OpenSSH - aber sicher!

André Niemann, becon GmbH,
andre.niemann@becon.de

GUUG FFG, March 24, 2017

becon
Data Center Services for Enterprise

Über mich

- IT Security (Master)
- System Engineer
- WebPKI, Orchestrierung, Monitoring, SSH
- bei der becon GmbH

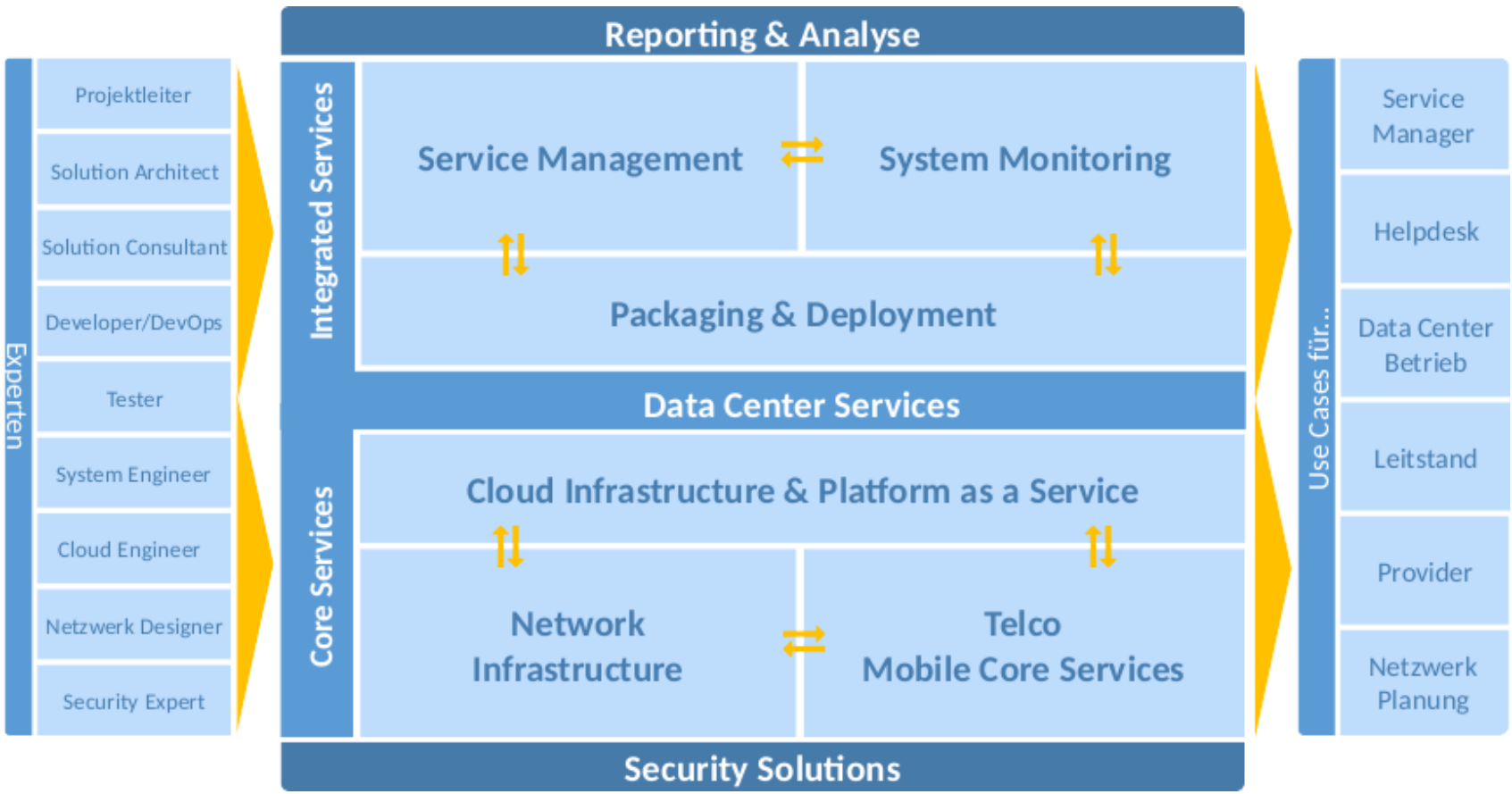
Über becon GmbH

becon
Data Center Services for Enterprise

- Gründung in 1988 aus dem Konzernumfeld heraus
- Standorte in München, Berlin und Fulda
- Dienstleister für integrierte Data Center Services auf Konzern Niveau
- Kunden wie Atos, Bosch, Linde, Nokia, Siemens, T-Systems, Wincor
- GmbH in privater Hand mit starker Finanzkraft
- International tätig, ISO 9001:2008 zertifiziert
- Inkubator für Startups und Open Source Projekte
- Mitbegründer der sys4 AG

Data Center Services for Enterprise

becon
Data Center Services for Enterprise



(Was gefällt euch an) OpenSSH?

> “das es klappt, es geht halt”
>
> — OpenSSH User, IRC

> “-NL ist die Magic, die man immer braucht ”
>
> — another OpenSSH User, IRC

> “SSH funktioniert einfach(, nicht wie TLS)”
>
> — bei ner Limo

Was ist (Open)SSH?

- OpenSSH - wohl populärste sshv2 Implemtierung
- IETF RFC 4251-54
- Secure remote shell + (secure) Tansportlayer Tunneling
- andere: Dropbear, ..

SSH vs TLS

becon
Data Center Services for Enterprise

SSH

- built-in PFS
- Tofu, (priv) CA optional
- modul. Ciphersupport
- mehrere Protos, erweiterbar
- beidseitig Authentisiert(Key, Host based, pass)

TLS

- PFS optional
- (public) CA-Trustmodel
- modul. Ciphersupport
- ebenfalls Modular
- beideseitig nur mit Client-Cert

Authentication Protocol

The Secure Shell Protocol (SSH) is a protocol for secure remote login and other secure network services over an insecure network. .. The SSH authentication protocol runs on top of the SSH transport layer protocol and provides a single authenticated tunnel for the SSH connection protocol.

Connection Protocol

This document describes the SSH Connection Protocol. It provides interactive login sessions, remote execution of commands, forwarded TCP/IP connections, and forwarded X11 connections. All of these channels are multiplexed into a single encrypted tunnel.

Transport Layer

This document describes the SSH transport layer protocol, which typically runs on top of TCP/IP. The protocol can be used as a basis for a number of secure network services. It provides strong encryption, server authentication, and integrity protection. It may also provide compression.

OpenSSH - Protokolle

- Transportlayer Proto
- Authentication Proto
- Connection Proto

12 Live!

Live Notes

- ssh [-v] user@host
- ~ + .
- ~ + ⇧ + c

Client Konfigurationen

man 5 ssh_config

- command-line options
- /.ssh/config
- /etc/ssh/ssh_config

/.ssh/config


```
1  Host *
2      KexAlgorithms curve25519-sha256@libssh.org,diffie-
           hellman-group-exchange-sha256
3      Ciphers aes256-gcm@openssh.com,chacha20-
           poly1305@openssh.com
4
5  Host localhost
6      VisualHostKey yes
7      Identityfile legacyKey
8
9  Host Jump.box
10     User andre
11     ForwardAgent yes
12     Port 4242
```

Key Authentication

man 1 ssh-keygen

- id_rsa
- id_dsa
- id_ecdsa
- id_ed25519
- id_??-cert ?

Hostkey-Austausch

- ’local Database’ (/.ssh/known_hosts)
- Textfile (/.ssh/known_hosts2)
- SSHFP Records
- SSH CA -> (AUTHORIZED_KEYS FILE FORMAT section)

SSH Key signing/CA

- ssh-keygen -f ssh-ca -b 4096
- echo ”cert-authority $(cat ssh-ca.pub)” » /.ssh/authorized_keys
- ssh-keygen -s signing-key -I key-identifier -h -n hostname -V +52w host-key

siehe /etc/ssh/sshd_config

- SSH Version
- Root login
- AllowUsers/Groups
- ..

Ansätze zur Härtung

- keine CBC Cipher
- keine alten Hash-Alogs
- kein pass-auth
- privatekeys schützen.

- bettercrypto.org
- mozilla wiki
- Vorschläge für aktuelle?

Tunneling

- ssh -NL 9002:wieistmeineip.de:80 andre@example.net
- ssh -NR *:50020:localhost:22 example.net
- ssh example.net -p 1337 -ND 33333

SSHD conf für -R

GatewayPorts [no,yes,clientspecified]

Jump Host


```
# First jumphost. Directly reachable
Host alphajump
  HostName jumphost1.example.org

# Host to jump to via jumphost1.example.org
Host behindalpha
  HostName behindalpha.example.org
  ProxyCommand  ssh alphajump netcat -w 120 \%h \%p
```

```
# First jumphost. Directly reachable
Host betajump
  HostName jumphost1.example.org

# Host to jump to via jumphost1.example.org
Host behindbeta
  HostName behindbeta.example.org
  ProxyJump  betajump
```

— https://wiki.gentoo.org/wiki/SSH_jump_host

Channel Multiplexing


```
Host machine1
        HostName machine1.example.org
        ControlPath /.ssh/controlmasters/%r@%h:%p
        ControlMaster auto
        ControlPersist 10m
```

```
ssh (-M) -S /home/andre/.ssh/control@mp example.host
```

Pubkey + 2FA

```
1 AuthenticationMethods publickey,password
```

```
1 local \  # ssh root@box
2 Authenticated with partial success.
3 root@box's password:
4 Welcome to box
```

siehe https://www.privacyidea.org/ssh-keys-and-otp-really-strong-two-factor-authentication/

- mosh
- sshfs(automounter)
- rsync
- SFTP(mit Keys)
- SCP
- ...

weitere Optionen

- TunnelDevice
- commands whitelist
- restricted shells
- fail2ban
- SSH auth_command
- ssh-agent
- AutoSSH
- sshlh

Was ist noch zu tun?

- mehr über eure Infrastrukturtools reden!
- alle Jahre mal Configs reviewen
- mit Ciphern ebenso.

Literatur

- Siehe Cookbooks (unten)
  https://en.wikibooks.org/wiki/OpenSSH/Overview
- die Distro Wikis.
- SSH manpages

Weiterhin Wissenvermittelsdurstig?

- Tolle Themen im Angebot?
- Tolle Vorträge in Berlin?
- Tolles Thema(mit Vortragenden) zu vermitteln?
- Tolles Publikum jeden ersten Donnerstag des Monats
- kontakt@flarp.de