Physische IT-Sicherheit

Hans Georg Krojanski

- **Überblick und Abgrenzung**
- **Gelände**
  - Entfernte Standorte
- **Gebäude**
  - PC-Pools, Infoterminals
  - Öffentlich zugängliche IT-Komponenten
- **Server- und Verteilerräume**
  - Beispiele und Tipps
- **Server**
- **Portable Geräte**

Überblick & Abgrenzung

- Schutz vor **physischer Einwirkung** auf **IT-Systeme**
  - Technische Defekte (Brand, Wasser, Klima, Energie)
  - Schadstoffe (Staub, Aerosole, ...)
  - (Un)befugte Personen
- **Ergänzung** zu „üblichen“ **logischen** Sicherheitsmaßnahmen
  - Zugangsschutz Administratornetz (HiWis, Reinigungspers.)
  - Zugangsschutz Serverraum?
- Wie geht ein Angreifer in der Praxis vor?
- **Manipulation, Diebstahl**
- **Maßnahmen**:
  - Abschottung, Vorbeugung
  - Monitoring, Reaktion

Universität: öffentliches Gelände

- **Entfernte Standorte: Anbindung an Infrastruktur**
  - Netzwerk, Energieversorgung
  - Absicherung des Netzwerks (WLAN, rogue access points, offene Zugänge, ..., Abstrahlung geknickter LWL-Fasern)
- **Bauarbeiten**
  - Unfälle (Bagger vs. LWL => 1 Tag Netzausfall)
  - Diebstähle

- **Zugangsschutz**
  - ~~Mauern~~
  - ~~Wachdienst~~
- Kameras?

Kameraüberwachung

- Sinnvoll oder sinnlos? (Abschreckung, Beweise, Monitoring, ...)

Gebäude

- Physische Angriffe werden oft übersehen

- Mitarbeiter oder Fremder?
- „Gesichtskontrolle“
- Ansprechen
  - Besucher
  - Handwerker
  - Reinigungspersonal

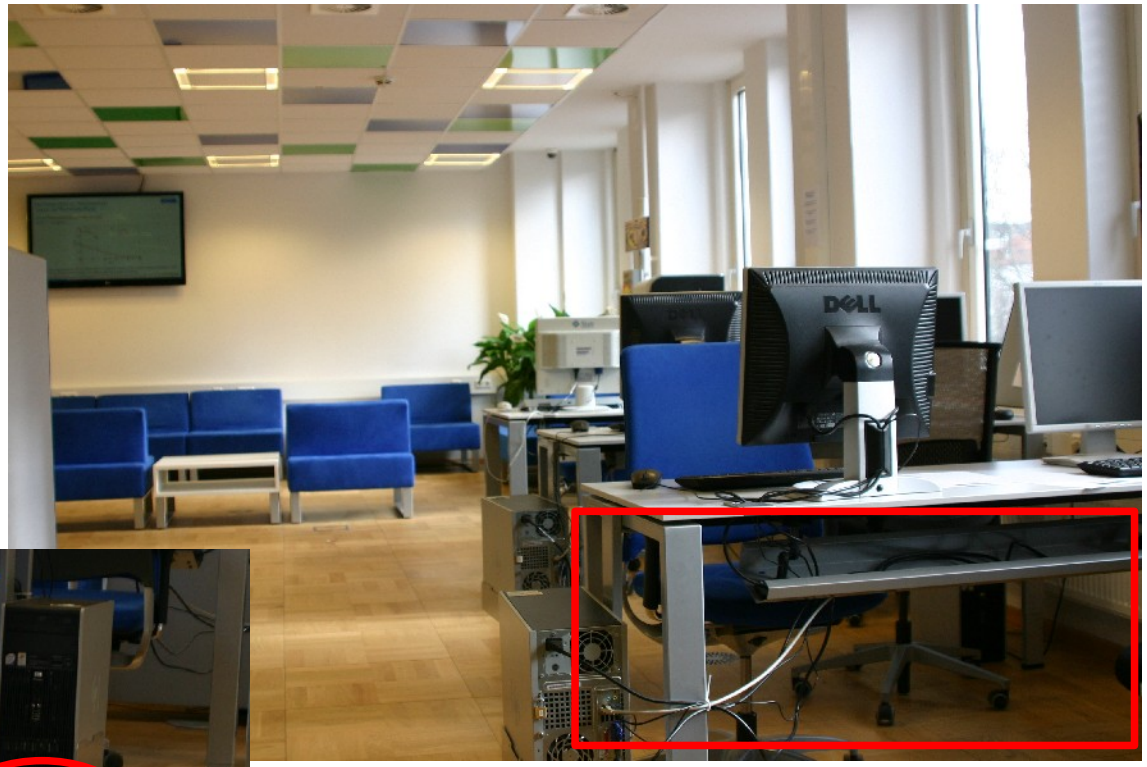
- Innentäter

Öffentlicher Bereich

- Infoterminals

Öffentlicher Bereich

- PC-Pool
- Ziele
  - Hardware
  - Informationen



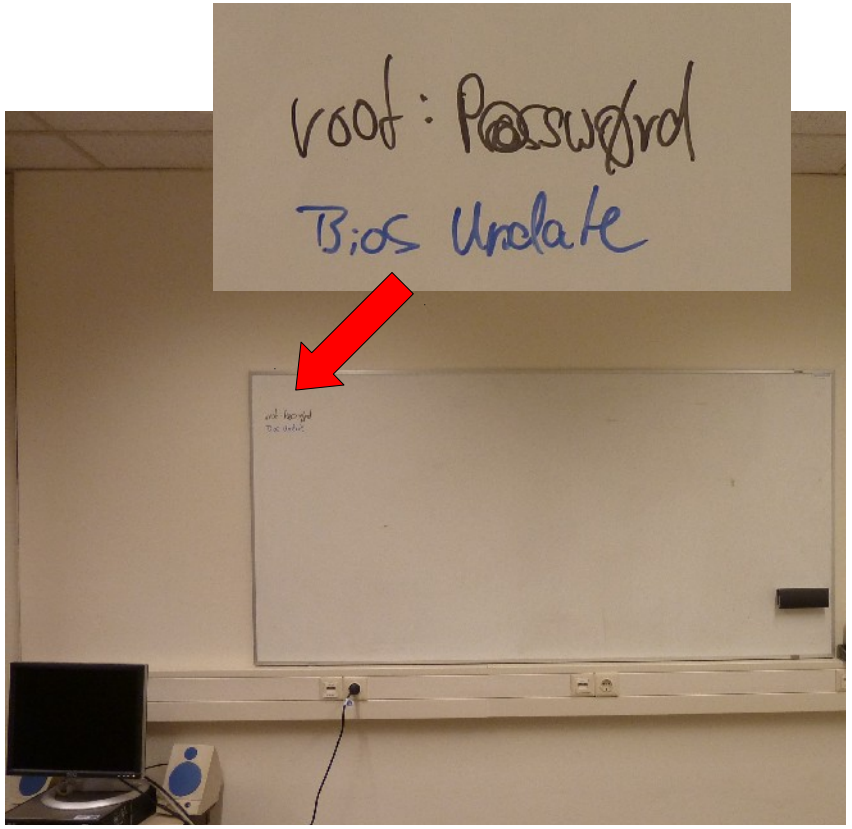
Öffentliche PCs

- **Benutzung absichern**

- Kein lokales Betriebssystem
- Kein Start von externen Medien erlauben (CD, USB-Stick)
- **Netzboot** (PXE, ...) evt. mit Netzlaufwerk für /home/<user>

Ausspähen von Informationen

- **Shoulder surfing**
  - PC-Pools
  - mobile Geräte
- Zettel, Whiteboards, ...
- **Dumpster diving**
  - Verborgene Datenspeicher!
- **Social Engineering**
- Keylogger (PS/2, USB, eingeb.!)
- Screenlogger (VGA, DVI, HDMI)
- **Zugängliche IT-Komponenten**
- TEMPEST
- Acoustic cryptoanalysis (Ultraschallmessung Kondensatoren)



Bsp.: Bildschirmsperre

- Umgehung bei physischem Zugriff (Linux)
  - **Ctrl** & **Alt** & **Backspace** (DontZap flag in xorg.conf o. ä.)
  - **Ctrl** & **Alt** & **F1**, ... (nicht eingeloggt bleiben)
  - **Alt** & **SysRq** (Druck, PrtScr) & **F**
    (echo 0 > /proc/sys/kernel/sysrq)
  - **Strg** & **Alt** & **KP_Multiply** (Feature for debugging X-Server)
    (Disable AllowClosedownGrabs in xorg.conf)

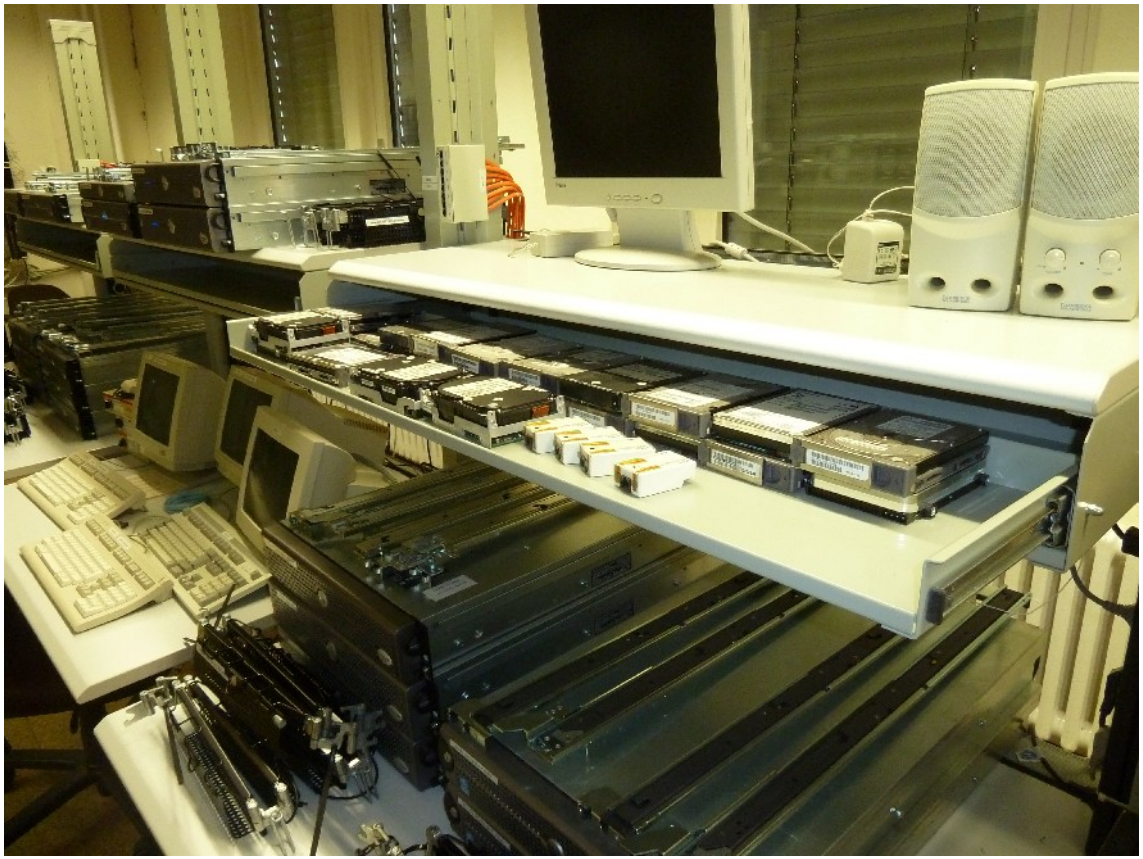
> There's little that I can do to make the screen locker secure so long as the kernel and X11 developers are *actively* working against security. **The strength of the lock on your front door doesn't matter much so long as someone else in the house insists on leaving a key under the welcome mat.**
>
> http://www.jwz.org/xscreensaver/faq.html#no-ctl-alt-bs

Öffentlich zugängliche IT-Komponenten

- **Standort** (Gänge, Empfangsbereiche, Büros, Labore)
  - Unberechtigte Benutzung
  - Ausspähen vertraulicher Informationen
- **Aufbewahrung** von Dokumenten und Datenträgern
- **Projektoren, TVs, …** (Diebstahlsicherung)
- **Fax, Kopierer, Drucker** (Umweltbelastung => nicht in Büros)
- **Server**
  - Neugierde, Manipulation, Unfälle (Kaffee, Stolpern, …)
- **Switche,** Netzwerkdosen
  - Zugang zu anderen Netzen (Backbone!)
- **Versteckte Speichermedien** (Drucker, Kopierer, WLAN, …)
  - Vorsicht bei leasing!

Entsorgung

- Server und Festplatten



Entsorgung

- Daten nicht wieder herstellbar?

Dokumente & Datenträger

- Safe > Rollcontainer

Zugangsschutz

- HLRN: Separates Gebäude
- Kameraüberwachung
- Elektronische Schließanlage

Entfernte Standorte

- Verteilerräume
  - Rechenzentrum, Fernsprechzentrale (eigenes Schließsyst.)
  - Weitere Nutzung

Verteilerräume

- **170 – 180 Verteilerräume**
- **Gebäudeversorgung**, z.T. **Etagenversorgung**
- Anforderungen (Größe, Anschlüsse <90m, Klimatisierung)
- **Probleme** bei **Mehrfachnutzung**
  - Zweckentfremdung (Abstellkammer, ...)
  - Zusätzliche Server => mehr Zugänge nötig (auch Firmen)
  - Transponderverwaltung uneinheitlich (zentral vs. lokal)
    Plötzlich versperrte Zwischentür
  - Zuständigkeitsprobleme

    Verantwortung für die Wartung der Raumklimaanlagen?
- Bsp.: Telefon abhanden gekommen; entdeckt durch Nagios
- **Schränke** mit **speziellen Schlössern** versehen
- **Monitoring** (Zugang, Feuer, Wasser, Klimatisierung, ...)

Monitoring

- Temperatur
- Luftfeuchte
- Rauchmelder
- Wassersensor
- Glasbruchsensor
- Airflow Sensor
- Bewegungsmelder
- Magnetkontakt-Sensor
- Stromsensoren (Gleich-, Wechselstrom)
- Überwachungskameras
- ...
- **Einsatz ist Abwägungssache**

Serverräume

- **Server-Standort**: hinter **verschlossenen** Türen, nicht einfach hinter einer Tür mit Schloß
- Elektromagnetismus (Blitz)
- Schadstoffe (Staub, ...)
- Klimatechnik
- **Brandschutz**
- **Wasserschutz**
- Zugangsbeschränkung
- **Aber:** irgendjemand benötigt Zugang, daher...
- **Limitierung des Umgangs**
- Bildschirmsperre (Lights Out Management & lok. KVM), BIOS, Diebstahlsicherung, ..., Full Disk Encryption

Brandschutz

- **Baulicher Brandschutz:** Feuerbeständige Wand F-90, ...
  (F-90: Wohnungstrennwände, Türen darin T-30)
- **Vermeidung** von **Brandlasten**
- Automatische Feuerlöschanlage?
- **Brandfrüherkennung**
- **Verhaltensweisen**
- Routine durch **Übungen**
- **Bsp.**: Serverraum ohne Brandlasten
  - Aber Nachbarraum!
  - Hitzeübertrag durch Wände
  - Schnell & unerkannt

Löschmittel

- Einsatz je nach **Brandklasse** (brennende Stoffe)
- **Haupt**- und **Nebenlöschwirkung** beachten!
- Evt. Explosionsgefahr, Säurebildung
- **Wasser** (Abkühlen, Ersticken)
- **Löschschaum** (Stickeffekt durch Trennung, Abkühlen)
- **Löschpulver** (Ersticken oder Inhibition)
- ... können mehr Schaden zufügen
  als ein verschmortes Kabel (o.ä.)
- **Inertgase** (Ar, N, CO_2)
  (Stickeffekt; Verdrängung des Luft-
  sauerstoffs unter den Grenzwert
  für Verbrennung 13,8 Vol.-% [von 20,9])
- **Halone** (Inhibition)

Fluchtwege

- **Notwendig** (Gaslöschanlagen in Serverräumen)

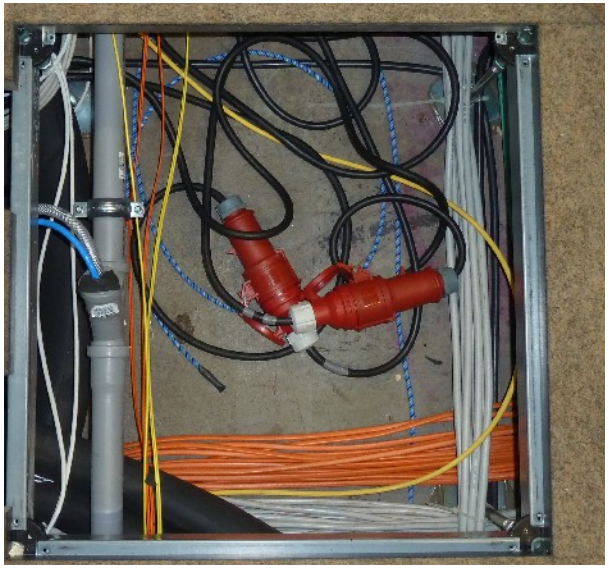
- **Angreifer** können Fluchtwege rückwärts gehen…
- Fluchttüren von Außen öffnen mit **Türklinkenangel**

Wasserschutz

- **Leckage** der **Klimaanlage**
  (hochreines Wasser)
- **Leckage wassergekühlter Serverschränke**
- **Kondenswasser**
- **Wasserrohrbruch**
- **Heizleitungsbruch**
- **Sprinkleranlagen**
- **Witterungsschäden**
- **Grundwasserschäden**
- Vandalismus
- Wiederanlaufzeit ???

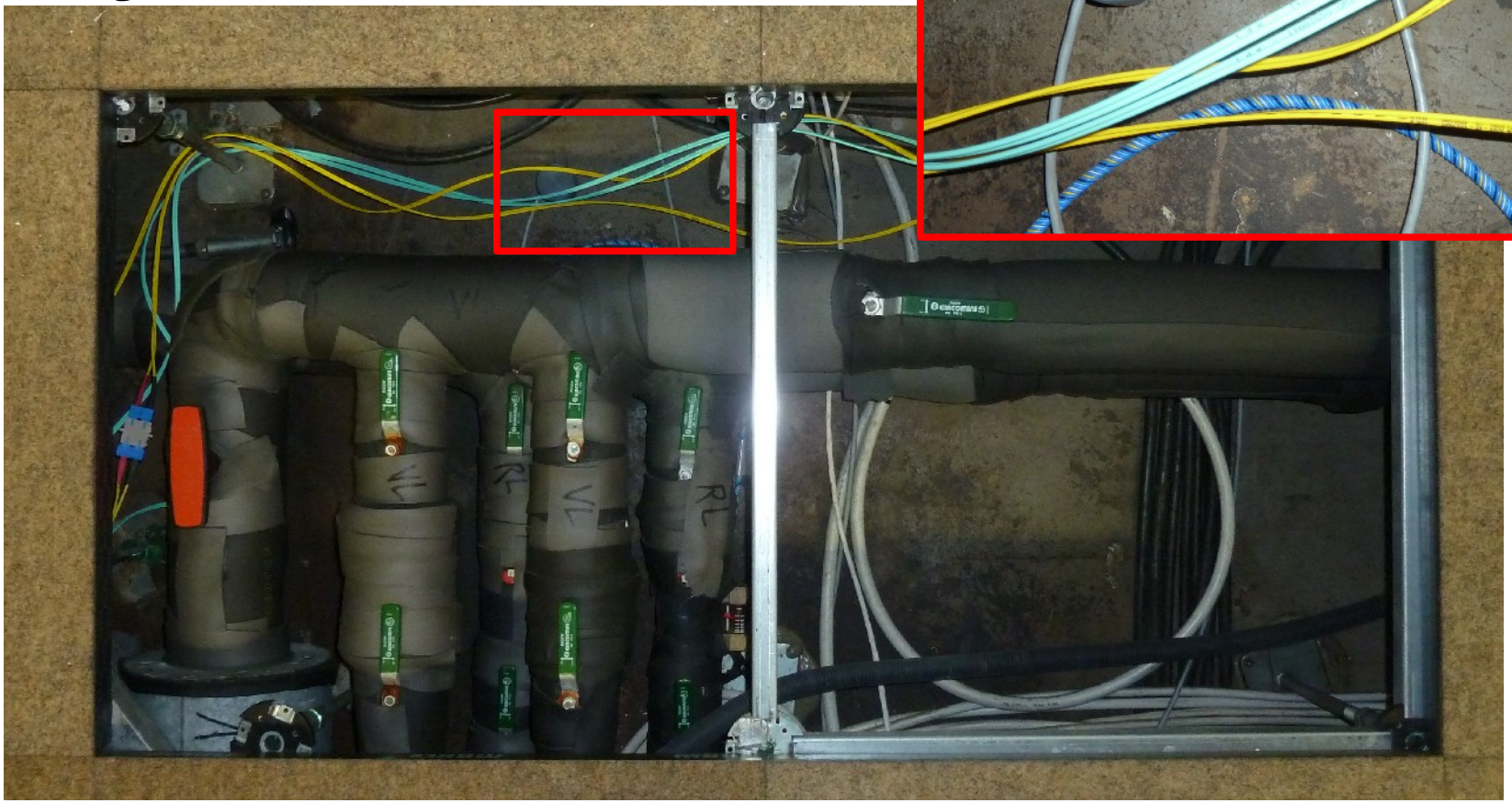
Wassersensoren

- Einsatz in weiten Bereichen:
  Sensor-Kabel
  Hauptsensormodul
- **Funktionsweise**:
  kapazitive Widerstands-messung
- Unterscheidung Wasserart möglich
- **Alarmierung**: E-Mail, SMS, Telefonanruf, SNMP-Traps, ...
- **Punktgenaue Ortung**
  (R ~ l)



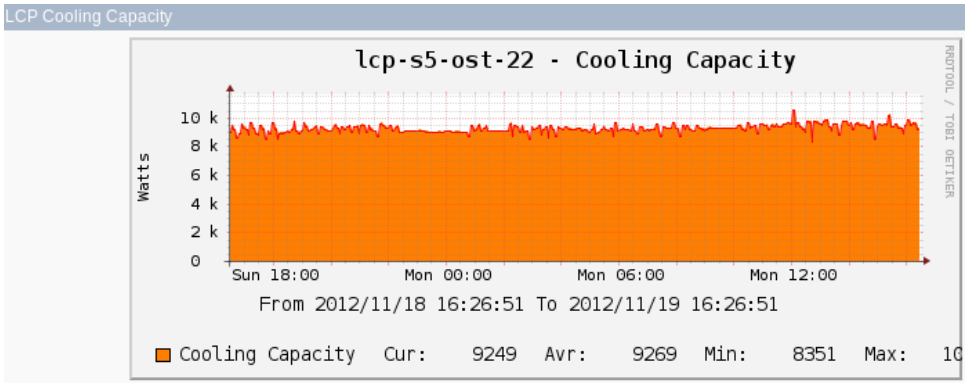
Wassersensoren

- Wasserkühlung
- Digitales Sensorkabel



Bsp.: Wassergekühlte Racks

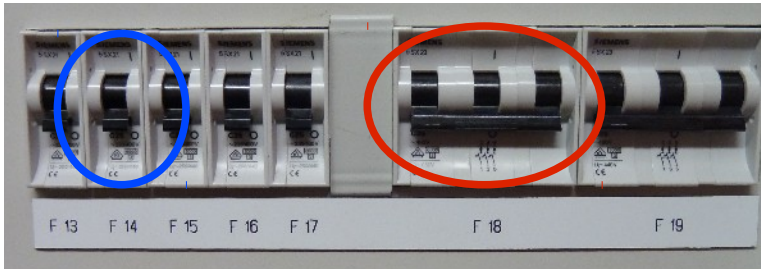
- Automatische Türöffnung (?!)
- Überwachung (Nagios, Cacti)
  - Flow Rate 19 L/min
  - Server-In/Out Temp. 20°/28°
  - Water-In/Out Temp. 11°/18°

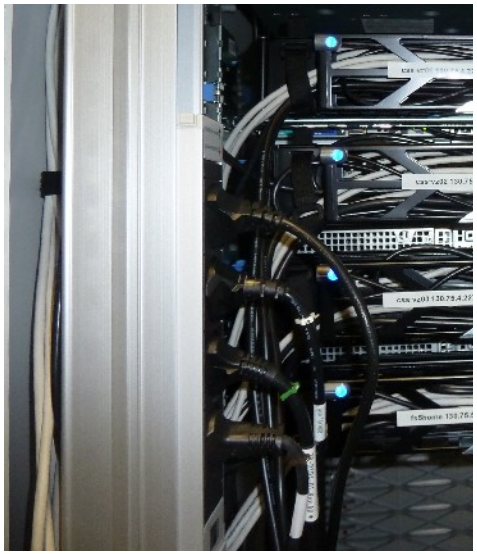


Host	Service	Status	Last Check	Duration	Attempt	Status Information
lcp-s5-ost-22.tin	Cooling Capacity [Watts]	OK	2012-11-19 16:30:51	182d 6h 47m 4s	1/4	SNMP OK - 9831
	Fan Speeds [rpm]	OK	2012-11-19 16:29:11	182d 6h 47m 4s	1/4	SNMP OK - 1590 1620 1590 1545 1470 1455
	Flow Rate [l/min]	OK	2012-11-19 16:30:56	161d 4h 59m 44s	1/4	SNMP OK - 19
	Server-In-Temperature [deg C]	OK	2012-11-19 16:29:58	161d 5h 12m 51s	1/4	SNMP OK - 20
	Server-Out-Temperature [deg C]	OK	2012-11-19 16:28:00	182d 6h 46m 55s	1/4	SNMP OK - 28
	Water-In-Temperature [deg C]	OK	2012-11-19 16:29:41	182d 6h 46m 55s	1/4	SNMP OK - 11
	Water-Out-Temperature [deg C]	OK	2012-11-19 16:29:58	182d 6h 46m 55s	1/4	SNMP OK - 18

Stromverteilung im Rack: PDUs

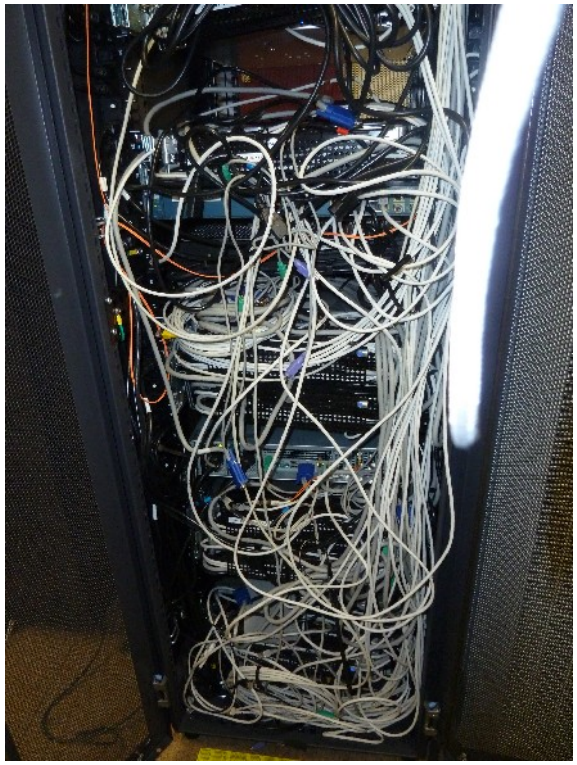
- PDUs – wo angeschlossen?
- CEE-Drehstromsteckverbinder
  - 1-phasig (230V/16A)
  - 3-phasig (400V/16A)





Racks & Verkabelung

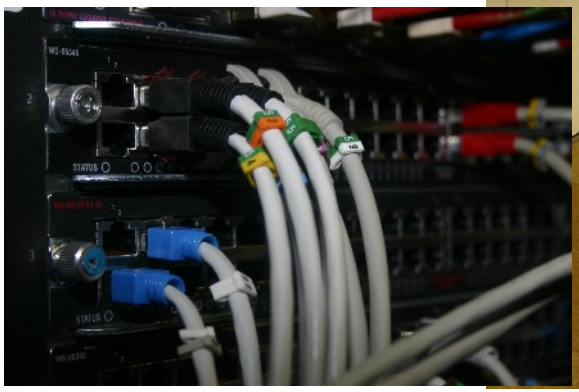
- Kabelgewirr und die Folgen…



Racks & Verkabelung

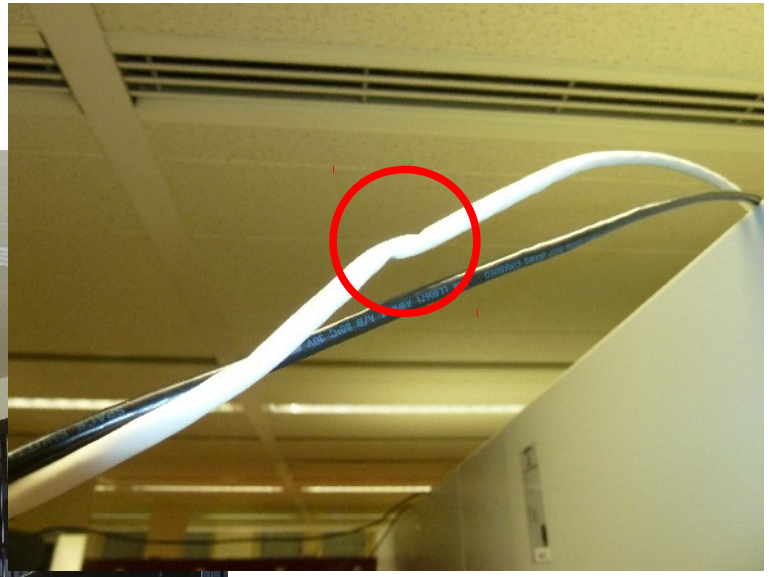
- Normale Verkabelung

- Kennzeichnung



Sonstige Verkabelung

- cosh(x)



Sonstige Verkabelung

- Für Testsetup duldbar; sollte nicht von Dauer sein…

Gefährliche Konstruktionen

- Server (19'') balanciert auf Tower; Monitor, Tastatur oben drauf

- Server...

  ... auf dem Boden

  ... direkt unter Arbeitsplatz

Lampertz Sicherheitsraum

- Im HLRN-Gebäude (Backup & Archiv)
- Brandschutz
- Wasserschutz
- Staubdicht
- Korrosive Brandgase
- Trümmerlasten
- Fremdzugriff
- Explosion
- Sauerstoffreduziert

- Auch für 19''-Racks, modular, eigenständige Klimatisierung, unabhängige Stromversorgung, Brandmeldeanlage, ...

Abstellraum

- Baustaub
- Klimatisierung
- Zugang (Drucker)
- Externe Festplatte
- Serverhardware?

Serverhardware und -absicherung

- **Konfiguration**:
  - 2HE, 2 CPU Sockel
  - Redundante Netzteile; USV
    Vorsicht bei Anschlüssen
  - ECC-RAM (1-Bit-Fehler Korrektur, 2-Bit-Fehler Erkennung)
  - RAID-Kontroller (mit BBU: Akku für Cache)
  - Festplattentyp (SAS, Nearline-SAS, SATA, SSD, ...)
- **Gefährdungen**:
  - „Backup“-Festplatte
  - RAID: Monitoring nötig;
    Sonst unentdeckte Entwendung möglich
    Bsp.: RAID-1 & hot swap & automatischer rebuild

Nutzer tragen Daten mit sich herum

- **Diebstahlgefahr** (mobile Geräte, USB-Sticks & -Festplatten)
- NASA Laptop und Dokumente aus Auto entwendet (31.10.)

  http://www.spaceref.com/news/viewsr.html?pid=42609

  => zukünftig Festplattenverschlüsselung
  => Löschung nicht benötigter Dateien
  => keine Speicherung auf mobilen Geräten
- **Reisen:** Notebooks in ICEs, Hotelzimmer, ...
  - Verschlüsselung, ..., „leere“ Notebooks & VPN
- Notebook-Anschlüsse (Firewire, PCMCIA, ExpressCard, ...)
  - DMA (Direct Memory Access via PCIe Bus)
  - Lesen und überschreiben beliebiger RAM-Inhalte
  - CPU & OS bekommen nichts davon mit
  - Firewire, Thunderbolt (=> daisy chaining up to 6 devices...)