil A)

$V_{server} = (12*5*52 - 8)/(12*5*52) = 3112/3120 = 99{,}744\%$

$V_{client} = (12*5*52 - 16)/(12*5*52) = 3104/3120 = 99{,}487\%$

$V_{netz} = (12*5*52 - 24)/(12*5*52) = 3096/3120 = 99{,}231\%$

$V_{gesamt} = V_{server}*V_{client}*V_{netz} = 99{,}744\%*99{,}487\%*99{,}231\% = 98{,}469\%$

Teil B)

$V_{netzcluster} = 1 - (1 - V_{netz})^2 = 1 - (1 - 0{,}99231)^2 = 99{,}994\%$

$V_{gesamt\_neu} = V_{server}*V_{client}*V_{netzcluster} = 99{,}744\%*99{,}487\%*99{,}994\%$
$= 99{,}226\%$