Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 8. Übung im SoSe 2007:
Praktische Anwendungen zur IT-Sicherheit

8.1 Probleme bei VoIP

fernmelde-/datenschutzrechtliche Probleme:

- Kompromittierung der Unverletzlichkeit des Wortes und Mitschnitt von Kommunikationsverbindungen → Sniffing
- unzureichende Gewährleistung der Zugriffs-/Weitergabekontrolle
- Verhinderung des Zustandekommens der Kommunikation (z.B. durch Vortäuschen des Besetzzeichens)
- Abrechnungsbetrug durch Konfiguration eines 0190-Rufzugangs

sicherheitstechnische Probleme:

- (funktionsbedingte) Schwachstellen des IP greifen auch bei VoIP
  - ° Vortäuschen einer falschen Identität
  - ° Fälschung von Übermittlungsadressen
  - ° Fälschung von Registrierungsinformationen

  → Man-in-the-Middle-Attack bzw. Call-Hijacking
- DoS-Attacken mittels SYN-Flooding
- SPAM over Internet Telephony (SPIT)
- Verschlüsselung (via IPsec) kann zu unerwünschtem Zeitverzug führen

8.2 WLAN-Sicherheitsprobleme

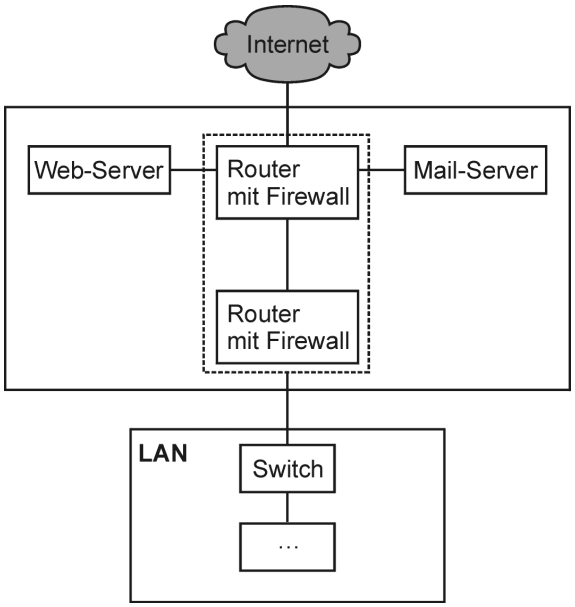
Sicherheitsprobleme:

- Auslieferungskonfiguration nur mit schwacher Sicherheit versehen
- Netzwerkname (Service Set Identifier = SSID) leicht zu ermitteln
- Media-Access-Control-Adresse leicht abhör- und manipulierbar
- Verschlüsselung „von Hand“
- bei Wired Equivalent Privacy (WEP) Schlüssel zu kurz & Initialisierung leicht zu berechnen → Authentisierung kann gesnifft werden
- Cyclic Redundancy Check (CRC) gewährleistet nicht Integrität
- unkontrollierte Funkwellen
- Störung durch andere elektromagnetische Funkwellen
- Bewegungsprofile erstellbar

Vorgaben zur Nutzung:

- Änderung der voreingestellten Standard-SSID
- Einrichtung von Virtual LANs (VLAN)
- Nutzung von Access Points vorzugsweise als closed network bzw. zumindest mit eingeschränkter Sicherheit (da SSID weiterhin leicht ermittelt werden kann) nur mittels eingetragener SSIDs im cloaked mode
- Verwendung des WPA2 mit AES-Verschlüsselung unter Ausnutzung von IEEE 802.11i → Authentifizierung mit (P)EAP
- Access Point außerhalb des LAN ansiedeln, damit Firewall LAN weiter schützen kann
- Verbindung mittels VPN via PPTP
- rudimentäre Paket-Integrität via TKIP

8.3 DMZ



8.4 Sicherheitskonzept Telearbeit (1)

- Festplatte des Laptops gemäß dem Stand der Technik verschlüsseln
- systemseitiges Abklemmen externer Laufwerke & Wechseldatenträger; Einrichtung eines Boot-Schutzes
- kein Zugriff auf Betriebssystemebene und Konfigurationen der eingesetzten IT-Komponenten (→ Nutzerrechte, keine Administrationsrechte)
- vorzugsweise Identifizierungs- und Authentisierungsmechanismus mittels Smartcard- oder Fingerabdruckverfahren
- monatliche Änderung der Zugangs- und Zugriffspassworte durch den Beschäftigten unter Einhaltung der Komplexitätsvorschriften
- Erschwerung mehrfach missglückter Neuanmeldeversuche (durch Geringhalten zulässiger Fehlversuche und sukzessive Erhöhung der Zeitabstände für erneute Versuche)
- Automatische Bildschirmsperre bei fehlender Aktivität von 10 Minuten und deren Aufhebung nur mittels Authentifizierung

8.4 Sicherheitskonzept Telearbeit (2)

- Konfiguration minimal entsprechend der zu erfüllenden Aufgaben
- Protokollierung aller sicherheitsrelevanten Aktivitäten
- Virenscanner so installieren, dass dieser bei jeder Anmeldung am LAN und in regelmäßigen Abständen auch während einer bestehenden Verbindung automatisch aktualisiert wird
- kein freier Zugriff auf das Internet
- Freischaltung nur der zur Aufgabenerfüllung zwingend erforderlichen Ports
- Kommunikation zwischen Laptop und LAN nur unter Ausnutzung einer dem Stand der Technik entsprechende starke Transportverschlüsselung (üblicherweise Triple-DES); ein Verbindungsaufbau darf nur nach ausdrücklicher Bestätigung durch den Beschäftigten erfolgen
- Absicherung einer erfolgreichen Datenübertragung mittels Quittierungsverfahren

8.4 Sicherheitskonzept Telearbeit (3)

- zur Telearbeit dürfen ausschließlich gestellte IT-Komponenten (Hardware und Software) eingesetzt, an den Einstellungen keine Änderungen vorgenommen und keine weiteren IT-Komponenten angeschlossen werden
- Zutrittsrecht des Arbeitgebers zum Telearbeitsplatz ist mit dem Beschäftigten zu vereinbaren
- Laptop ist in einem klar separierten und verschließbaren Arbeitszimmer so aufzustellen, dass keine unbefugte Einsichtnahme auf den Bildschirm (weder im Zuge des Betretens des betreffenden Arbeitszimmers noch durch Beobachtung durch etwaige Fenster) stattfinden kann
- streng vertrauliche Unterlagen dürfen außerhalb der Arbeitszeit bzw. Tätigkeit des betreffenden Beschäftigten ausschließlich in verschließbaren Behältnissen gelagert werden

8.5 Gegensätze von Datenschutz und IT-Sicherheit

- **Datenschutz**: Grundsatz der Datensparsamkeit
  IT-Sicherheit: Datensicherung durch Redundanz zur Ausfallsicherheit
- **Datenschutz**: Informationelles Selbstbestimmungsrecht
  IT-Sicherheit: Nachvollziehbarkeit und Überwachung von Aktionen
- **Datenschutz**: Transparenz der Verfahren
  IT-Sicherheit: Verschleierung von Sicherheitseinstellungen
- **Datenschutz**: Inhaltsebene der Daten im Vordergrund
  IT-Sicherheit: Transportebene der Daten im Vordergrund
- **Datenschutz**: Schutzbereich personenbezogene Daten
  IT-Sicherheit: Schutzbereich alle (Unternehmens-)Daten
- **Datenschutz**: Ausgangspunkt = Interesse von Betroffenen
  IT-Sicherheit: Ausgangspunkt = Interesse von Systembetreibern