

Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 5. Übung im SoSe 2008:
Gefährdungen der IT-Sicherheit

5.1 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

5.1 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

5.2 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**

5.2 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**

5.2 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)

5.3 Empfohlene Gegenmaßnahmen 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

5.3 Empfohlene Gegenmaßnahmen für Security (2)

Maßnahmen gegen Bedrohungen der Integrität:

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

5.3 Empfohlene Gegenmaßnahmen 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

5.3 Empfohlene Gegenmaßnahmen 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

5.3 Empfohlene Gegenmaßnahmen 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 längenbedingte Angaben zu einem Überschreiben unvorherbestimmter Speicherblöcken führen
- Web-Defacing durch DNS-Cache-Poisoning
→ den eigenen DNS-Server als Secure Proxy (statt als Cache Proxy) konfigurieren

5.4 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

5.4 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 insbesondere unsicher übertragene Passwörter abgreifen zu können
- **Keylogger** = passiver Angriff:
Mitloggen der Tastaturanschläge, um insbesondere unsicher übertragene Passwörter abgreifen zu können
- **Password-Phishing** = passiver Angriff:
Vortäuschen einer „vertrauenswürdigen“ Anforderung zur Angabe von Passwörtern o.Ä. (z.B. PIN & TAN)

5.4 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 bössartigen Codes in in dynamischen Web-Seiten eingebettete Scriptbefehle, der vom Browser automatisch ausgeführt werden soll
- ...

5.5 Empfohlene Gegenmaßnahmen für Safety (1)

- Brand → Notfallvorsorgekonzept (z.B. Datenspiegelung, redundante Technik, Ausfallrechenzentrum in räumlich ausreichender Entfernung)
- Stromausfall → Unterbrechungsfreie Stromversorgung
- Hardware-Defekt → regelmäßige Erneuerung korrosionsgefährdeter Hardware-Komponenten
- Software-Defekt → Einrichtung eines Testsystems getrennt vom Produktivsystem mit identischer Konfiguration
- Bedienungsfehler → Bereitstellung einer ausreichenden Dokumentation und Mitarbeiterschulung