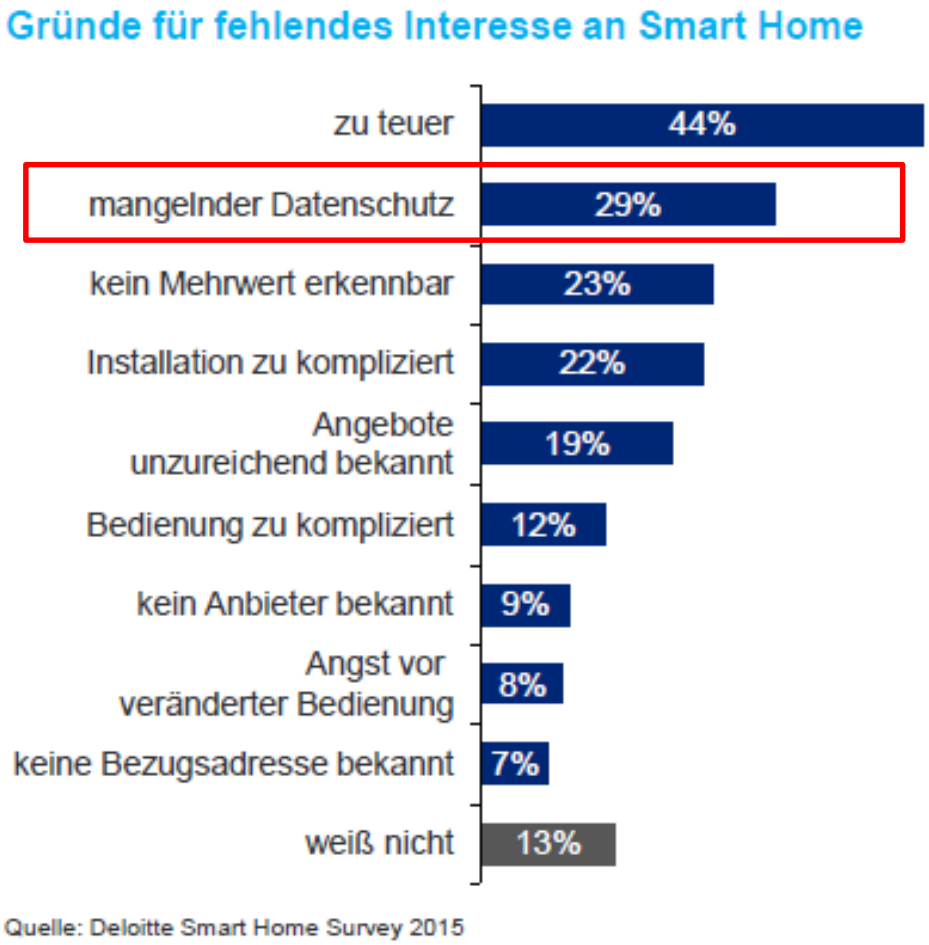
Visualisierung und Informationssicherheit

KNX Symposium

23. Oktober 2015

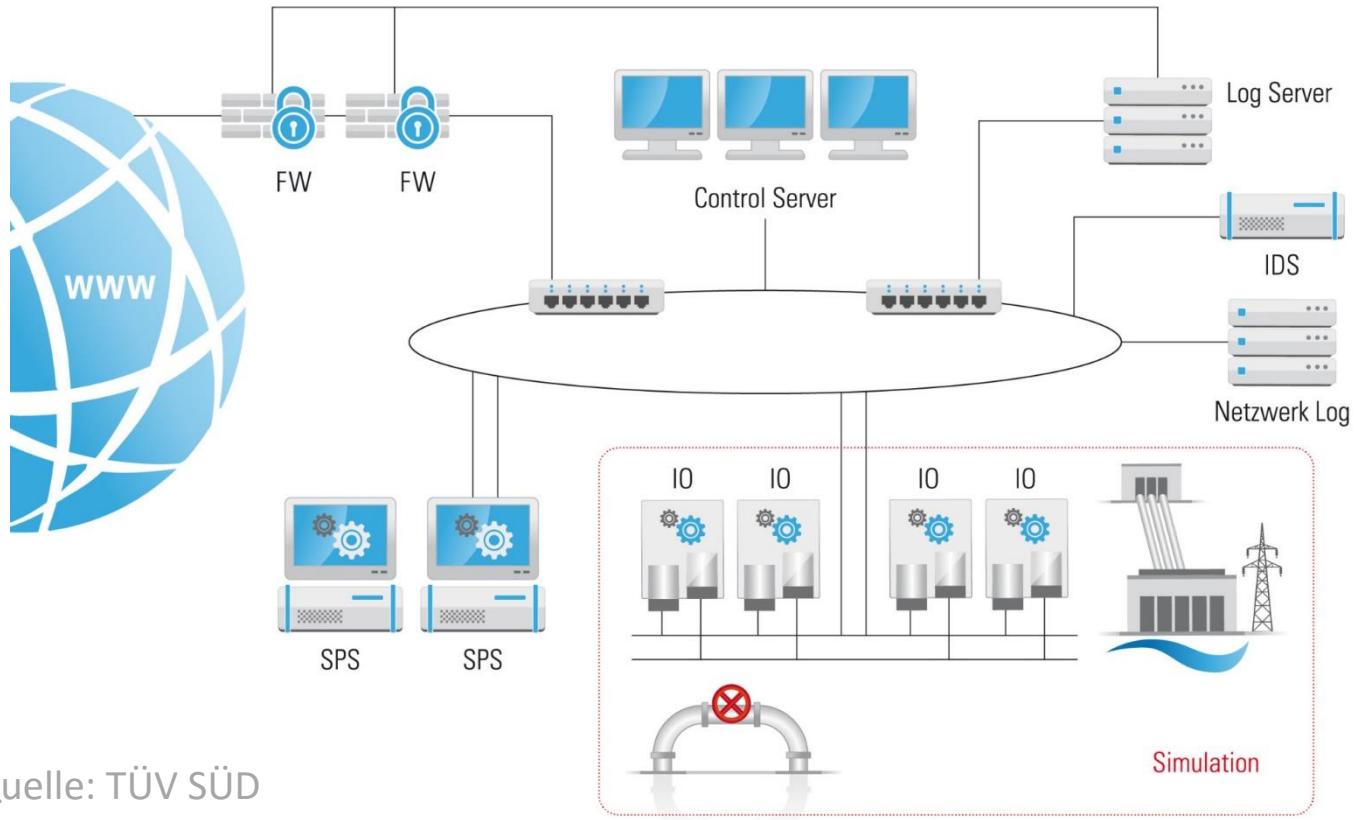
Markt Schwaben

Sicherheitsbedenken



… zu recht!

Logische Struktur des Honeynet



Quelle: TÜV SÜD

… zu recht!

28.07.2015

Mehr als 60.000 Zugriffe auf eine virtuelle Infrastruktur verzeichnete TÜV SÜD in der achtmonatigen Laufzeit eines Honeynet-Projekts. […]

Mit dem Honeynet-Projekt hat TÜV SÜD den Nachweis erbracht, dass Infrastrukturen und Produktionsstätten gezielt ausgeforscht werden.

Quelle: Pressemitteilung TÜV SÜD

Wachsende Gefahr
oder wachsende Aufmerksamkeit

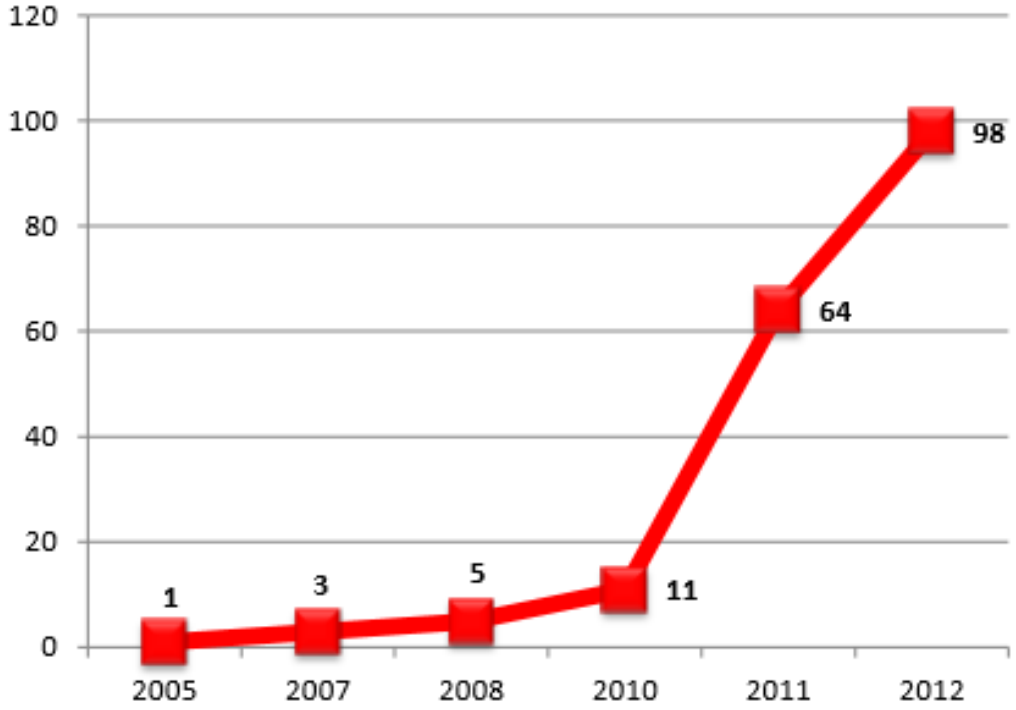
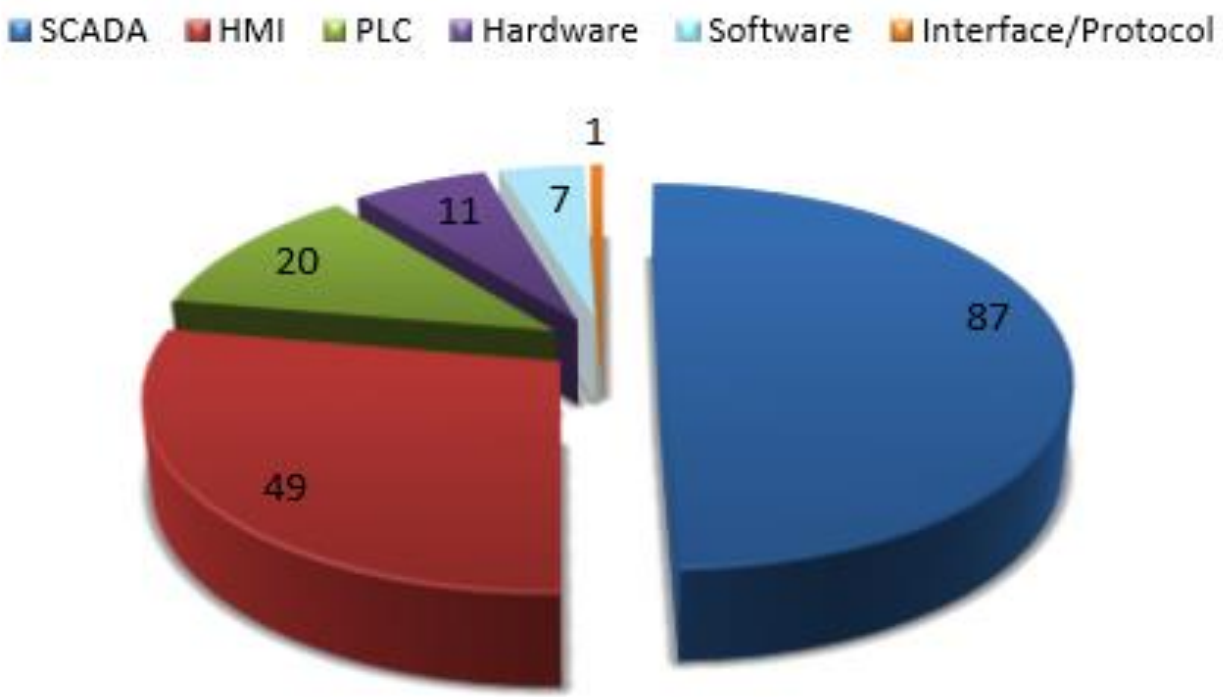


Figure 1. Number of ICS Vulnerabilities Reported

Quelle: http://www.ptsecurity.com/upload/ptcom/SCADA_WP_A4.ENG.0018.01.DEC.29.pdf

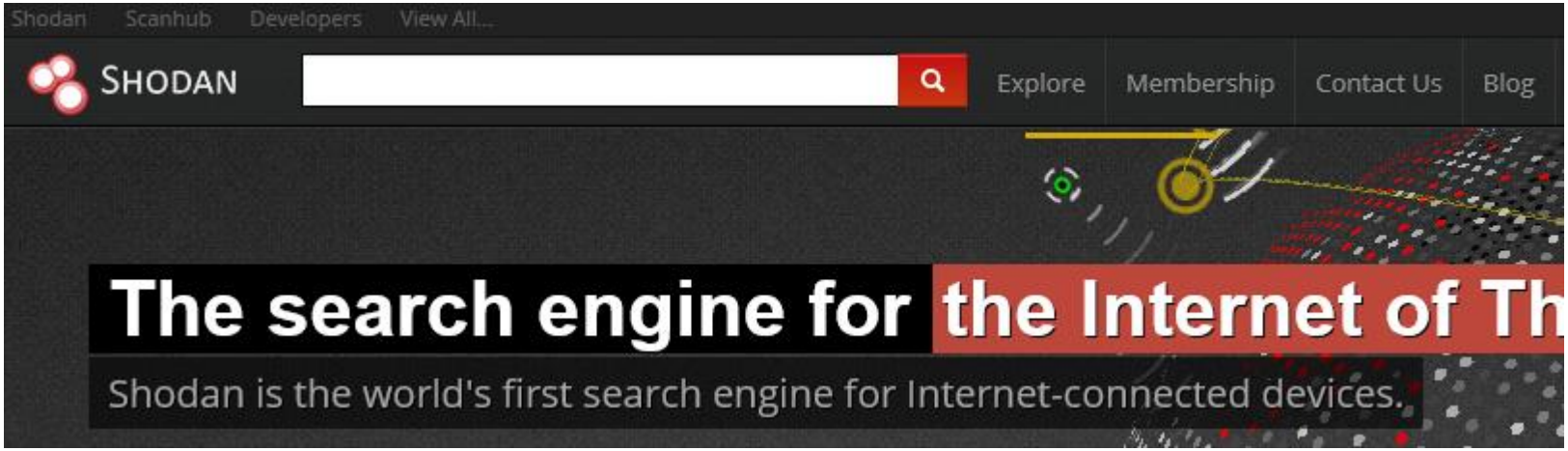
Visualisierung als Einfallstor



Quelle: http://www.ptsecurity.com/upload/ptcom/SCADA_WP_A4.ENG.0018.01.DEC.29.pdf

Wachsende Gefahr

- https://www.shodan.io/



Sicherheitsanalyse

- Schützenswerte Güter
- Bedrohungsanalyse
- Sicherheitsziele
- Sicherheitsfunktionen

Szenarien

- Eigenheim
- Hotel
- Universität
- Industriebetrieb
- Bank
- Krankenhaus
- …

Schützenswerte Güter

- Passiv
  - Aktuelle Zustände
  - Historische Daten
    (Alarm, Werte-Aufzeichnungen)
  - Zustand von Funktionen
    (z.B. Zeitprogramme)
  - Verwaltungsdaten (z.B. Login-Protokolle)
  - Webcams etc.
  - Personenbezogene Daten

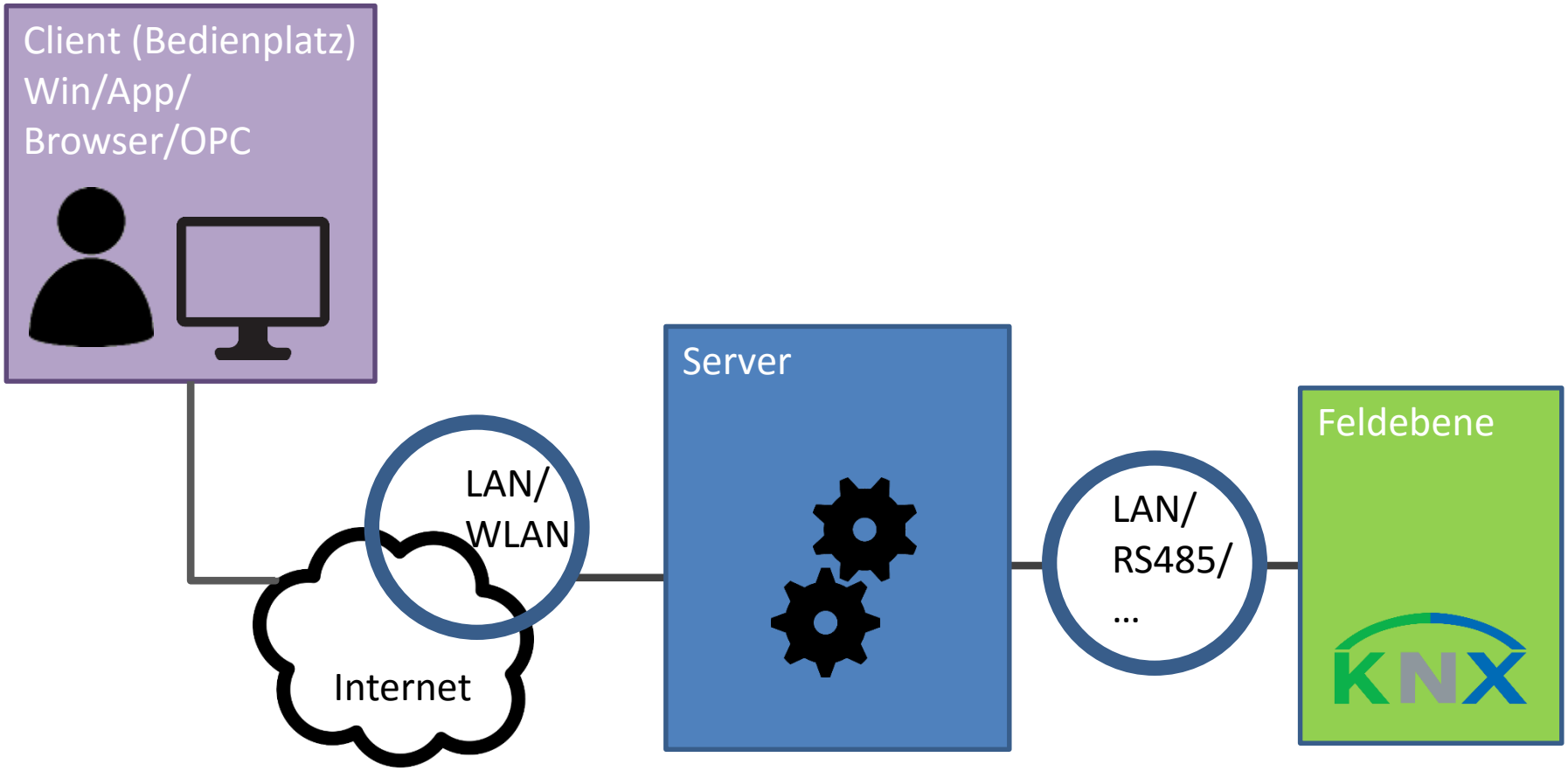
Schützenswerte Güter

- Aktiv
  - Ändern von Werten
  - Ändern von Funktionen (z.B. Zeitprogramme)
  - Ändern der Konfiguration
  - Ändern der Zugriffsrechte

Schützenswerte Güter

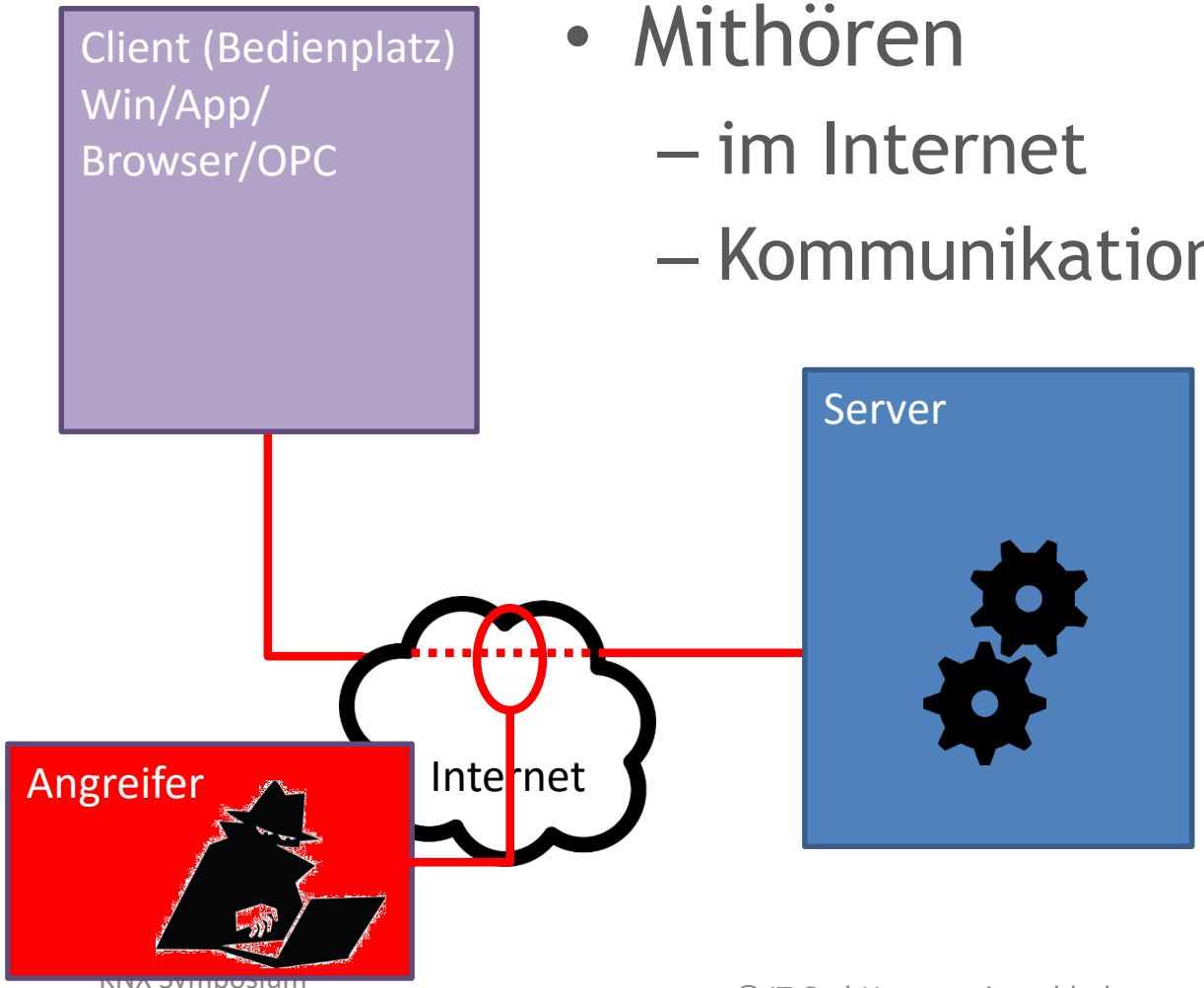
- Manipulation
  - Anzeige aktuelle Zustände
  - Historische Daten
    (Alarm, Werte-Aufzeichnungen)
  - Zustand von Funktionen
    (z.B. Zeitprogramme)
  - Verwaltungsdaten (z.B. Login-Protokolle)

Bedrohungsanalyse

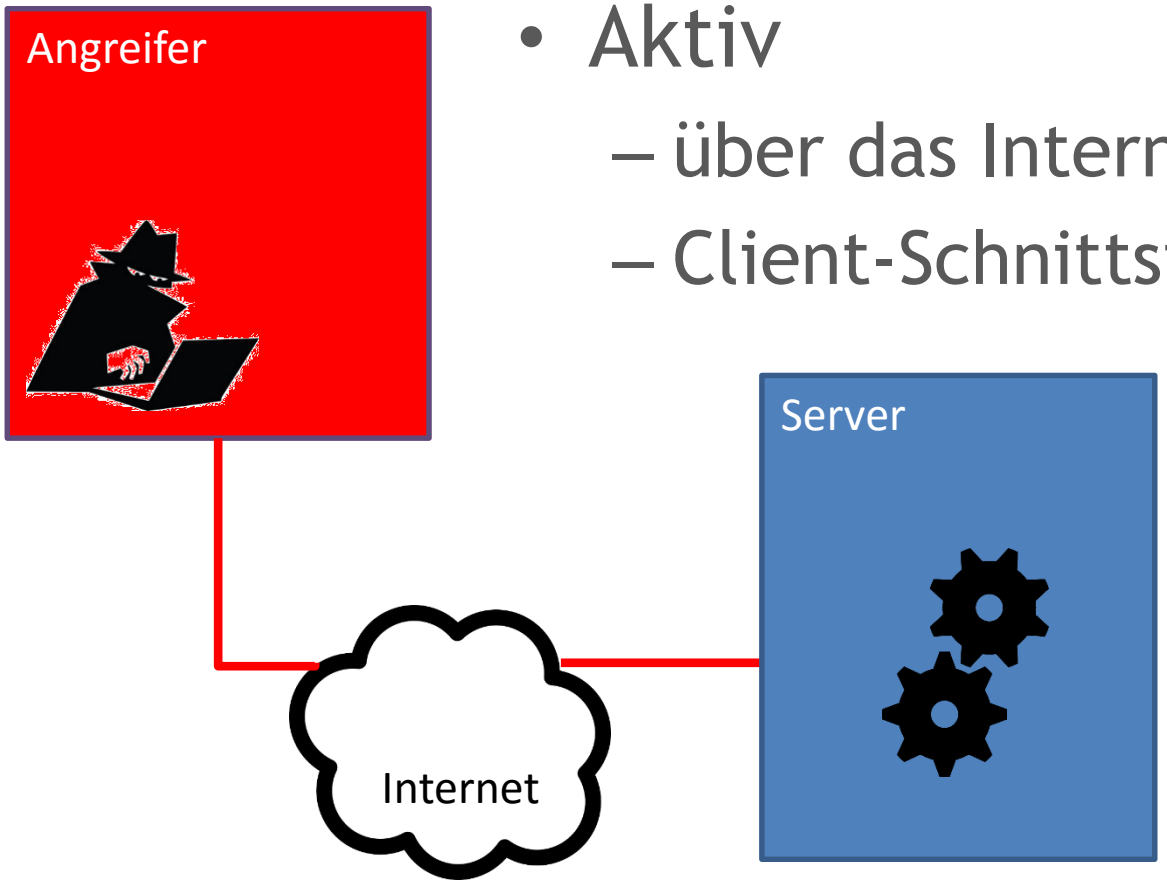


Bedrohungsanalyse

- Mithören
  - im Internet
  - Kommunikation Client-Server



Bedrohungsanalyse



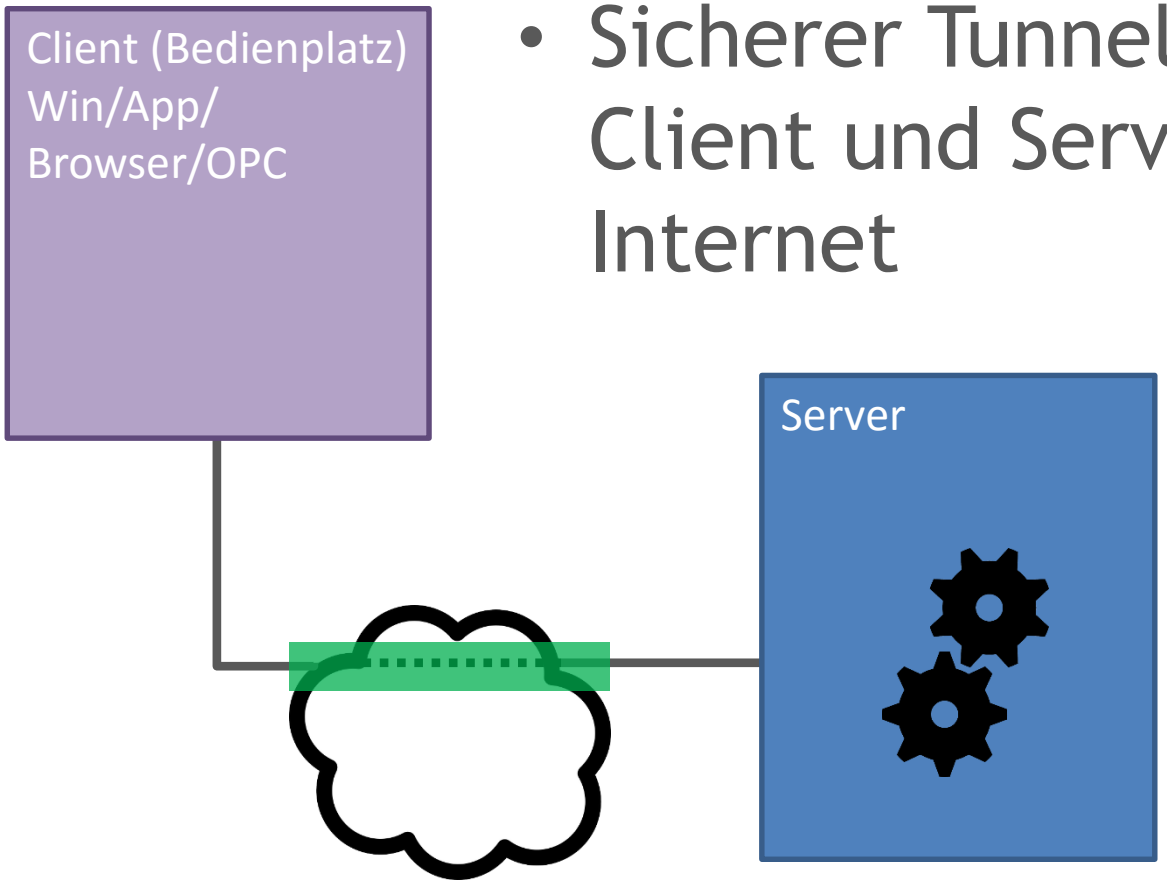
- Aktiv
  - über das Internet
  - Client-Schnittstelle des Servers

Client-Schnittstelle im Internet

- „Port-Weiterleitung“
  = Server im öffentl. Internet sichtbar
- Nur akzeptabel, wenn
  - HTTPS mit vertrauenswürdigem Zertifikat
  - Client muss Zertifikat auch prüfen
  - Minimierung der exponierten Dienste
  - Ständige OS-Pflege gewährleistet
  - Einbruchserkennung (Intrusion detection)

→Das wollen Sie nicht wirklich

VPN

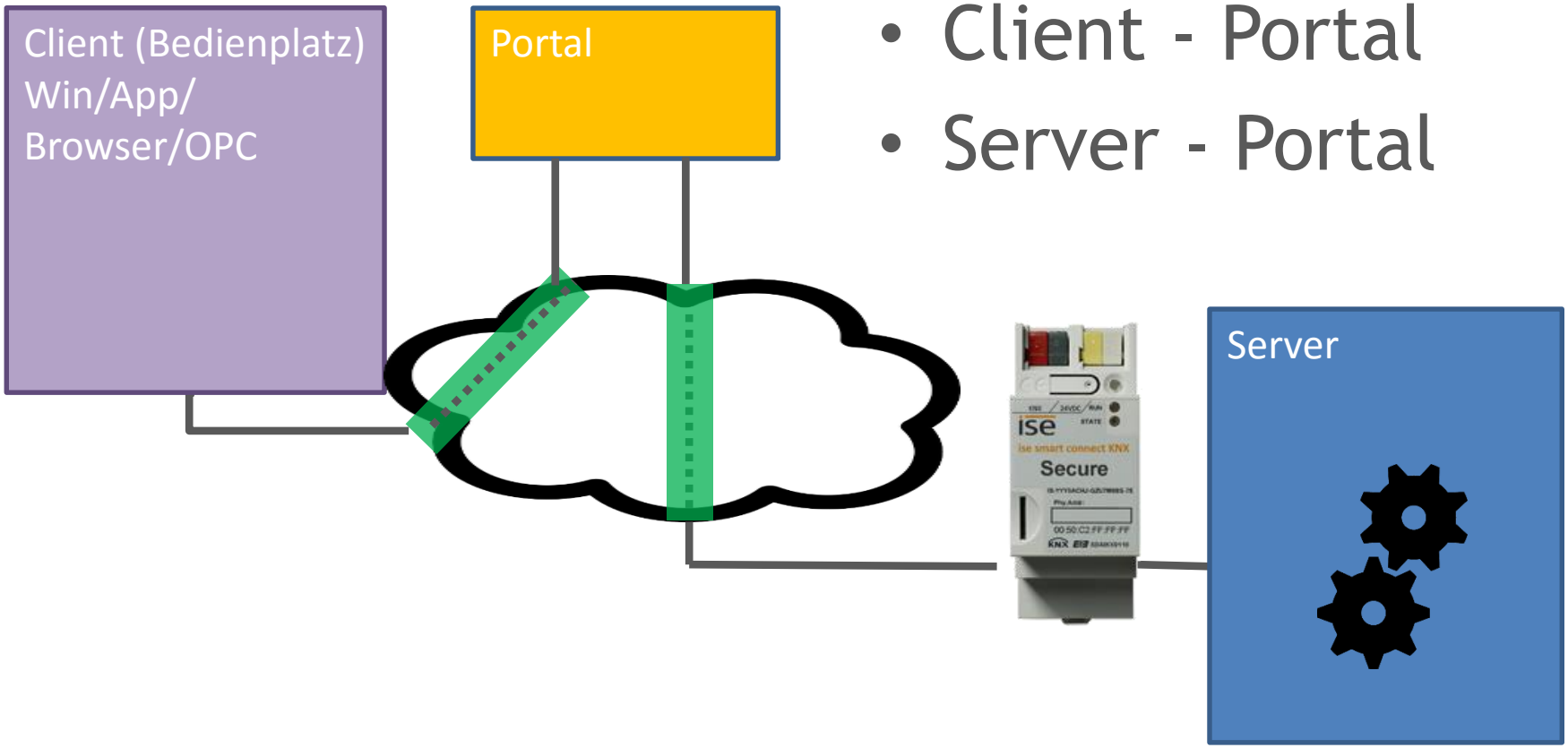


- Sicherer Tunnel zwischen Client und Server durch das Internet

VPN

- Konfiguration auf dem Router
- Konfiguration/Installation auf dem Client-Gerät/Computer
- „VPN on demand“ vereinfacht Handling auf Client-Gerät/Computer

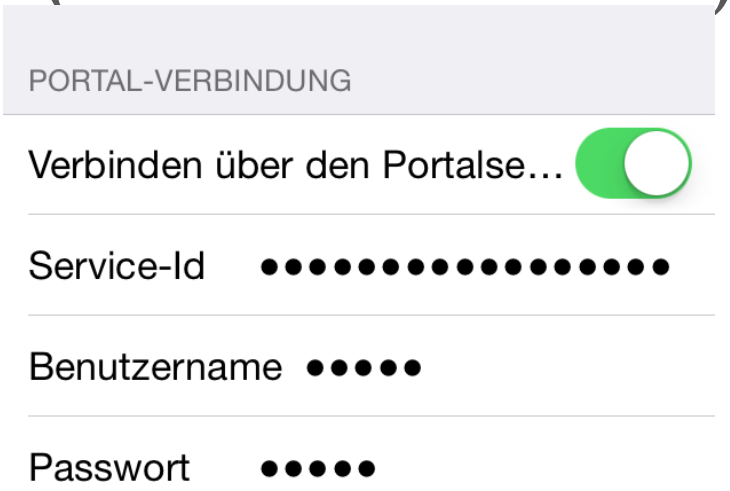
ise smart connect KNX secure



- Client - Portal
- Server - Portal

ise smart connect KNX secure

- Konfigurationsfrei auf dem Server
- Auf dem Client (hier Elvis Viewer)

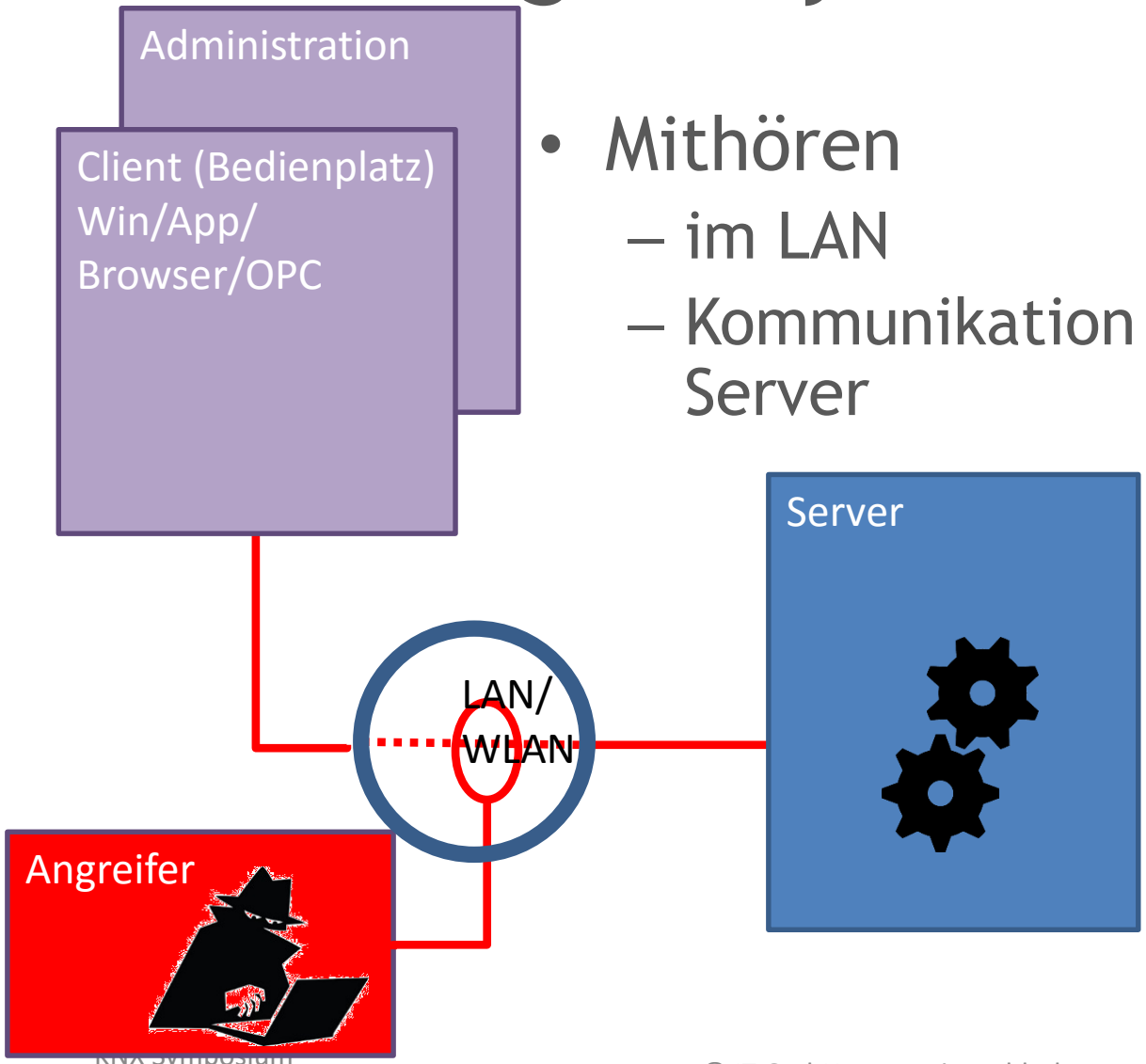


Im LAN alles im Griff?

- Wirklich alle Geräte vertrauenswürdig?
  - Router
  - Fernseher, HiFi, Kühlschrank, …
  - Smartphones
  - Zugängliche Netzwerkdosen
  - Gastzugänge

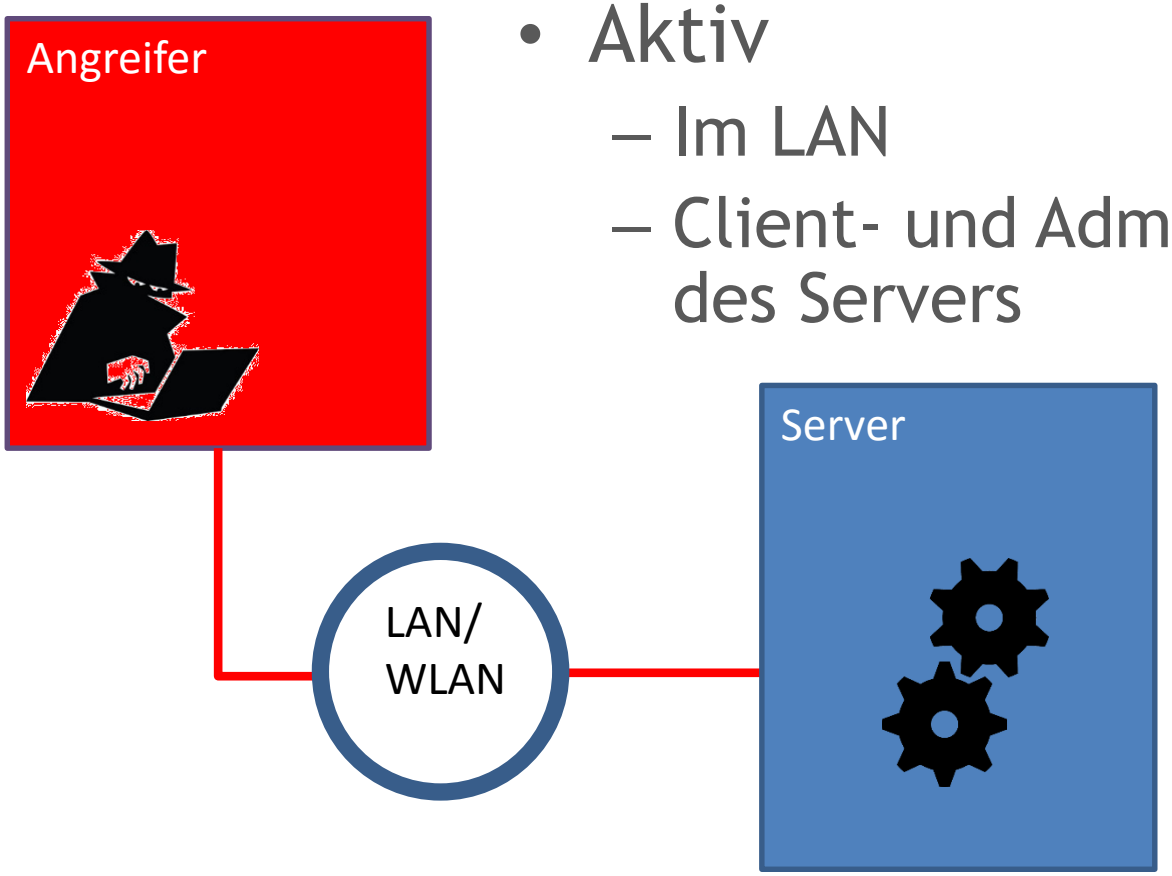
→ Perimeter-Sicherheit reicht nicht

Bedrohungsanalyse



- Mithören
  - im LAN
  - Kommunikation Client-/Admin-Server

Bedrohungsanalyse



- Aktiv
  - Im LAN
  - Client- und Admin-Schnittstelle des Servers

Verschlüsselung

- In Elvis automatisch
- Server-Zertifikat
  - Selbstsigniert
    - nur Verschlüsselung
    - keine Identitätssicherstellung
  - CA-signiert (z.B. Domäne)
    - Nachweis der Server-Identität
- Überprüfung: Wireshark

Verschlüsselung

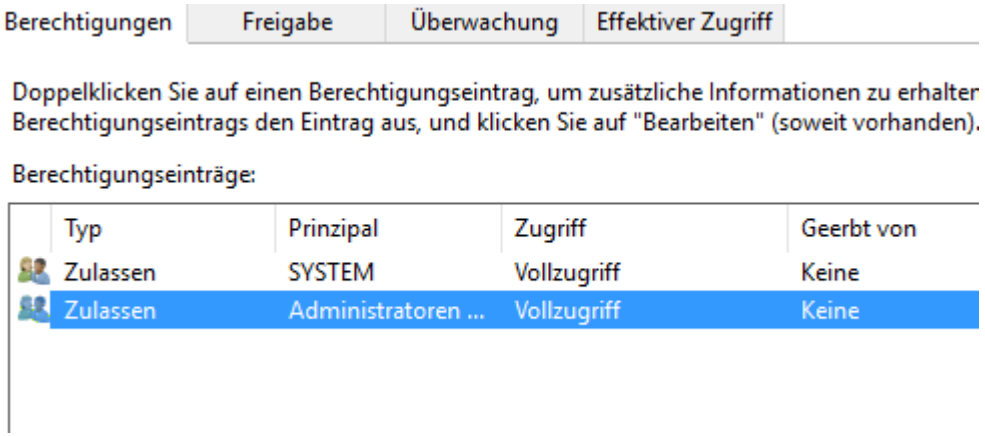
```
D.... ..3D.......V.W......+uuid-4758803e-b888-408f-8130-19ddcaba4fe7-1..t~..uRhttp://
docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsdW...t.................`...M..V.o..9.[h.0.yu.;\I.*...}d
$...x.. ..... ......+.3*0R).<T......H.."......................0...0.........'..."*..GB
[.Z...0
..*.H..
.....0.1.0...U...
SUPPORT-110..
121120230000Z.
221120230000Z0.1.0...U...
SUPPORT-110.."0
..*.H..
..........0..
.........IX.3......

p.b|.4.X...=..-..zR..o>...<...~,Rh5.%.;..X
C.2......WY......"*....C....`8.....T...^]s.,;...g.G.
..._V...M.........W....
UR]....$.r.3W.@. .yCW9..<......B.V...4...;..N.......&|......M.*(
,...F1lq.{....'....?;..u..=[..'.9V8..*FB.h..#%`..J.C..0.
D..p.....}$7S]..h..p8..f..i.s....._....T.W..Yr..??..v..Z.0.y<1....uda.._.[.2.!
cPu...d..b..).i8.sZ..S..7...4Z\.c&S....{lDu.4...V...y..:f.H*P........<
+Q;.~...TZ...O.3.......J;{...@...'.^....<;.'.n...I...FO..U.@
..........1/....jvXhLbq.3.#..x}r..i.......s.!P.c........O
..*.H..
..........^>p>j..:..P.......$....%
~b.4.......*.<.a........&..C.....>t?..h..1Be......k..NuN\.}n
```

VLAN

- Sicherheitsfeature?
  - „Dynamisches VLAN“
  - Switch
  - Router / Firewall

Weitere Sicherheitsmaßnahmen

- Server physisch wegsperren
- Wenig Netzwerkdienste (nur Elvis Server, ggf. IIS und Remote Desktop) + Firewall
- Zugriff auf Server-Dateien auf Elvis-Dienstkonto und Administratoren beschränken

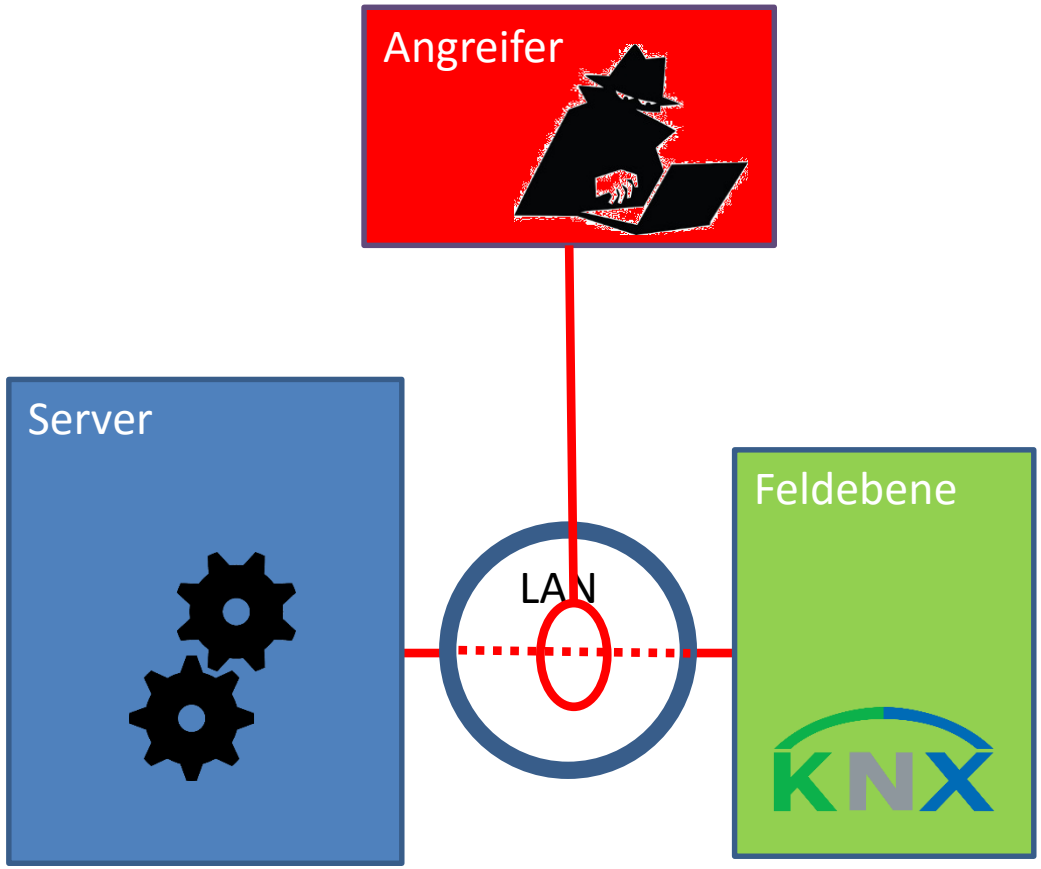


Feldebene

- Direkter Angriff auf KNX, Modbus, …

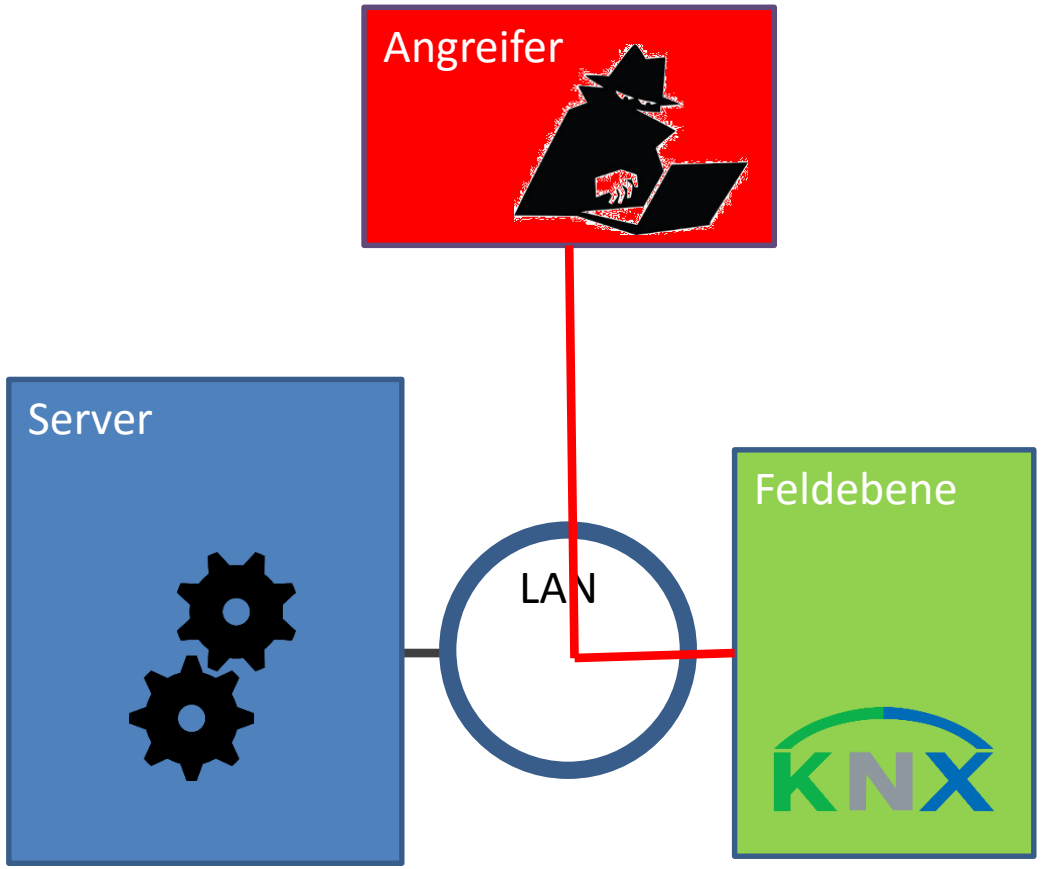
Bedrohungsanalyse

- Mithören
  - Z.B. KNXnet/IP-Kommunikation



Bedrohungsanalyse

- Aktiv
  - Z.B. KNXnet/IP-Kommunikation



Sichere KNX-Kommunikation

- Besonders relevant für IP und RF
- Einführung 2016 (ETS 5.5)
- Telegramme verschlüsselt
- Geräte im Secure-Mode
  - Nur mit Geräteschlüssel umkonfigurierbar
  - Akzeptieren nur korrekt verschlüsselte Gruppentelegramme von bekannten Sendern

Sichere KNX-Kommunikation

- Auswirkungen auf Visualisierung
  - Empfangen: Visualisierung muss Gruppenadress-Schlüssel kennen
    → Import der Schlüssel aus ETS
  - Senden zusätzlich: Visualisierung muss Empfängern bekannt sein
    → Visualisierung in ETS zu projektieren!
    (ähnlich Visu-Dummy)

Elvis: Sichere KNX-Komm.

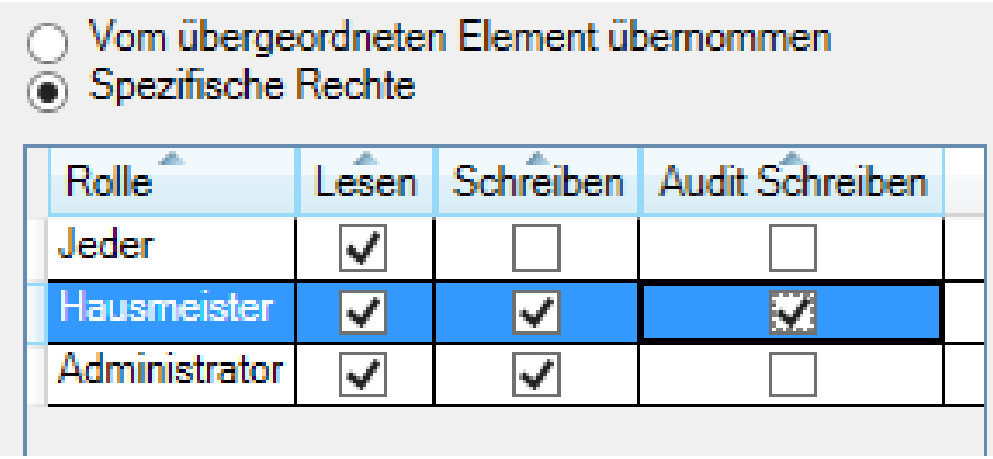
- Unterstützung, sobald ETS + Falcon verfügbar
- Keine zusätzlichen Projektierungsschritte

Zurechenbarkeit (Nichtabstreitbarkeit)

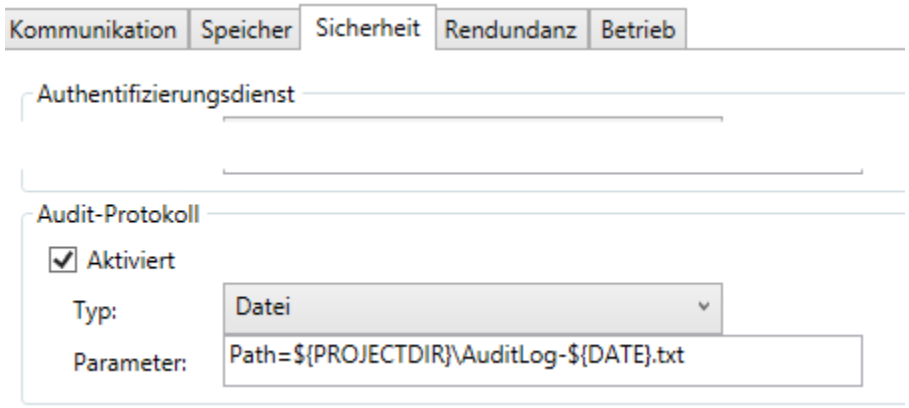
- Protokollieren von Änderungen mit Urheber und Zeitstempel
- Überzeugende / ggf. „fälschungssichere“ Ablage

Elvis: Audit

- Ins Elvis-Rechtesystem integriert:



Elvis: Audit



- Typ:
  - Textdatei
  - Datenbank
  - Windows Eventlog
  - …

Markthemmnis Sicherheits-Defizite

- Aufgabe für
  - Institutionen (KNX)
  - Hersteller (Geräte, Visualisierungen)
  - Systemintegratoren
- Mit Elvis sind durchgehend sichere Lösungen einfach realisierbar