Linux – eine sichere Alternative

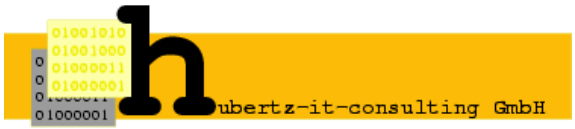
VPN-Firewalls, Standortvernetzung, Hochverfügbarkeitslösungen

Johannes Hubertz

hubertz-it-consulting GmbH

MacExpo Köln

8. Juni 2006



Gliederung

- Vorstellung, Übersicht
- OpenOffice und Sicherheit?
- Verfügbarkeit, Vertraulichkeit, Datenintegrität
- Netzwerksicherheit

Vorstellung: Johannes Hubertz

- 1954 in Köln-Lindenthal geboren
- 1973 Abitur in Köln-Mülheim
- Studium der Elektrotechnik an RWTH und FH Aachen
- ab 1980 bei großem europ. IT-Hersteller
- ab 2002 bei europ. IT-Dienstleister
- seit 1973 Bundesanstalt THW Köln-Porz, Fü – S6
- seit 2001 Segeln, am liebsten auf Salzwasser

Vorstellung: hubertz-it-consulting GmbH

Etwas Erfahrung war Voraussetzung

- Gründung am 8. August 2005
- Sitz: Köln
- Geschäftsinhalt: Dienstleistungen im Umfeld der IT-Sicherheit
- Logo: Johannes Hubertz Certificate Authority als ASCII-7Bitmuster
- Diese paar Bits findet sich in einigen 10000 X.509 Anwenderzertifikaten in der Seriennummer wieder
- Wir sind käuflich ;-)

Muß jeder **alle** Erfahrungen selbst erleiden?

- Bellovin and Cheswick: Firewalls and Internet Security, 1994
- Fazit: Keep it simple!
- Oder mit Einstein: So einfach wie möglich, aber nicht einfacher!

IT-Sicherheit: Versuch einer Ortsbestimmung

Vier Dimensionen der Sicherheit in der Informationstechnologie

- Vertraulichkeit — Confidentiality
- Integrität — Integrity
- Verfügbarkeit — Availability
- wirtschaftlicher Aufwand –

PDCA: Vorgehensweise beim Management der IT-Sicherheit

- Plan
- Do
- Check
- Act

Freie Software: Versuch einer Ortsbestimmung

Freie Software mit Pflichten

- Public Domain
- Open Systems
- Open Source
- Unterschiedlichste Lizenzmodelle
- Freie Software – Frei wie in Freiheit . . .
- Free Software Foundation: GNU General Public License
- Pflichten: Weitergabe mit Quellen, Urheberrecht

- Freie Software

Softwarequalität ist auch ein Sicherheitsfaktor

Ein Artikel in der Computer Zeitung Nr. 21 / 22. Mai 2006, Seite 21:
Im Opensource-Umfeld hebt das Ethos das Niveau

Hobbyfrickler sind ein Mythos

. . . Es ist übrigens nicht so, daß viele Hobbyprogrammierer an Opensource-Projekten arbeiten. Die weitaus überwiegende Zahl der hier aktiven Programmierer sind hoch qualifizierte IT-Profis. . . .

Qualitätsbewußtsein

. . . Die Qualität von quelloffener Software belegen auch unabhängige Studien. So hat jüngst Reasoning, ein Anbieter automatisierter Softwareinspektions-Services, die TCP/IP-Implementierung von Linux mit fünf kommerziellen Versionen verglichen. Das Resultat lautet, daß die Umsetzung im Linux-Kernel deutlich weniger Fehler aufweist als die der verglichenen Betriebssysteme proprietärer Herkunft.

Lars Herrmann, Solution Architekt, Redhat/fg

Freie Software: Beispiele zur Verfügbarkeit

- Linux High Availability
- Apache mod_security
- OpenOffice.org

OpenOffice.org

- Kostenlose Alternative zu bekannter, proprietärer Bürosoftware
- $\longrightarrow$ISO/IEC 26300[1] wird auch übermorgen noch gültig sein!
- freies Dokumentenformat $\rightarrow$ Applikationsunabhängigkeit!
- freies Dokumentenformat $\rightarrow$ beliebige Datenkonvertierung möglich
- freie Programm-Quellen $\rightarrow$ Dokumente sind auch übermorgen noch lesbar
- freie Programm-Quellen $\rightarrow$ Sicherheit vor Hintertüren
- $\longrightarrow$ Meine Daten gehören mir!

Bezugsquelle: http://www.openoffice.org/

[1] `http://www.heise.de/newsticker/meldung/72668` vom 3.5.2006

Apache mod_security

Funktionalität

Feingranulare Einstellung (mit regex) dessen, was der Webserver servieren darf. Exaktheit verhindert den Systemeinbruch, der Mißbrauch wird also stark erschwert.

Sorgfalt führt zum Ziel

Fehlende Angriffsfläche führt zu unterbrechungsfreiem und damit längerem Betrieb.

Linux High Availability

sind 99,999 Prozent genug?

Linux-HA ist schon einige Jahre alt. **heartbeat** ist das zentrale Element.

Hochverfügbarkeit für:

- Dateisysteme (drbd)
- Serverfunktionalität (dhcp,email,web)
- Netzwerkfunktionalität (router,firewall,vpn)

Verfügbarkeit 100 Prozent?

Manager haben **Träume**

- Wir haben eine Firewall, da ist alles sicher.
- Software installieren, fertig.
- Software installieren, einrichten, . . .
- Software installieren, einrichten, regelmässige Wartung, . . .
- Albtraum: Systemausfall!

Managers **Reality-Show**

- Verfügbarkeit ist de facto immer kleiner als 100 Prozent
- 99 Prozent bedeutet 3,6 Tage Ausfall im Jahr!
- 99,9 Prozent bedeutet 0,36 Tage = 9 Stunden
- Hochverfügbarkeit ist i.a. teuer!
- Linux-HA gibts kostenlos

Vertraulichkeit, was ist das?

Manager haben **Träume**

- Ich bin Ihr Systemadministrator, wie war doch gleich Ihr Passwort?
- Daten sind manchmal sehr wichtig.
- Verschlüsselung schützt, vorbeugen mußt Du!
- GnuPG, OpenSSL, OpenSSH, OpenVPN, cacert.org . . .

Managers **Reality-Show**

- Verschlüsselung contra Verfügbarkeit
- Wer darf an meine Daten?
- Wer darf nicht an meine Daten?
- Schlüssel sollten verschlüsselt abgelegt werden!
- Schlüsselverwaltung z.B. mit OpenLDAP als PKI
- SmartCard hilft, GnuPG kostet nichts.
- Software gibts umsonst, das KnowHow kostet . . .

Datenintegrität

Lokale Integrität

- Sind Ihre Daten in 10 Jahren noch die gleichen?
- Wie stellen Sie das sicher? Hält Ihr Programm so lange?
- Kryptographische Hashfunktionen können helfen, z.B. OpenSSL
- Backup, Archivierung, Regelmäßige Tests . . .

Integrität beim Transport

- Datenübertragung mit Checksummen (TCP/IP)
- Offengelegte, herstellerunabhängige Standards (RFCs)
- Verschlüsselung kann zusätzliche Sicherheit herstellen

Sicherheit

Sicherheit als Balanceakt

- Verfügbarkeit und Vertraulichkeit sind offensichtlich Gegensätze
- Integrität über lange Zeiten macht Vertraulichkeit zunichte
- Eine gesunde Mixtur der drei Anforderungen ist anzustreben.
- Der wirtschaftliche Aufwand beschränkt und balanciert die Realisierung
- Ist Vertraulichkeit beim OnlineBanking auch überflüssig ???

Haftung für Sicherheit

- Geschäftsleitung ist verantwortlich im Sinne der Gesetze
- Geschäftsleitung haftet bei Verschulden

Gliederung

- Vorstellung, Übersicht
- OpenOffice und Sicherheit?
- Verfügbarkeit, Vertraulichkeit, Datenintegrität
- Netzwerksicherheit

Netzwerk, wo brauche ich das?

- Mehr als ein Computer?
- Netzwerk verbindet!
- IP <=> Internet Protokol, RFC 791, September 1981
- Offener Standard <=> allseitiger wirtschaftlicher Nutzen
- Zu Hause, in der Firma, unterwegs, in der Raumfahrt . . .
- immer und überall mit allen Fehlern
- Firewalls mindern das Risiko

IP-Filterung: Geschichte

Freie Software und Paketfilterung

- Linux 2.0: ipfwadm, Juli 1996
- Linux 2.2: ipchains, Januar 1999
- Linux 2.4: iptables (netfilter), Januar 2001
- Linux 2.6: iptables (netfilter), Dezember 2003

Firewalls

einfache Firewall-Lösungen mit Linux mit und ohne Grafik

- Shell-script mit iptables
- Shorewall, Ipcop, Firewall-Builder, u.v.a.m.
- TIS Firewall-Toolkit, smtpd, squid, apache, bind, . . .

Werkzeuge und Hilfsmittel

- netstat, ping, telnet
- tcpdump, ethereal
- satan, nessus, sara, nmap, snort, autopsy, . . .
- ettercap, metasploit, . . .

zentral gesteuerte Firewalls

Firewall-Lösungen für komplexe Umgebungen

- `iscs.sf.net` Integrated Secure Communications System
- Status: beta, in Entwicklung, allumfassender Ansatz
- `NetSPoC.berlios.de` a Network Security Compiler
- Status: Produktiv, Linux, Cisco, BSD
- `sspe.sf.net` **s**imple **s**ecurity **p**olicy **e**ditor
- Status: Produktiv, Linux, IPsec-VPN, ...

sspe: Lizenz

simple security policy editor

ist freie Software und unterliegt der
GNU General Public License

Firmenstandort

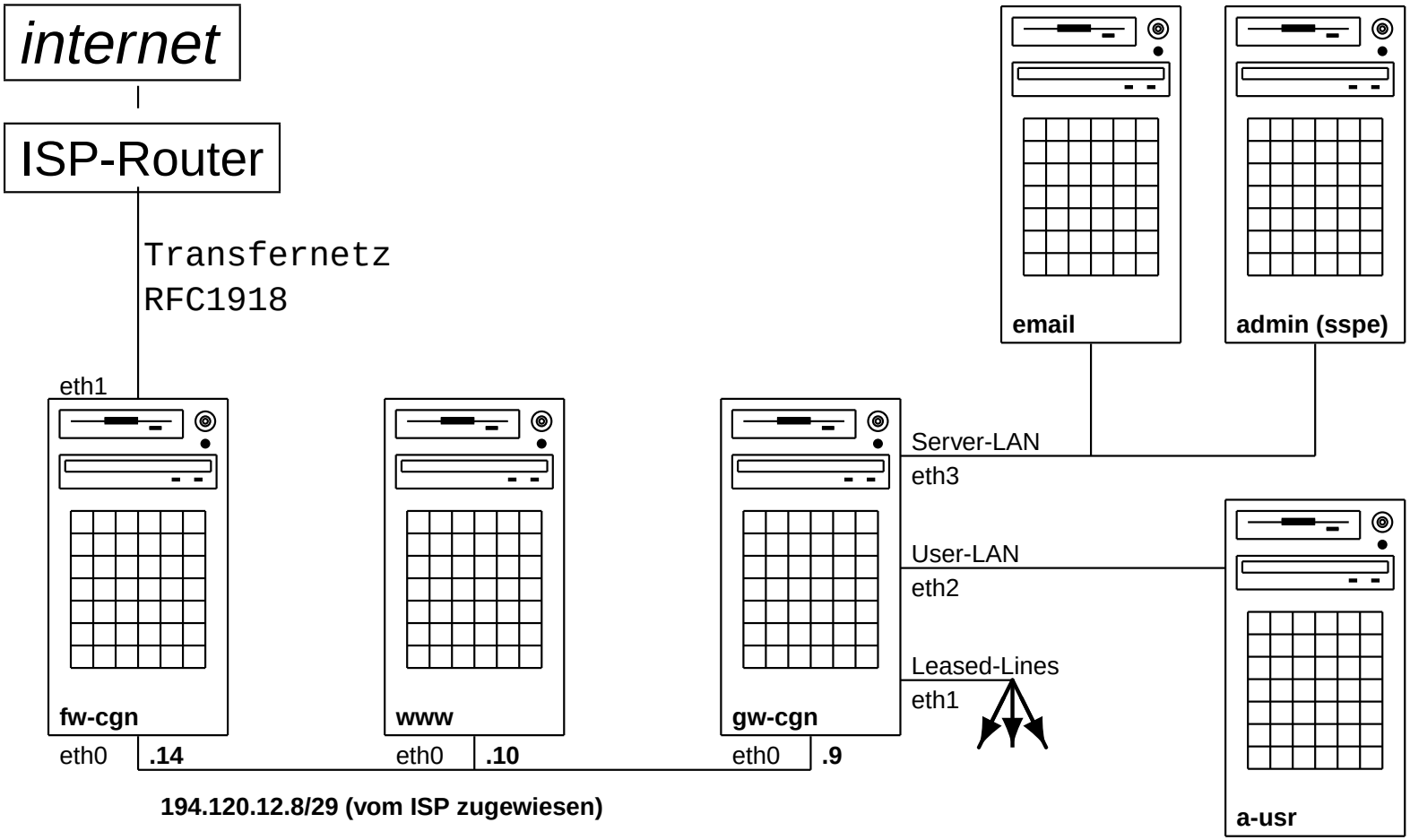
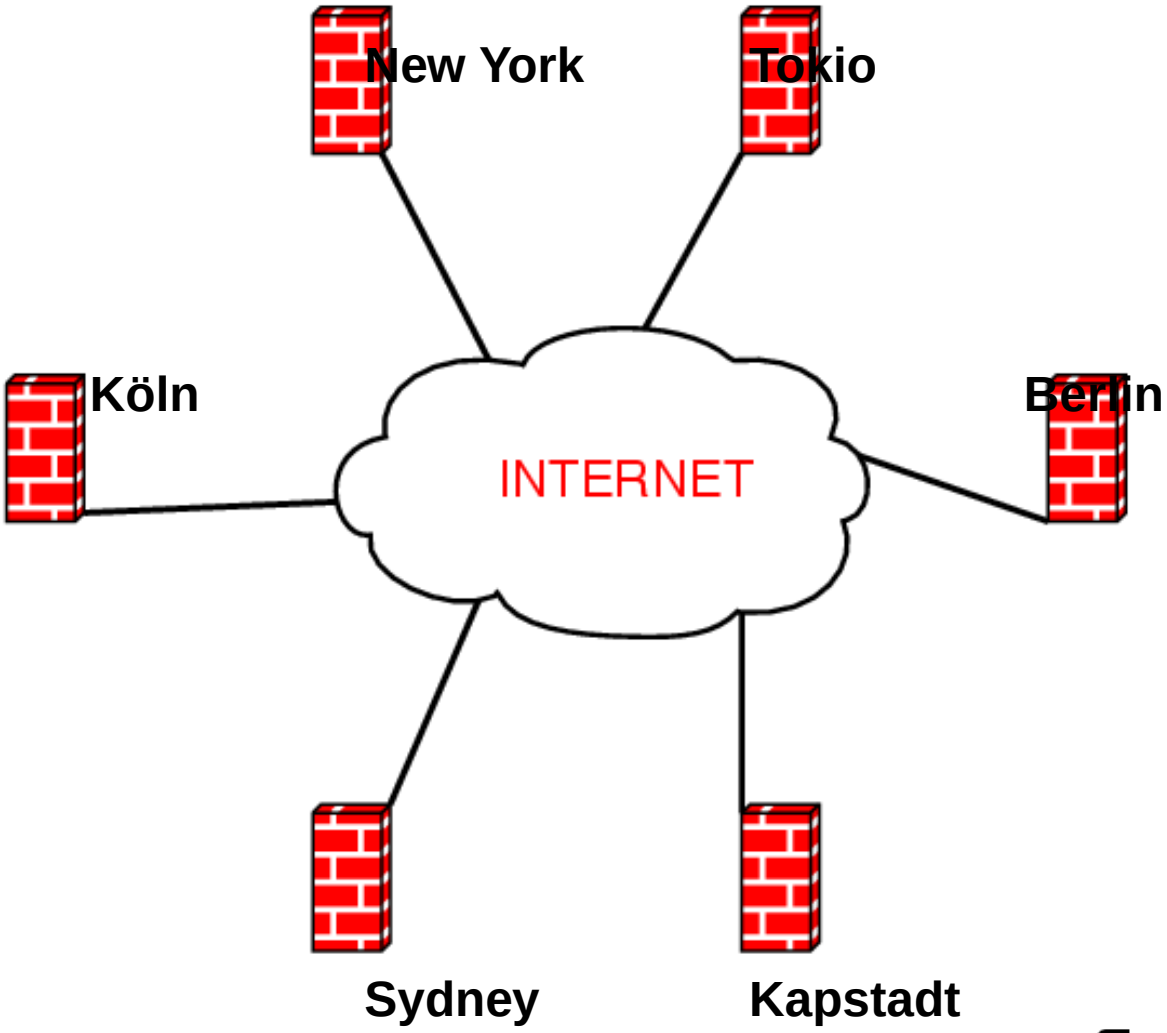


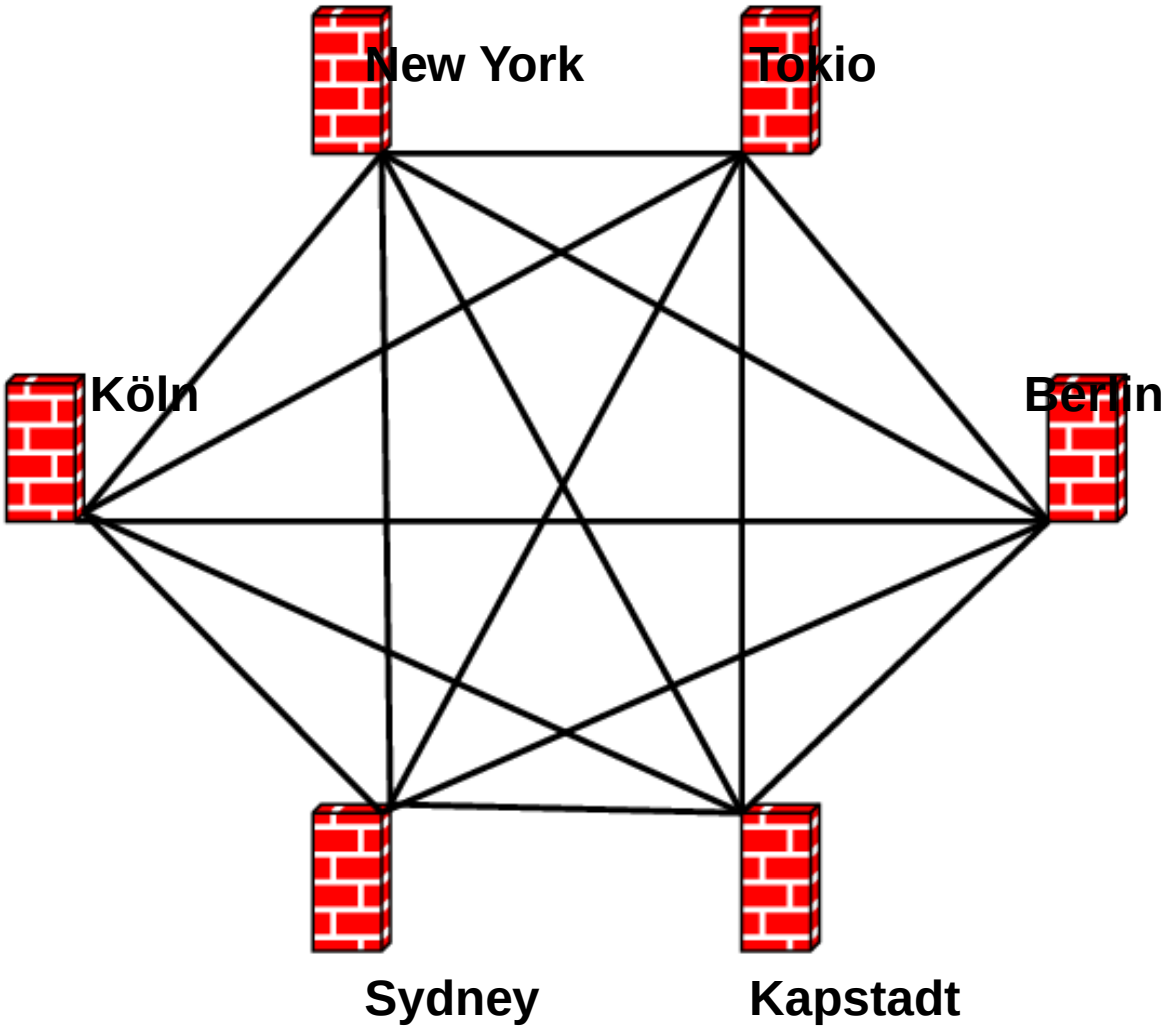
Abbildung: Typischer Firmen-Standort

Firmennetzwerk



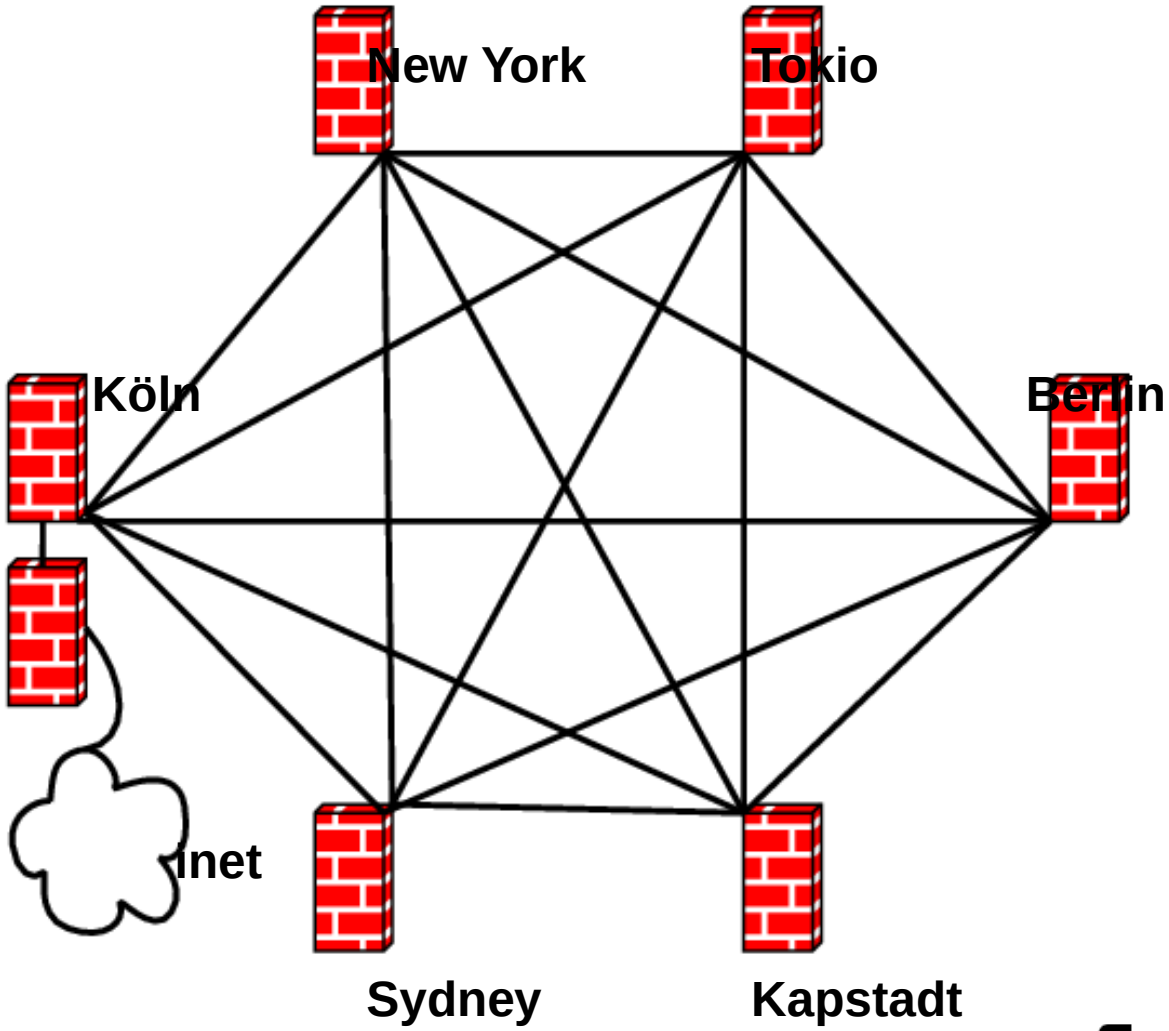
6 Standorte an beliebigen Internet-Providern

Firmennetzwerk als VPN



6 Standorte per IPsec voll vermascht mit $S * (S - 1) = 30$ Tunneln

Firmennetzwerk als VPN mit **einem** Internetanschluß



1 ISP + 6 Standorte an einem ISP-MPLS-VPN

VPN: weitere Möglichkeiten

IPsecVPN, universell und kompatibel

- Handlungsreisende (roadwarrior) mit X.509-Authentisierung
- `vpndialer.sf.net` für IPsec und L2TP vom beliebigen M$-PC
  (freie Software von Thomas Kriener)
- Sperrliste für einzelne Clients: CRL der Zertifizierungsstelle

OpenVPN, die sinnvolle Ergänzung

- Konfiguration einfach, überschaubar und flexibel
- einfacher Client für Apple, Linux und M$-PC
- Vorhandene Zertifizierungsstelle kann genutzt werden
- Die Sperrliste (CRL) ist ebenfalls wirksam

Betrieb: Erfahrungen

- Produktionseinsatz seit April 2002
- einige hundert Anwender-PC geschützt
- Aussichten: OpenBSD, Solaris, HA, dyn.Routing, . . .
- Kosten drastisch minimiert gegenüber kommerzieller Firewall-Lösung

Dokumentation

Eine Sicherheitsarchitektur ist nur so gut wie ihre Dokumentation
Bei sspe wird sie mit LaTeX aus der laufenden Konfiguration erzeugt:

- Übersicht der Netzwerkarchitektur
  einmalig zu zeichnendes Bild(dia),
  pstricks mit Referenzen (Seitenzahlen der Geräte-Seiten)
- Konfiguration der einzelnen Maschinen
  Interfaces, Routing, . . .
- Firewall Definitionen und Regeln
- VPN Konfiguration
- Geplant ist eine weitgehende Vollständigkeit, d.h.
  alles sollte aus der Dokumentation wiederherstellbar sein

Webseite: Mittelstand sicher im Internet

`http://www.mittelstand-sicher-im-internet.de/`

IT-Sicherheit bei Open-Source-Software

. . . Deshalb setzten z.B. Sicherheitsbehörden in kritischen Bereichen Open-Source-basierte Lösungen ein, deren Vertrauenswürdigkeit zuvor anhand der Quelltexte überprüft wurde. . . .

. . . Die Verantwortung für eine sichere Konfiguration und Wartung der Software bleibt deshalb auch bei Open-Source-Produkten beim Unternehmen. Die Verwendung unsicherer Voreinstellungen, schwache Passwörter und das Betreiben nicht benötigter Dienste auf dem System bleiben – wie bei proprietärer Software auch – eine Gefahr, die nur ein ausgebildeter Administrator eingrenzen kann.

Kurzwiederholung

- Freie Programme und ihre Daten – Verfügbarkeit strebt gegen ∞
- kostenloser Quelltext, Kostenvergleich bzgl. Administration!
- Quelltext macht Verstehen möglich
- Quelltext macht Änderungen möglich
- Quelltext macht Hintertüren fast unmöglich
- sichere Kryptografie ohne Quelltext ist undenkbar
- Freie Software möglicherweise sicherer als proprietäre Lösungen
- Firewalladministrator soll seine Geräte verstehen
- Nur mit freier Software hat er eine reale Chance!

Summary

KnowHow ist unerläßlich

- hierarchiche Sicherheit auf Abteilungs- oder Gebäudeebene beugt vor
- Verschlüsselung relevanter Daten und Kanäle wo immer möglich
- Einbruchserkennung ist kein Luxus, Vorbeugung tut Not!

Konsistenz und Konsequenz

- zentrale Steuerung aller Sicherheitskomponenten
- zentrale Überwachung und regelmäßige Kontrolle

Kosten und Nutzen

- freie Software kostet nichts außer Pflege
- kommerzielle Software kostet auch Pflegeaufwand
- Verständnis des Administrators bestimmt wesentlich die Qualität Ihrer Sicherheit!

Danke

Ich bedanke mich für Ihre Aufmerksamkeit.
Frohes Schaffen

Johannes Hubertz