

- Vorstellung des Unternehmens
- Projekte:
 - virtuelles privates Netzwerk
 - Serverüberwachung
 - Benutzerverwaltung
- Fazit

- OneVision Software AG
- produziert Software Lösungen für die Druckindustrie:
kompletter Workflow vom Anliefern der Vorlagen bis zum Drucken
- Hauptsitz in Regensburg und Außenstellen in:
 - Hannover (Entwicklung)
 - Frankreich
 - Großbritannien
 - Dänemark
 - USA

- Hauptsitz und Außenstellen haben eigenständige LANs
 - Anbindung zum Internet über Gateway-Rechner
 - private, im Internet nicht geroutete Adressen im LAN
 - Zugriff vom LAN ins Internet über NAT
- Probleme:
 - Administrationsaufwand für IT-Abteilung
 - Kommunikationsschwierigkeiten im Unternehmen
- Lösung:
 - virtuelles privates Netzwerk (VPN)

- zuerst Simulation des OneVision Netzwerks mit Testrechnern
 - benutztes Protokoll: IPSec mit RSA-Verschlüsselung
 - auf den Gateway-Rechnern (Tunnel-Endpunkte) läuft
 - iptables (Firewall, NAT) und
 - FreeS/WAN (IPSec-Software)
 - Hauptarbeit:
 - Konfiguration von FreeS/WAN
 - Integration der Firewall-Regeln
- danach Übernahme ins Produktionssystem

- Außendienstmitarbeiter sollten mit Windows-Laptops Verbindung ins VPN aufnehmen können:
 - direkte Verbindung über Modem oder
 - indirekte Verbindung über LAN eines Kunden
 - ⇒ Frage der Sicherheitspolicies
- Windows-Schlüsselverwaltung ⇒ Einsatz von X.509 Zertifikaten („eingepackte“ RSA-Schlüssel mit Eigentümer und Gültigkeitsdauer)

- Problemstellung: Arbeit bei OneVision abhängig von einigen zentralen Servern
 - RAID Systeme für Codeverwaltung und Dokumentation
 - Windows-Domänenverwaltung
 - diverse andere Dienste
- Lösung mit NetSaint:
 - Überwachung von Engpässen und Ausfällen
 - sofortige Alarmierung per E-Mail oder SMS
 - automatische Einleitung von Gegenmassnahmen

- Problemstellung: umständliche Benutzerverwaltung
 - mind. drei Passwörter: Windows, UNIX, Lotus Notes
 - nicht Standort-übergreifend: Mitarbeiter benötigt pro Standort jeweils einen Account ⇨ noch mehr Passwörter
- Lösung mit zentraler Benutzerverwaltung und LDAP
 - Microsoft Ansatz: Active Directory
 - OpenSource Ansatz:
 - LDAP-Server mit BerkeleyDB zur Datenhaltung
 - Kerberos für Authentifizierung ohne Passwörter
 - OpenSSL zur gesicherten Übertragung (zusätzlich IPSec Verschlüsselung zwischen den Standorten)
 - SAMBA als Domänencontroller und Fileserver

- Netzwerkkonfiguration und -administration
- interessant und lehrreich
- hoher Aufwand für Recherche
- kleine Fehler rächen sich erst Tage danach

- weitere Informationen liegen auf <http://www.gerald-able.de> bereit
- noch Fragen?
- vielen Dank für die Aufmerksamkeit!