

Kunsthochschule für Medien Köln
Atelier für Multimedia und Performance (Labor EXPORT)

**BECOMING AWARE OF SECURITY!
EIN WORKSHOP IN ANGEWANDTER
(UN)SICHERHEIT**

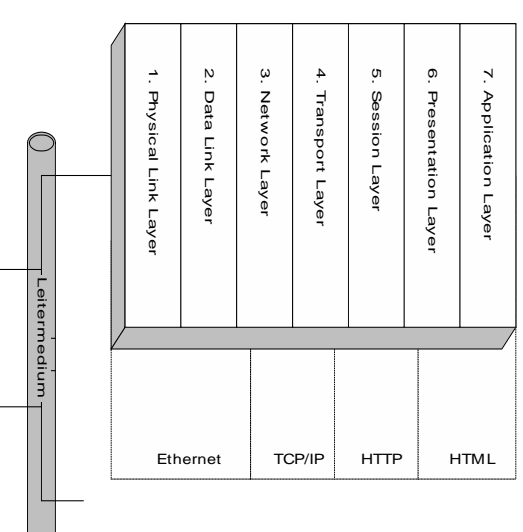
Matthias Leisi
matthias@astrum.ch
7. Februar 2001

Was ist Sicherheit (nicht)?

- Sicherheitsgefühl.
- Technische und Soziale Komponenten.
- Innen und Aussen.
- Sicherheitsdimensionen.

Netzwerk I: Modell

- Schichtenmodell als pädagogisches Konzept
- Keine strengen Grenzen in der Praxis
- Layer 8 und 9: Politik und Religion



Netzwerk II: TCP/IP

- Zur Vereinfachung beschränkt auf TCP/IP. Strassen und Hausnummern.
- IP-Adressen und Ports Dienste im Hintergrund.
- Routing und Nameserver
- Protokolle und Ports. Klartext (POP3) und verschlüsselt (HTTPS)

TCP-Datenpakete enthalten vor den eigentlichen Daten die IP-Adresse und den Port von Absender und Empfänger sowie einige weitere Verwaltungsinformationen.

Netzwerk III: Client und Server

- Jeder Rechner im Netz ist zugleich Client und Server.
- Server stellen verschiedene Dienste zur Verfügung (z.B. Mail, Web).
- Server ohne Überwachung sind ein Risiko für den Rest des Netzes.
- Server und Client müssen nicht zwingend direkt und synchron miteinander kommunizieren.

Typologie von Unsicherheiten

- Angriffe von Innen und von Aussen
- Awerness von Usern, Administratoren, Herstellern
- Vor- und Nachsorge
- → Ethisches Verhalten?

Unsicherheit I: Viren, Trojaner

- **Ausbreitung**
Mails, Programme, . . .
- **(Schadens-) Funktion**
Aufmerksamkeit, Löschen, Verändern, . . .
- **Tarnung**
Existenz, Funktion, Herkunft, . . .
- **Beliebige Kombinationen**

Kategorie: von Aussen, Awerness

Unsicherheit II: Social Engineering

”Hallo, hier spricht (unverständlich) von der Netzwerkadministration. Wir hatten ein Problem mit dem Server und müssen ihr Passwort haben, damit nicht alle ihre Daten verloren gehen.”

Kategorie: von Innen, Awerness

Unsicherheit III: DoS-Attacke

- Einzelne Dienste oder ganze Server lahmlegen.
- Zugriff ist erst nach manuellem Eingriff wieder möglich.
- Verteilte Attacken (DDoS) sind schwierig zu bekämpfen.
- Angriffe auch auf einzelne Clients.
Geschicht relativ häufig in Chats und anderen Orten sozialer Interaktion.

Kategorie: von Aussen, Prävention

Unsicherheit IV: Sniffing

- Mitschneiden des Datenverkehrs im eigenen Netzwerk.
- Klartext-Protokolle sehr ergiebig.
- Administratoren können teilweise noch einfacher mitlesen – sie können auf Dateien direkt zugreifen.

Kategorie: von Innen, Prävention und Administration

Unsicherheit V: Persönliche Daten

- Bewusste und unbewusste Preisgabe persönlicher Daten.
- Datenschutz(un)freundliche Technologien.
- Datenschutz ist ein Grundrecht auf Privatsphäre.

Kategorie: Awareness

Beispiel Viren: LOVEYOU

- Relativ harmlose Schadensfunktion
- Schnelle Verbreitung v.a. durch unvorsichtige User und ungeschickte Voreinstellungen von MS-Outlook.
- User Awareness? Vor ILY gab es schon Melissa und andere Viren/Trojaner.
- Hersteller Awareness? Automatismen und Transparenz.

Beispiel Viren: Aufbau ILOVEYOU

- Veränderung von Systemeinstellungen.
- Erzeugen einer HTML-Seite für Weiterverbreitung.
- Versenden via Mail (Outlook).
- Script- und Mediadateien auf erreichbaren Laufwerken verstecken und durch Kopie des Scripts ersetzen.
- Verbreitung via mIRC (Chatprogramm).

Beispiel Sniffing: Werkzeuge

- `tcpdump`
Mitlesen und abspeichern
- `strings`
Lesbare Zeichenketten extrahieren
- `grep`
Suche nach bestimmten Mustern

Diese oder ähnliche Werkzeuge sind für alle Plattformen verfügbar.

Beispiel Sniffing: How-To

- `tcpdump -n -s 1600 -w pop3.dump tcp port pop3`
Alle Datenpakete auf dem Standardport für POP3 mitschneiden und in Datei "pop3.dump" speichern.

- `strings pop3.dump | egrep 'USER|PASS'`

Lesbare Zeichenketten aus der Datei extrahieren und Benutzernamen und Passwörter ausgeben:

```
USER matthias . Leisi  
PASS sachichnicht
```

Nein, das sind keine realen Daten. Ja, das Resultat sieht tatsächlich so aus.

Beispiel Sniffing: Resultate

- **Mail I: Passwörter lesen**
Wer hat bei POP3 das gleiche Passwort wie auf seiner ec-Karte?
- **Mail II: Inhalte lesen**
Wer schreibt worüber mit wem?
- **Web: Zugriffe auf Webseiten**
Was hast du auf der Webseite zu suchen?

Beispiel Mobbing

- Änderungen in einem wichtigen Dokument vornehmen.
- Lesen aktueller Entwürfe.
- Fremde Ideen als eigene ausgeben.
- Insbesondere Administratoren haben vereinfacht Zugriff und damit höhere Verantwortung

Beispiel Persönlichkeitsprofile

- <http://mesa.rrzn.uni-hannover.de/> (Mailadressen)
"Metasuchmaschine", befragt andere Verzeichnisse.
- <http://www.deja.com/> (Usenet-Postings)
Bis vor einem Jahr war das *komplette* Usenet-Archiv seit ca. 1995 durchsuchbar.
- <http://www.google.com/> (Websuche)
Webseiten, archivierte Mailinglisten, . . .
- Erst die Kombination ergibt ein Persönlichkeitsprofil. Für kommerzielle Zwecke zu aufwändig.

Verschlüsselung

- Jede Ebene des Schichtenmodells ist angreif- und verschlüsselbar.
- Schlechte Verschlüsselung ist schlechter als keine Verschlüsselung, weil eine falsche Sicherheit vorgegaukelt wird.
- Jede Verschlüsselung hat Schwachstellen: mathematisch, Umsetzung, Administration, User, . . .
- Verschlüsselung \neq Geheimniskrämerei

Motivation von Angreifern

- Neugier: Sehen was möglich ist.
- Emotionen: Wut, Hass, Rache.
- Mangelnde Sozialkompetenz.
Wer in der U-Bahn Scheiben zerkratzt, greift auch Rechner an.
- Spieltrieb? Lerneffekt?

Pseudonym und Anonym

- Echte Anonymität gibt es nur selten.
- Hinter Trojanern sind Angreifer relativ sicher.
- Zugriff auf Logdateien von Providern haben im Prinzip nur Staatsanwaltschaften.

Prävention

- Vertrauenswürdigkeit der Administration.
- Massvolle(?) Überwachung und Kontrolle.
- Voreinstellungen im Hinblick auf Sicherheit.
- Konflikt zwischen Sicherheit und anderen Zielen (Komfort, Kosten, Geschwindigkeit, . . .).
- Awareness von Usern, Administratoren, Herstellern.

Was ist Sicherheit?

- Sicherheit ist kein Zustand, den man einmal erreichen kann, sondern ein Prozess.
- Sicherheit ist nicht von Programmen abhängig, sondern von einem Bewusstsein.
- Sicherheit ist eine Kosten / Nutzen-Abwägung.