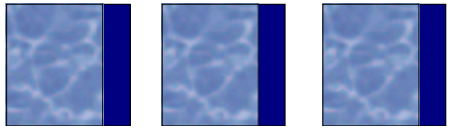
Linux & Security

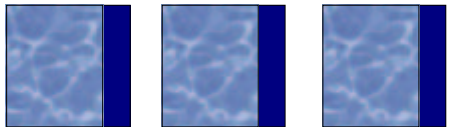
Andreas Haumer − xS+S

Einsatz von Linux in
sicherheitsrelevanten Umgebungen

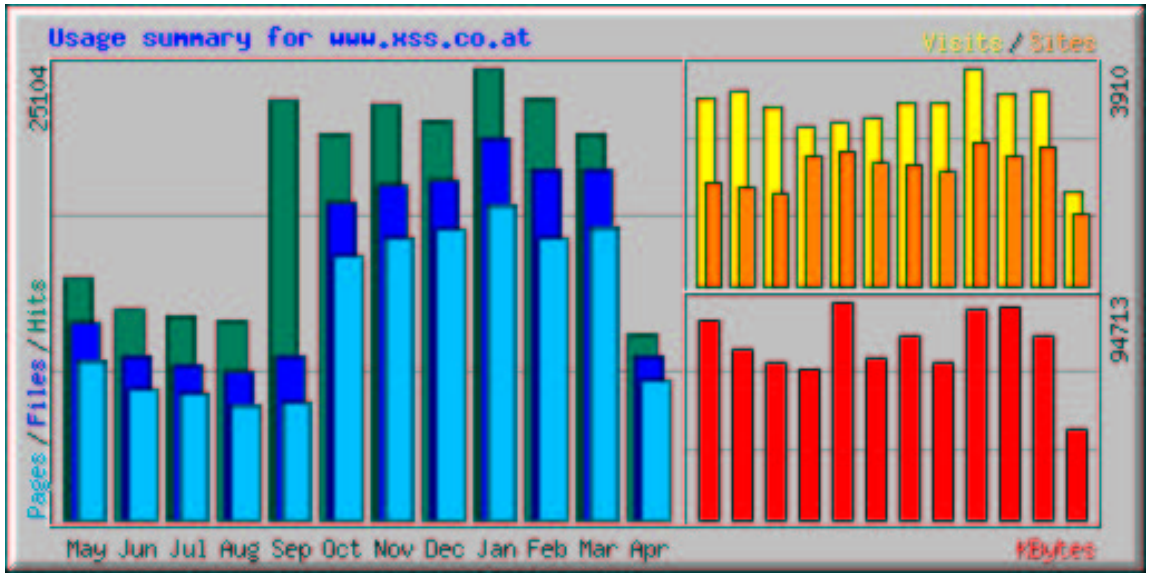


Einführung

- Netzwerksicherheit – wichtiger denn je
- Unternehmenskritische IT Infrastruktur
- Abhängigkeit von E-Services
- Abhängigkeit von Herstellern
- Aktuelle elektronische Angriffsszenarien



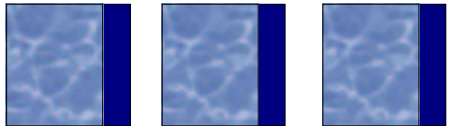
Code Red Auswirkungen



Verdoppelung der Page Hits durch Code Red und Nimda im September 2001 − mit Auswirkungen bis heute!

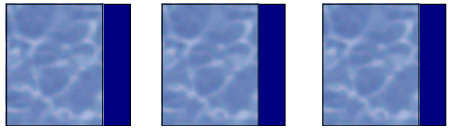
Überblick

- Was bedeutet Security?
- Anforderungen an die IT Abteilung
- Linux?
- Eigenschaften von Linux
- Konkrete Anwendungsbeispiele



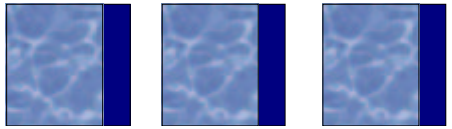
Was bedeutet Security?

- Betriebssicherheit
- Datensicherheit
- Investitionssicherheit



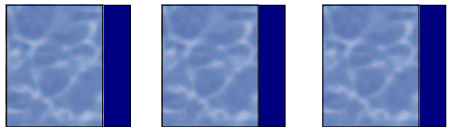
Betriebssicherheit

- Verfügbarkeit der Dienste
- Sicherheit vor Datenverlust
- Sicherheit vor unbefugter Benutzung
- Updateplanung und Administration



Datensicherheit

- Sicherheit vor Datenmanipulation
- Sicherstellung der Vertraulichkeit
- Sicherheit vor unbefugtem Zugriff
- Sicherstellung der Reputation
- Rechtliche Rahmenbedingungen



Investitionssicherheit

- Investition in Hard− und Software
- Investition in Schulung und Know How
- Betriebskosten
- Verfügbarkeit von Erweiterungen, Updates und Support
- Abhängigkeit von Herstellerentscheidungen

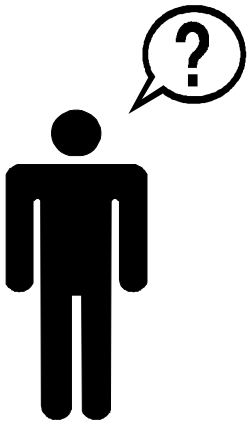
Anforderungen an die IT Abteilung

- Administrierbarkeit der Lösung
- Stabiler Betrieb
- Flexibilität und Erweiterbarkeit
- Geringe Kosten
- Externer Support

Anforderungen an die IT Abteilung

Administrierbarkeit

Geringe Kosten



Stabiler Betrieb

Betriebssicherheit

Externer Support

Flexibilität und
Erweiterbarkeit

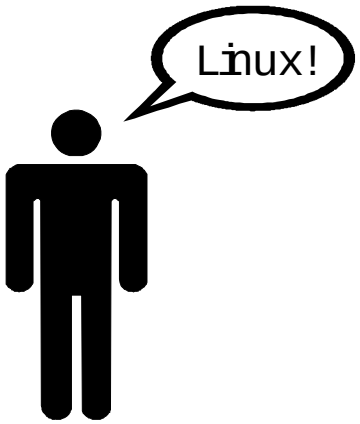
Datensicherheit

Investitionssicherheit

Die Lösung!

Administrierbarkeit

Geringe Kosten



Stabiler Betrieb

Betriebssicherheit

Externer Support

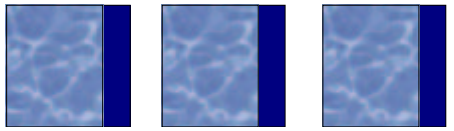
Flexibilität und
Erweiterbarkeit

Datensicherheit

Investitionssicherheit

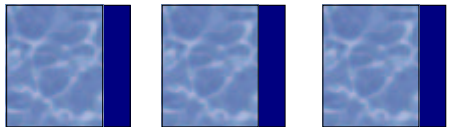
Linux?

- Was ist Linux?
- Etwas Geschichte
- Das Linux Entwicklungsmodell
- Einsatzmöglichkeiten von Linux
- Vorteile
- Linux erfüllt die Anforderungen!



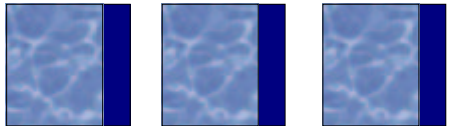
Was ist Linux?

- Unix® kompatibles Betriebssystem
- Viele verschiedene Hardwareplattformen
- Open Source Komponenten
- Weltweite Entwicklung
- Weltweiter Einsatz



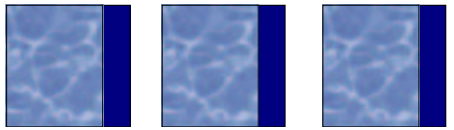
Etwas Geschichte

- Unix®
- TCP/IP und Internet
- Das GNU Projekt
- Die Entwicklung von Linux
- Der Begriff "Open Source"



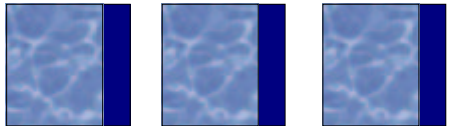
Das Linux Entwicklungsmodell

- Komponenten des Systems
- Open Source
- Linux Core Entwickler
- Linux 2nd Level Entwickler
- Anwender
- Distributoren und Dienstleister



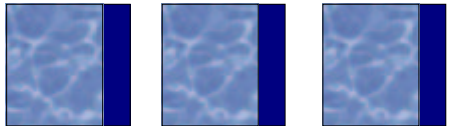
Einsatzmöglichkeiten von Linux

- "Black Box" Lösungen im Netzwerk
- Standard Services (Mail, Web, File)
- Administrative Dienste und Directory Services
- Datenbank Server
- Softwareentwicklung
- u.v.a



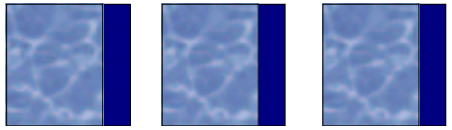
Vorteile von Linux

- Vorteile für den Administrator
- Vorteile für den Anwender
- Vorteile für das Unternehmen



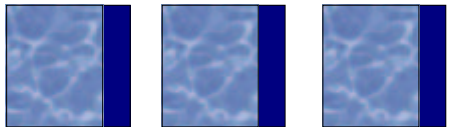
Vorteile von Linux (2)

- Stabil, offen, flexibel
- Gute Dokumentation, guter Support
- Leistungsfähige Netzwerkfunktionen
- Standardkonform, keine proprietären Erweiterungen, klare Konzepte
- Kein "Calling Home", keine Geheimnisse
- Freiheit für den Anwender



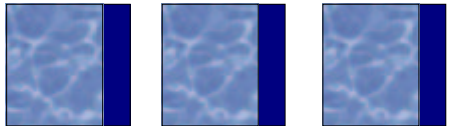
Eigenschaften von Linux

- Linux erfüllt die Anforderungen
- Ideale Plattform für heterogene Netzwerke
- Besondere Stärken im Netzwerk− und Security−Bereich
- Kein Hype, sondern Realität!



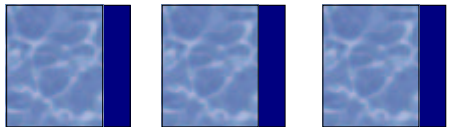
Betriebssicherheit

- Ausgereiftes System
- Bewährte Systemkonzepte
- Versionsverwaltung für Programme und Konfiguration
- Modularisierung und Paketverwaltung
- Werkzeuge und besondere Eigenschaften



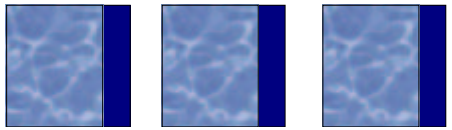
Datensicherheit

- Klassische Unix Rechtestruktur
- Access Control Lists
- IP Paketfilter
- Datenverschlüsselung
- Erweiterte Eigenschaften



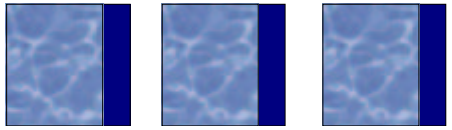
Investitionssicherheit

- Know How und Dokumentation
- Offene Schnittstellen
- Versionspflege
- Modularisierung
- Herstellerunabhängig



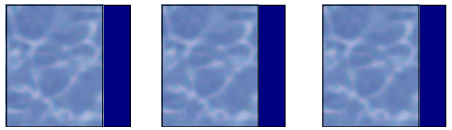
Einfache Administration

- Was ist "einfach"?
- Anforderungen des Administrators
- "Point−And−Click" Administration?
- Das Unix/Linux Konfigurationsinterface
- Vollständiger Zugriff auf Systemparameter
- Keine Geheimnisse



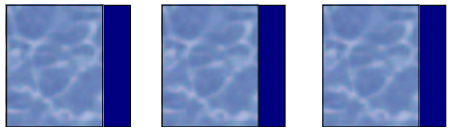
Vorteile des Unix/Linux Administrationskonzepts

- Einfaches Backup & Recovery
- Einfache Fernwartung über SSH oder IPsec
- Versionskontrolle
- Reproduzierbarkeit
- Dokumentation und Kommentare
- Modul− und Paketverwaltung



Stabiler Betrieb

- Permanente Code−Pflege
- Modulares System
- Austausch der Module im laufenden Betrieb
- Kein unnötiger Ballast

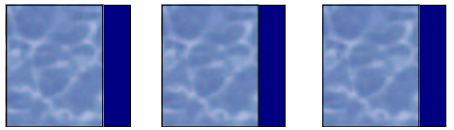


Geringe Kosten

- Open Source − Software im Quellcode
- Keine künstlichen Lizenzbeschränkungen
- Wiederverwendbarkeit des Know How
- Genügsam bei Hardwareanforderungen
- Kein Zwang durch den Hersteller

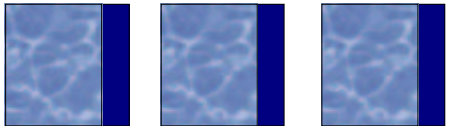
Flexibilität und Erweiterbarkeit

- Modulkonzept
- Scriptingfähigkeiten
- Werkzeuge und Softwarepakete
- Offene Schnittstellen



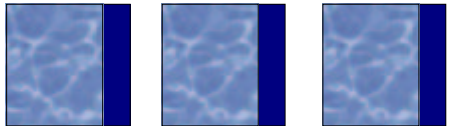
Linux Support

- Die "Linux Community"
- Dokumentation
- Linux Dienstleister
- Fernwartung, verschiedene Support−Pakete

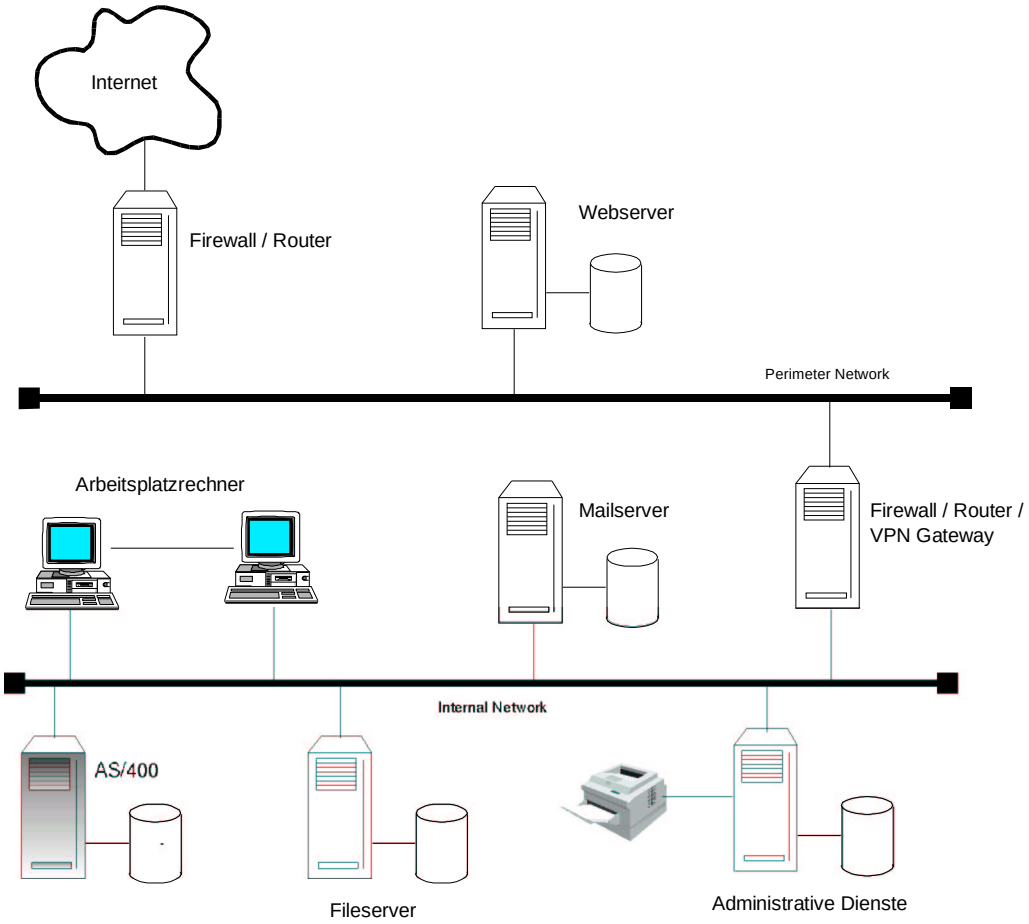


Anwendungsbeispiele

- Router und Firewall
- VPN Gateway
- Web Server
- Datenbank Server
- Mail Server
- File Server
- Administrative Dienste

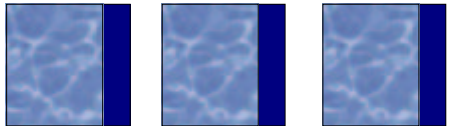


Beispielnetzwerk



Router und Firewall

- Linux Basisfunktionalitäten
- Policy Based Routing
- Quality of Service
- Masquerading
- Network Adress Translation
- IP Paketfilter

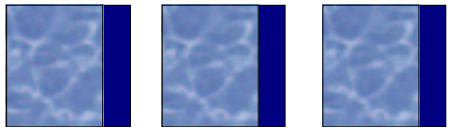


VPN Gateway

- PPTP für Windows Clients
- IPsec – Der Internet Standard
- RSA Public Key Authentifizierung
- x.509 Zertifikate
- Certification Authority
- Sichere Verbindung über unsichere Transportwege

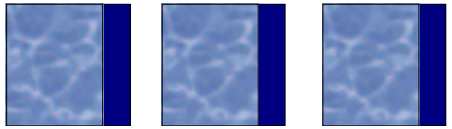
Web Server

- Apache − die Nr. 1 im Internet
- Web−Applikationen mit PHP und Perl
- JSP und XML
- Sicherheit mit SSL und x.509 Zertifikaten
- Datenbank Anbindung für dynamische Inhalte



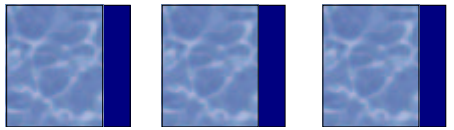
Datenbank Server

- Von wenigen MB bis mehrere 100 GB
- Open Source Datenbanken
- Kommerzielle Datenbanken
- Storage Infrastruktur: SAN, Backup, RAID



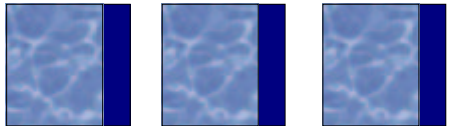
Mail Server

- Standard Internet Protokolle: SMTP, POP, IMAP
- Auch mit SSL
- Virenscanner, Attachment−Filter
- Access Control, Anti Relay, Anti Spam



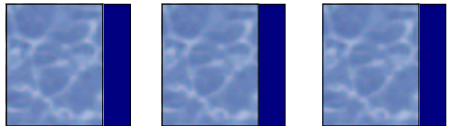
File Server

- Unix Network Filesystem (NFS)
- Fileserver und PDC für SMB/CIFS Clients
- Fileserver für AppleTalk
- Fileserver für Novell Clients



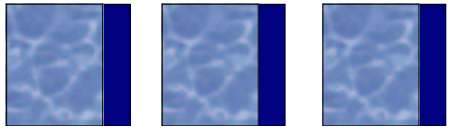
Administrative Dienste

- Directory Services (DNS, LDAP, NIS)
- DHCP Server
- Timeserver (NTP)
- Backup Server
- Network Boot Server
- Web Proxy mit Adressfilterung und Access Control Lists



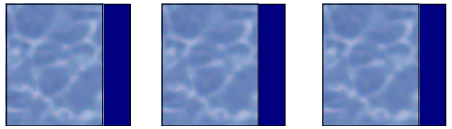
Ausblick auf die Zukunft

- Der Linux Kernel
- Hochverfügbarkeitslösungen
- Anwendungen
- Linux am Desktop
- Embedded Linux und Spezialhardware



Zusammenfassung

- Ideale Plattform im Unternehmensnetzwerk
- Hervorragende Netzwerk− und Sicherheitsfeatures
- Kostengünstig
- Herstellerunabhängig



Danke für die Aufmerksamkeit

Andreas Haumer − xS+S
Karmarschgasse 51/2/20
A−1100 Wien

Tel: +43−1−6060114−0
Fax: +43−1−6060114−71

Web: http://www.xss.co.at/
Mail: andreas@xss.co.at