

IT-Security

# Maßnahmen in der Praxis

Technische Maßnahmen:

- Virusscanner
- Firewall
- VPN (Virtual Private Network)
- Verschlüsselung/Authentifizierung

Lothar v. Droste, SecuSoft GmbH

# Datenverlust – ein zufälliges Ereignis

Das Unwahrscheinliche ist wahrscheinlich

Aristoteles

Murphy's Law: If anything can go wrong – it will

# Grundansatz – IT-Sicherheit

- Datensensibilität entwickeln
- Organisatorische Maßnahmen  
Mechanische Sicherheit, Zutrittskontrolle,  
Zugriffsberechtigung, Ablaufrichtlinien
- Technische Maßnahmen  
Storage Management,  
Datensicherungskonzept
- IT-sicherheitstechnische Maßnahmen  
Virusscanner, Firewall, VPN, Verschlüsselung

# Szenario

## Firma A

15 Mitarbeiter,  
Fileserver, Email-Server, Ethernet LAN und Internet-Zugang  
3 Gruppen: Vertrieb, Technik, Geschäftsleitung

## Firma A(ext.)

2 Mitarbeiter mit Home Office

## Partner B

- Allgemeine Korrespondenz
- Arbeiten an gemeinsamen Projekten
- Austausch von sensiblen Daten, wie technische Entwicklungen

## Temporäre Partner C und D

Gemeinsame Angebote, Austausch von sensiblen Daten

# Sicherheitsmaßnahmen in Stufen

1. Virenschutzprogramm
2. Firewall
3. VPN – VPN-Client
4. Verschlüsselung – Email-Kommunikation
5. Verschlüsselung – Gruppenverschlüsselung
6. Passwort / Biometrische Erkennung
7. Digitale Signatur / Trustcenter

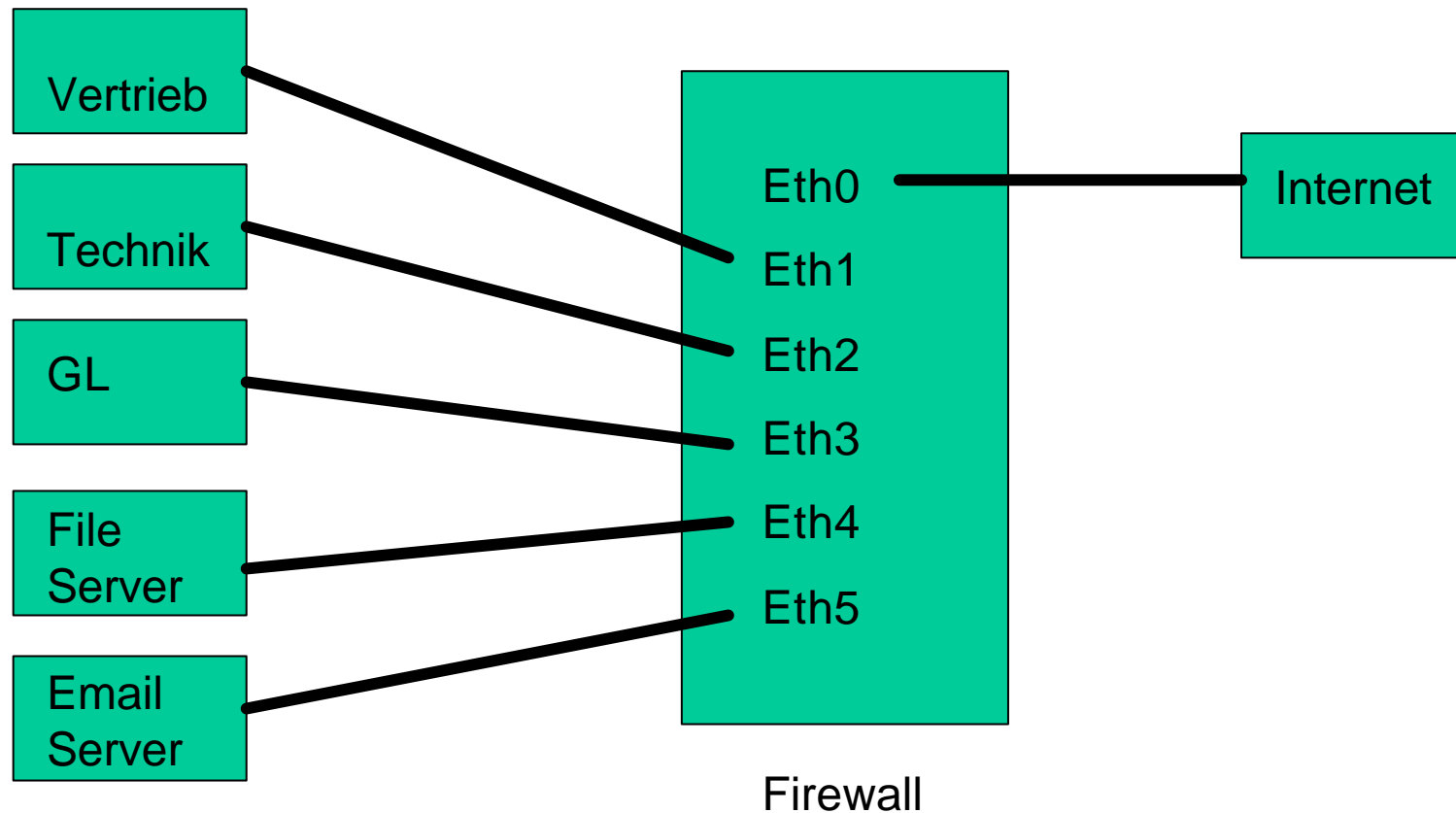
# 1. Virenschutzprogramm

- a. Im Hintergrund auf allen PCs im Netz
- b. Laufende Aktualisierung
- c. Auswahl eines Herstellers für die PCs
- d. Auswahl eines weiteren Herstellers für die Firewall

## 2. Firewall

- a. Betriebssystem der Firewall-Software ist LINUX
- b. Separiert Netzgruppen über Ethernetkarten
- c. Vergibt Dienste und Verbindungsrechte
- d. **IDS** (Intrusion Detection System) schützt vor unberechtigten Zugriffen und führt Statistik
- e. Virenschutzprogramm für die durchgehenden Datenpakete

## 2.1 Firewall im Netz



## 2.2 Firewall einrichten

- a. Definition von Rechnergruppen
- b. Definition der Verbindungen und Dienste (Regeleditor)
- c. Überprüfung aktiv vergebener Dienste
- d. Erweitern des Netzes
- e. Statistik – abgewiesene unberechtigte Zugriffe
- f. Statistik – Top-Listen im WWW
- g. Statistik – Traffic über die Firewall

# 3. VPN – VPN-Client

Stellt eine virtuelle exklusive Verbindung im Internet dar

Zwei sichere Verfahren:

- a. PPTP (Point-to-Point Tunneling Protocol)
- b. IPsec (IP Security)

Lösung für Home Office: Server-Client-Verbindung

Lösung für Firmenanbindung: Server-Server-Verbindung

# 4. Verschlüsselung – Emails

## Verschlüsselungsverfahren mit Passwort

- symmetrische Verfahren: 3DES, BlowFish, IDEA +++
- selbst extrahierende Programmdatei möglich, z.B. PGP, Safeguard

## Verschlüsselungsverfahren mit Authentisierung

- in Verbindung mit einem asymmetrischen Verfahren: RSA, AES
- Es muss ein PKI (Public Key Infrastructure) Management aufgebaut werden, z.B. Safeguard, MailCrypt

# 4.1 Verschlüsselung - Techniken

## Symmetrisches Verschlüsselungsverfahren

Schlüssel: 3DES (Länge 192 Bit)

Übertragung des Schlüssels mit gleichem Verfahren,  
jedoch mit Passwort als Zufallszahl

Verschlüsselung der Nachricht mit dem 3DES-Schlüssel

Ergänzende Hash-Funktion bestätigt die Unverfälschtheit der Datei  
(Integrität)



# 5. Gruppenverschlüsselung

- Schutz vor Datenmissbrauch
- - Über Festplattenverschlüsselung
- - Über lokale Datenverschlüsselung

-Gruppenverschlüsselung

als Beispiel automatisch verschlüsselter Daten.

# 5.1 Aufbau und Ablauf

## 1. Administrator:

- a. Anlegen der Gruppen mit den Gruppenmitgliedern
- b. Definition eine Gruppenleiters
- c. Definition der Verschlüsselungsverzeichnisse

## 2. Gruppenleiter

- a. Erzeugen seines asymmetrischen Schlüsselpaars
- b. Ablage des geheimen Schlüssels Passwort verschlüsselt auf ein Token
- c. Automatische Erzeugung eines symmetrischen Schlüssels
- d. Verschlüsselt mit dem privaten Schlüssel des Gruppenleiters auf File Server

# 5.1 Aufbau und Ablauf

## 3. Gruppenmitglied

- a. Erzeugen seines asymmetrischen Schlüsselpaares
- b. Ablage Passwort geschützt auf einem Token
- c. Anfrage beim Gruppenleiter für den symmetrischen Schlüssel mit Übersendung seines öffentlichen Schlüssels
- d. Der Gruppenleiter übersendet den symmetrischen Schlüssel authentisch verschlüsselt an das Gruppenmitglied
- e. Nach Neueinwahl in das Programm wird automatisch dieser symmetrische Schlüssel verschlüsselt auf dem File Server abgelegt

## 4. Arbeiten

Arbeiten auf den vorgesehenen Verzeichnissen  
→ Daten automatisch mit Gruppenschlüssel verschlüsselt

# 6. Passwort - Biometrie

## - Gefahren beim Passwort:

- - zu einfach
- - leichtes Ausspähen
- - Ist keine wirkliche Zuordnung zur Authentifizierung einer Person

## - Biometrischer Ersatz als Passwort

- - Authentischer Beweis für den Zugriff einer Person
- - Passwort mit beliebiger Länge hinterlegbar (Single-Sign-On)
- - Fingerprint Template (Minutiae-File)  
kann z.B. mit privatem Schlüssel auf einem Token hinterlegt werden

# 7. Digitale Signatur / Trustcenter

- digitale Signatur = Verschlüsseln mit privaten Schlüssel des Absenders
- digitale Signatur benötigt
  - eindeutige Zuordnung des öffentlichen Schlüssels zum Absender (Zertifikat)
  - Aufbau einer PKI (Public Key Infrastructure)
  - Dies geschieht über ein Trustcenter mit Zertifizierungsstelle (CA) und z.B. dem Dienst Zeitstempel zertifizieren
  - Jede Digitale Signatur läuft über ein Trustcenter

# Ende – IT-Sicherheit

Sicherheitstechnische Maßnahmen in der Praxis:

- Virusscanner
- Firewall
- VPN (Virtual Private Network)
- Verschlüsselung/Authentifizierung
- Biometrische Erkennung
- Digitale Signatur / Trustcenter