Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2007:
Einführung in die IT-Sicherheit

5.1 Beispiele für Bedrohungen der IT-Sicherheit (1)

Bedrohungen der Verfügbarkeit:

- Höhere Gewalt (z.B. Unwetter) kann zum Ausfall des Servers/Rechenzentrum führen
- Sabotage kann wichtige Einrichtungen oder Verbindungen gezielt beschädigen/manipulieren
- Vandalismus kann wichtige Einrichtungen oder Verbindungen z.T. unkontrolliert zerstören oder in Mitleidenschaft ziehen
- Denial-of-Service-Angriff kann Betriebssystem zur Überlastung bringen
- Virenangriff kann zum Verlust wichtiger Dateien führen

→ IT-Systeme sind nicht mehr funktionsfähig, Daten sind nicht mehr vollständig

5.1 Beispiele für Bedrohungen der IT-Sicherheit (2)

Bedrohungen der Integrität:

- Man-in-the-Middle-Angriff (Maskerade) kann dazu führen, dass zwischengeschalteter Mittelsmann Daten manipulieren kann
- Virenangriff kann dazu führen, dass automatisch Daten-verändernde Makros aufgerufen werden

→ Daten sind nicht mehr originalgetreu und unverfälscht

5.1 Beispiele für Bedrohungen der IT-Sicherheit (3)

Bedrohungen der Vertraulichkeit:

- Trojanische Pferde können dazu führen, dass einzelne Speicher-Bereiche eingesehen werden können
- kompromittierende Abstrahlung ermöglicht in hinreichender Nähe das Aufzeichnen der Tätigkeiten am Rechner
- Keylogger oder Network Analyzer (sniffen) können dazu genutzt werden, dass eingehender Datenverkehr unbefugt mitprotokolliert wird

→ Daten sind nicht mehr geheim

5.1 Beispiele für Bedrohungen der IT-Sicherheit (4)

Bedrohungen der Zurechenbarkeit (Authentizität):

- Address Spoofing kann zur Vortäuschung einer falschen und damit vertrauenswürdigen Adresse führen, da i.d.R. physische Adressen nicht von Netzsoftware überprüft werden bzw. selbst manipulierbar sind

→ Kommunikationspartner ist nicht korrekt erkannt und damit auch nicht sicher, ob korrekte Daten empfangen wurden

- Password-Phishing kann dazu führen, dass Zugriffsrechte umgangen werden

→ Daten stammen nicht vom korrekten Kommunikationspartner

5.1 Beispiele für Bedrohungen der IT-Sicherheit (5)

Bedrohungen der Rechtsverbindlichkeit:

- DNS-Cache-Poisoning kann dazu führen, dass die korrekte IP-Adresse nicht erreicht wird
- Password-Phishing kann dazu führen, dass Zugriffsrechte umgangen werden
- Identitätsdiebstahl durch Social Engineering kann dazu führen, dass Angreifer Zugriffsrechte zugebilligt werden, die dieser nicht haben darf

→ Identität eines Kommunikationspartners ist nicht sicher

5.2 Empfohlene Gegenmaßnahmen (1)

Maßnahmen gegen Bedrohungen der Verfügbarkeit:

- Höhere Gewalt → Notfallvorsorgekonzept (z.B. Datenspiegelung, redundante Technik)
- Sabotage & Vandalismus → Einsatz von Überwachungstechniken
- Denial-of-Service-Angriff → Intrusion Detection System und restriktive Schreibrechte
- Virenangriff → Virenscanner

Maßnahmen gegen Bedrohungen der Integrität:

- Man-in-the-Middle-Angriff (Maskerade) → Verschlüsselung + Authentisierungsprotokolle
- Virenangriff → Virenscanner

5.2 Empfohlene Gegenmaßnahmen (2)

Maßnahmen gegen Bedrohungen der Vertraulichkeit:

- Trojanische Pferde → restriktive Schreibrechte und Installationsbeschränkung auf Original-Software vertrauenswürdiger Partner
- kompromittierende Abstrahlung → Tempest-Rechner
- sniffen → Intrusion Detection System und Verschlüsselung

Maßnahmen gegen Bedrohungen der Zurechenbarkeit:

- Address Spoofing → Proxy mit Firewall
- Password-Phishing → SPAM-Filter

Maßnahmen gegen Bedrohungen der Rechtsverbindlichkeit:

- DNS-Cache-Poisoning → DNS-Server abschotten und Einsatz eines VPN (verschlüsselte Verbindung) und Network Address Translation
- Password-Phishing → SPAM-Filter
- Identitätsdiebstahl → Schulung der Mitarbeiter

5.3 Informationstechnische Angriffsformen (1)

Hinweis:

- passiver Angriff = Angriff, ohne Daten zu verändern
- aktiver Angriff = Angriff mit Änderung von Daten

Beispiele:

- **Virenangriff** = aktiver Angriff:
  reproduktionsfähige Befehlsfolgen, die einen Wirt zur Infizierung benötigen, mit der Schadensfunktion nach ihrer Aktivierung beginnen und in File-, Makro- und Boot-Viren unterschieden werden können
- **Trojanisches Pferd** = aktiver Angriff:
  ausführbare Programme, die eine sichtbare Nutzenfunktion und eine verdeckte Schadensfunktion ausführen

5.3 Informationstechnische Angriffsformen (2)

Fortsetzung Beispiele:

- **Denial of Service** (DoS) = aktiver Angriff:
  Verbrauchen von Systemressourcen mit dem Ziel, dass der angegriffene Dienst nicht mehr seine Funktion erfüllen kann
- **Sniffing** = passiver Angriff:
  Mitloggen von Netzwerkverkehr, um insb. unsicher übertragene Passwörter abgreifen zu können
- **Keylogger** = passiver Angriff:
  Mitloggen der Tastaturanschläge, um insb. unsicher übertragene Passwörter abgreifen zu können
- **Password-Phishing** = passiver Angriff:
  Vortäuschen einer „vertrauenswürdigen“ Anforderung zur Angabe von Passwörtern o.Ä. (z.B. PIN & TAN)

5.3 Informationstechnische Angriffsformen (3)

2. Fortsetzung Beispiele:

- **Spoofing** = aktiver Angriff:
  Vortäuschen logischer Netzwerkadressen
- **Man-in-the-Middle-Attack** = aktiver Angriff:
  Einklinken in ein Netzwerk mit dem Ziel, dass eine Kommunikation zwischen beteiligten Netzwerkknoten über einen eingeschleusten oder gekaperten Netzwerkknoten stattfindet und ggf. manipuliert werden kann
- **Cross-Site-Scripting** = aktiver Angriff:
  Einbinden bösartigen Codes in in dynamischen Web-Seiten eingebettete Scriptbefehle, der vom Browser automatisch ausgeführt werden soll
- **...**

5.4 Sicherheitsziele & Kontrollbereiche

	Verfügbarkeit	**Integrität**	**Vertraulichkeit**	**Zurechenbarkeit**	**Rechtsverbindlichkeit**
Organisationskontrolle	X	X	X	X	X
Zutrittskontrolle	X		X		
Zugangskontrolle	X	X	X		
Zugriffskontrolle	X	X	X	X	X
Weitergabekontrolle	X	X	X	X	X
Eingabekontrolle		X		X	
Auftragskontrolle					X
Verfügbarkeitskontrolle	X				
Datentrennungskontrolle		X	X	X	X

5.5 Verfügbarkeitsberechnung

$Verfügbarkeit_{HW}$ = (24*7*52-8)/(24*7*52) = 8728/8736 = 99,9 %

$Verfügbarkeit_{BS}$ = (24*7*52-16)/(24*7*52) = 8720/8736 = 99,8 %

$Verfügbarkeit_{AP}$ = (24*7*52-24)/(24*7*52) = 8712/8736 = 99,7 %

$Verfügbarkeit_{IT} = Verfügbarkeit_{HW} * Verfügbarkeit_{BS} * Verfügbarkeit_{AP}$
<=> $Verfügbarkeit_{IT}$ = 99,9 % * 99,8 % * 99,7 % = 99,4 %
[genauer: $Verfügbarkeit_{IT} = (8728*8720*8712)/(8736)^3$ = 99,45 %]

Das IT-System ist zu 99,45 % der vereinbarten Servicezeit verfügbar!