



Dienste zur Kommunikation

- Die Killer-Applikation des Internet heisst elektronische Post
- Das grösste verteilte Dokumenten-System des Internet heisst World Wide Web
- Mit beiden kann man hochgradig produktiv sein, gut kommunizieren und arbeiten ...
- ... und jede Menge Missbrauch treiben!

**Email, Proxy, Spamfilter, Virenschutz
(und ein bisschen DHCP)**



Was ist E-Mail?

- Asynchrone Kommunikation
- Endanwender benutzen einen E-Mail Client
- Senden und Empfangen läuft über verschiedene Protokolle und somit Server-Anwendungen:
 - smtp: Senden von Mail (RFC 821)
 - pop / imap: Empfangen und Verwalten von Mail, RFC's: 1939 (pop3) und 2060 (imap4)
- Alles **KLARTEXT!!!**



Senden von Mail

- Clients z.B.:
 - Outlook (Microsoft, GUI, IMAP und POP)
 - Mulberry (portabel, GUI, vollst. IMAP-Impl.)
 - Thunderbird, Mozilla, Netscape (allround)
 - pine, elm (CUI) ...
- Server z.B.:
 - sendmail oder postfix für Linux / UNIX
 - Exchange für MS Windows



Ablauf des Sendens

- Client erzeugt E-Mail, bestehend aus Headern und Body
- Client nimmt Kontakt mit dem (fest eingestellten) smtp-Server auf
- Server übernimmt Header, prüft Zulässigkeit und Korrektheit
- Server übernimmt Body und queued Mail
- Client terminiert



Probleme beim Senden

- Email-Header können gefälscht werden
- IP-Adressen können gefälscht werden („gespoofed“)
- Jeder smtp-Server fügt seine Header hinzu, wenn er regulär arbeitet (muss er nicht)
- Sind die Header gefälscht, kann man nichts zurückverfolgen
- Inhalte können mitgelesen werden



Prüfungen / Schutz smtp

- Keine Mails annehmen, die nicht aus der eigenen Domain stammen oder nicht für die eigene Domain bestimmt sind („relaying“)
- Prüfen, ob die Inhalte der Header plausibel sind:
 - Domains auflösbar?
 - IP-Adressen sinnvoll? (Schwierig!)
 - Header komplett?
 - Absender authentifiziert?



Ablauf Weiterleitung / Zustellen

- smtp-Server analysiert den Empfänger, z.B. michael.jackson@neverland.com
- Sind wir selbst der Empfänger? Dann lokal zustellen.
- Nicht lokal? Dann per DNS-Abfrage den zuständigen Mail-Server und eventuelle Stellvertreter ermitteln (MX-Records für die Empfänger-Domain).
- In definierter Reihenfolge mit den MX-Servern Kontakt aufnehmen und die Mail übermitteln.



Email-Empfang - Serverseite

- pop3 ist ein altes Protokoll, vergleichsweise wenig leistungsfähig und unsicher, aber weit verbreitet und leicht zu implementieren.
- Mit pop3 kann man Mail von einem Server holen und sie auf dem Client verarbeiten.
- IMAP4 verwaltet die Mails und ggf. eine ganze Ordner-Hierarchie auf dem Server.
- IMAP4 ist komplex und schwierig zu implementieren, aber vorteilhaft.

Beispiel Email-Header

From newsletter@bahn.de Thu May 12 19:01:25 2005

X-Delivered: at request of brun on drb9

Received: from insela.insel.de (insela.insel.de [192.109.16.71])
by drb9.drb.insel.de (8.9.0/8.9.0) with ESMTP id TAA15833
for <brun@drb9.DrB.Insel.DE>; Thu, 12 May 2005 19:01:25 +0200 (MEST)

From: newsletter@bahn.de

Received: from mail1.arcor-ip.de (mail1.arcor-ip.de [145.253.2.10])
by insela.insel.de (8.12.10/8.12.10/SuSE Linux 0.7) with ESMTP id
j4CH3duD020270
for <brun@insel.de>; Thu, 12 May 2005 19:03:39 +0200

Received: from fw1dbm.dbm.bahn.de (redaktion.bahn.de [145.253.167.26])
by mail1.arcor-ip.de (Arcor-IP) with SMTP id E614644ED
for <brun@insel.de>; Thu, 12 May 2005 19:01:23 +0200 (MET DST)

Received: by wsr6.bahn.de (Postfix, from userid 501)
id 2918A1F524; Thu, 12 May 2005 19:00:03 +0200 (CEST)

Content-Type: text/plain; charset="iso-8859-1"

Content-Disposition: inline

MIME-Version: 1.0

X-Mailer: MIME-tools 5.411 (Entity 5.404)

To: brun@insel.de

Subject: Pfingsten: Last-Minute-Ideen

Message-Id: <20050512170003.2918A1F524@wsr6.bahn.de>

Date: Thu, 12 May 2005 19:00:03 +0200 (CEST)

Content-Transfer-Encoding: 8bit

X-MIME-Autoconverted: from quoted-printable to 8bit by drb9.drb.insel.de id
TAA15833



Aufbau einer Inbox

- From ...
 - <Header der Email>
 - Leerzeile
 - Body
 - Leerzeile
- From ...
 - <Header der nächsten Email>
 - ...
- USW.



Konfigurationspunkte Linux

- Für sendmail: `/etc/sendmail.cf`
 - Ausgereiftes Paket
 - Schwierig zu konfigurieren
- Für postfix: `/etc/postfix/...`
 - Neuere Implementierung
 - Sicher, aber auch schwierig zu konfigurieren
- Dort werden jeweils auch Viren- und Spam-Schutzprogramme eingeklinkt

Bedrohungen Email

- **Ausspähen: Die Mails werden mitgelesen**
 - Abhilfe: Verschlüsseln des Mail-Body
- **Schadprogramme: Viren und Würmer**
 - Abhilfe: Viren-Scanner einsetzen, möglichst schon auf dem Mail-Empfangs-Server
- **Zeit- und Bandbreitenfresser: SPAM**
 - Abhilfe: Spam-Filter einsetzen, ebenfalls schon auf dem Mail-Empfangs-Server
- **Rechtsverletzungen, z.B. gegen den Jugendschutz durch pornografische Inhalte**
 - Abhilfe: Filterprogramme – Rechtslage beachten!



Kontrolle der WWW-Verkehrs

- Der Zugriff auf Web-Angebote soll für Mitarbeiter nicht unkontrolliert möglich sein.
- Neben dem Arbeitszeit-Missbrauch treten auch juristische Probleme auf (s. Mail)
- An der Schnittstelle Intra/Internet wird ein Kontroll-System installiert: Proxy-Server
- Zusätzliche Vorteile durch Zwischenspeicherung von Inhalten für alle User
- Weniger Bandbreite wird benötigt



Mehr zum Proxy-Server

- Unter Linux: squid, Konfigurationspunkt: /etc/squid/squid.conf
- Squid unterstützt mehrere Protokolle
- Es gibt komplexe Regeln (acl's), wer wann auf was im WWW zugreifen darf; per Firewall werden die gewünschten Ports für die Clients gesperrt
- Man stellt eine bestimmte Menge an Plattenplatz für das Caching zur Verfügung
- Auf den Clients muss der Proxy eingetragen werden, damit sie ihn benutzen



Verwaltung der Clients im LAN

- Die NetzwerkEinstellungen für Clients werden zweckmässigerweise zentral verwaltet:
 - Zuordnung von IP-Adressen, Netzmaske
 - DNS-Server-Adressen
 - WINS-Server-Adressen
 - Proxy-Server usw.
- Das übernimmt z.B. ein DHCP-Server



Dynamic Host Configuration Protocol

- RFC 951 definiert BOOTP (damit diskless clients ihr Boot-Image übers Netz laden können)
- Daraus entstand dann DHCP laut RFC 1541
- Unter Linux gibt es...
 - dhcpcd = DHCP Daemon
 - dhcpcd = DHCP Client Daemon
- Uns interessiert dhcpcd (/etc/dhcpcd.conf)

Beispiel für dhcpd.conf

- ```
subnet 192.109.16.0 netmask 255.255.255.192 {
 option routers 192.109.16.33, 192.109.16.3;
 option domain-name-servers insela.insel.de;
 option domain-name "insel.de";
} ...
```
- ```
group {  
    # hosts im 194.31.92.0 netzwerk  
    host drba  
        { hardware ethernet 00:00:E2:2F:37:FB;  
          fixed-address drba.drb.insel.de; }  
    host datics  
        { hardware ethernet 00:E0:7D:71:65:54;  
          fixed-address datics.drb.insel.de; }  
    host switch-a  
        { hardware ethernet 00:0E:6A:14:CD:C0;  
          fixed-address switch-a.drb.insel.de; }  
    ... }
```



Übungsaufgaben

- Untersuchen Sie die genannten Konfigurations-Dateien für smtp-, proxy- und dhcp-Services auf dem Übungsserver
- Informieren Sie sich über:
 - sendmail oder postfix
 - IMAP- und POP-Clients
 - Spam- und Viren-Filter für Linux/UNIX
- Hat IMAP bezüglich Schadprogrammen Vorteile gegenüber POP?