

Security – oder auch nicht: Das schwächste Glied der Kette

Wolfgang Dautermann

January 13, 2009

1 Motivation

Computersicherheit wird immer wichtiger. Wir verwenden verschlüsselte Protokolle (SSH statt telnet, pop3s statt pop3, imaps statt imap und https statt http) – doch das ganze nützt nichts, wenn wir wichtige Fehlermeldungen, wie fehlerhafte Zertifikate, geänderte SSH-Host-Keys etc. gedankenlos "wegklicken" und ignorieren.

2 Geplante Struktur des Vortrags

- Netzwerkprotokolle
- Verschlüsselung mit SSL
- Gegenseitige Authentifizierung
- Arten von Zertifikaten
- Nicht erkannte Zertifikate
- Arten von Zertifikaten
- Zusammenfassung

3 Zielgruppe

Keine besonderen Vorkenntnisse notwendig, ev. sind elementare Netzwerk-Kenntnisse von Vorteil...

4 Praktische Vorführung

Wenn Zeit bleibt (und eine Netzwerkverbindung für meinen Laptop zur Verfügung steht), sind am Ende einige praktische Vorführungen geplant.