KOMPETENZZENTRUM
DIGITALES HANDWERK

BFE
OLDENBURG

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Lösungen für den sicheren Fernzugriff auf die Unternehmensdaten

Vortrag am 11. April 2018 in HWK Oldenburg

BFE Oldenburg
Bundestechnologiezentrum für
Elektro- und Informationstechnik e.V.

Dipl.-Ing. Werner Schmit, Dozent und IT-Security-Beauftragter (TÜV)

Kurzvorstellung: Dipl.-Ing. Werner Schmit

- Dozent am Bundestechnologiezentrum für Elektro- und Informationstechnik (BFE Oldenburg)
- Arbeitsschwerpunkte
  - Informationssicherheit
  - Datennetzwerktechnik
  - GNU/Linux
  - Systempflege E-Learning-Server
  - Programmierung (C/C++, Java, PHP)

- IT-Security-Beauftragter (TÜV)
- IT-Security Auditor

- Kontakt
  E-Mail: w.schmit@bfe.de
  Tel.: 0441-34092458

Agenda

1. Einleitung
2. Lösungen / Konzepte für den Fernzugriff
3. Welche Lösung eignet sich wofür? – Einige Beispiele
4. Gefährdungen durch Fernzugriff
5. Sicherheitsmaßnahmen zur Absicherung des Fernzugriffs
6. Fazit

1. Einleitung

Warum ist Fernzugriff heute so wichtig?

- Ausgangssituation
  - Verändertes Arbeitsverhalten - mobiler Arbeitsplatz - mobile Endgeräte
  - Verteilte Anwendungen
  - Zugriff von überall auf Unternehmensnetz und Ressourcen erwünscht
- Beispiel: Arbeiten auf der Baustelle - Zugriff auf Firmendaten
- Beispiel: Remote helfen
- Beispiel: Fernwartungs-App für das SHK-Handwerk
- Anforderungen:
  - Umfassender Zugriff aus der Ferne erwünscht
    - Auf Daten, IT-Systeme und Maschinen
  - Plattformübergreifender Zugriff gefordert
    - Mit den unterschiedlichsten mobilen Endgeräten
  - Von überall erwünscht
- Motivation: Hilft, Zeit und Kosten zu sparen

Fernzugriff - die **W**-Fragen

- **Wozu?**
  - Fernwartung, Fernadministration, Fernsteuerung, Fernüberwachung, Client-Server Anwendungen (z.B. „Baustellen-App“), Home Office, beim Kunden
- **Womit?**
  - Notebook, „mobiler Kleintierzoo“ (Smartphone, Tablet, Phablet), unterschiedliche Betriebssysteme (iOS, Windows, Android, etc.)
- **Worauf?**
  - Daten, IT-Systeme und Maschinen
- **Wer?**
  - Mitarbeiter, Chef, Dienstleister, Kunde, Wartungspersonal (intern, extern)
- **Wie?**
  - Unterschiedliche Lösungen für Fernzugriff vorhanden
  - Differenzierung erforderlich - welche Lösung eignet sich wofür?
  - Kategorisierung der zugegriffenen Geräte und Daten
  - Zusätzliche Sicherheitsmaßnahmen berücksichtigen

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

2. Lösungen für den Fernzugriff

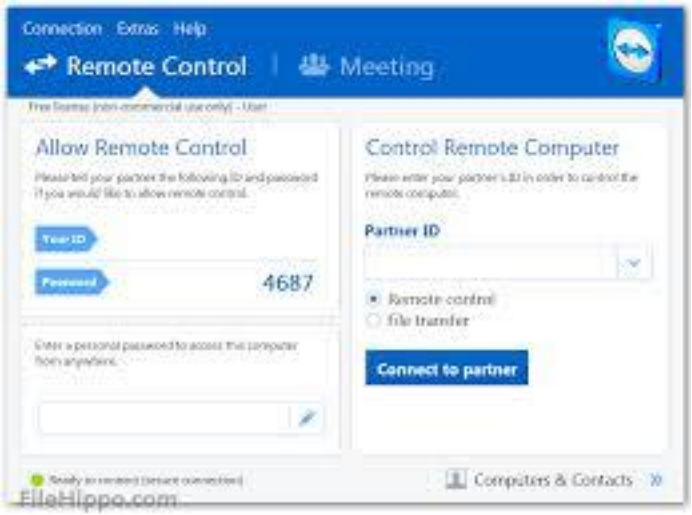
Lösungen für Fernzugriff im Überblick

- **Teamviewer:** das wohl bekannteste Werkzeug für Fernwartung und Onlinezusammenarbeit
- (Klassischer) **Fernzugriff über Portweiterleitung**
- **Fernzugriff über die Cloud**
- **Fernzugriff über MyCloud**
- **Fernzugriff über Virtual Private Network (VPN)**
- **Herstellerspezifische Lösungen**

Weitere, für das Handwerk weniger interessant:

- **Fernzugriff über Terminal-Service (TS) oder Virtual Desktop Infrastructure (VDI)**
- **SSH-Tunnel**

Teamviewer



Werbeslogan:

- Sicherheit für Remote-Zugriff und Remote-Support
- TeamViewer verbindet Menschen, Orte und Dinge rund um die Welt über die größte Bandbreite an Plattformen und Technologien.

Fernzugriff über Portweiterleitung

- engl.: *Portforwarding*, Alternativbezeichnungen: DNAT, Full NAT, PAT
- Prinzip:
  - Z. B.: Webserver läuft auf dem Gerät, auf das zugegriffen werden soll
  - Kommunikation über http- bzw. sicherer über https-Protokoll
  - Fernzugriff auf die Ressource mit Webbrowser über öffentliche IP und äußerer Portnummer, z.B.: http://212.30.8.7:4711
- Konfiguration:
  - Portweiterleitungsregel einrichten
    - Die Anfrage von Außen (über das Internet) wird auf das IT-System (die Maschine) im lokalen Netz weitergeleitet
    - Öffentliche IP / Port von außen → interne IP / Port des IP-Gerätes
    - Firewall-Regel erstellen
    - DynDNS einrichten, damit man sich die öffentliche IP nicht merken muss
  - In die Unternehmensfirewall muss dazu ein „Loch“ für den Zugriff von außen über das Internet gebohrt werden

Fernzugriff über Portweiterleitung

- Einige Anwendungsmöglichkeiten
  - Zugriff auf Webserver (IP-Kamera, KNX-Gateway, IP-Steckerleiste, ...)
  - Zugriff auf VNC-Server
  - Zugriff auf SSH-Server
  - Zugriff auf FTP-Server

- Anmerkungen:
  - Tipp: **DynDNS** sollte eingerichtet sein, wenn keine feste öffentliche IP vom Provider vergeben ist
  - Pro „Loch“ (Portweiterleitungsregel) ist nur der Zugriff auf einen Dienst auf dem IT-System möglich
  - Aktuell: Probleme mit speziellen Providern, DS-Lite,..., Provider muss auch IPv4-Adresse liefern (Dual Stack)

Vorteile – Fernzugriff über Portweiterleitung

- Einrichten einer Portweiterleitungsregel geht mittlerweile bei den meisten DSL-Router
- Wenig Netzwerkkenntnisse zum Einrichten der Portweiterleitung beim Einsatz gängiger DSL-Router, wie z. B. Fritz!Box, erforderlich
  - Portweiterleitungsregel einrichten
  - Firewallregel dazu („Loch in Unternehmensfirewall“) wird meist automatisch generiert

Nachteile - Fernzugriff über Portweiterleitung

- Das Gerät ist „frontal“ dem Internet ausgesetzt, ist direkt über das Internet erreichbar
- Zugegriffene Geräte sind meist nicht „gehärtet“
- Jeder, auch Hacker Joe kann versuchen, über den äußeren Port und die öffentliche IP auf die Ressource zuzugreifen
  - Es gibt bereits Suchportale für offene Ressourcen im Internet, z. B. https://shodan.io
- Die Daten werden bei http im Klartext (unverschlüsselt) über das Internet übertragen
- Pro Ressource ist jeweils eine eigene Portweiterleitungsregel erforderlich
- Probleme mit diversen Providern, die nur noch mit IPv6-Adressen im Internet arbeiten

Absicherung – Fernzugriff über Portweiterleitung

- Remotezugriff nur bei Bedarf aktivieren, ansonsten deaktivieren
- Äußeren Port in 5-stelligen Bereich legen
- Auf aktuelle Firmware des Gerätes, auf das zugegriffen werden soll, achten
- Falls möglich: Zur Kommunikation gesicherte Übertragung mit *https* statt *http* verwenden
- Standard-Accounts (Benutzername / Kennwort) ändern bzw. sperren
- Komplexe Kennwörter für die Anmeldung auf der Maschine verwenden
- Falls möglich, zusätzliches (Popup-)Anmeldefenster konfigurieren
- Gerät, auf das zugegriffen wird, in separates Netzsegment (DMZ) auslagern
- Risikobewertung: bei IP-Kamera sicherlich geringeres Risiko, als bei bei einer Heizungssteuerung

- **Wichtiger Hinweis!** Selbst AVM empfiehlt aus Sicherheitsgründen die Deaktivierung der Fernadministration bei der Fritz!Box

Cloud-basierter Fernzugriff ←voll im Trend

- ***„Teamviewer-Ansatz“*** (Copyright by Werner)
- Verbindungsaufbau über Gateway (Herstellerplattform) im Internet
- Zugriff des Anwenders über eine App (Anwendung)
- Registrierung des Anwenders und des Gerätes (zuzugreifende Ressource) auf Herstellerplattform (Gateway)
- Der Einsatz dieser Produkte setzt einen Account beim Hersteller voraus
- Achtung! Ich muss dem Anbieter dieser Sicherheitslösung (Hersteller) vertrauen
- Auf Gatewaystandort „Made in Germany“ achten → mindestens EU-Datenschutzregeln
- Problem: „Sie müssen **nur** dem Hersteller (Cloud-Anbieter) vertrauen“

- Produktbeispiel: Phoenix Contact: *Innominate mGuard Secure Cloud public*

Managementplattform mGuard Secure Cloud public

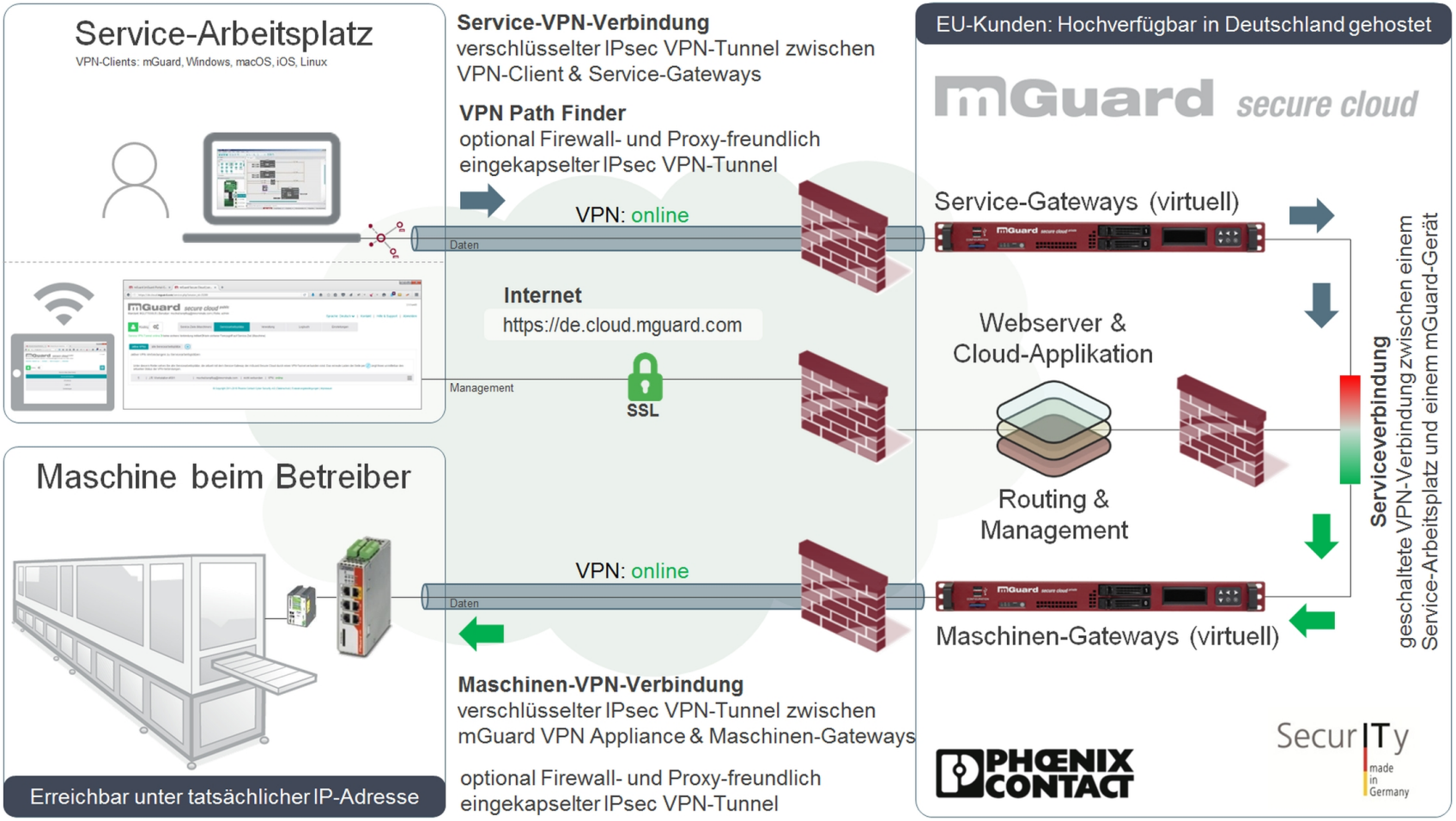


Bild: Phoenix Contact

Vorteile – Cloud-basierter Fernzugriff

- **Auf beiden Seiten keine Firewallkonfiguration erforderlich**
  - Kein „Löcher bohren in der Firewall“ auf Client- und Host-Seite
- **Keine Sicherheitsbedenken wie bei der Portweiterleitung**
  - Maschine steht nicht direkt im Internet
- **Keine Kenntnisse über VPN erforderlich**

Nachteile – Cloud-basierter Fernzugriff

- **Vertrauen auf die Sicherheit des Gateways und die Seriösität des Anbieters erforderlich**
  - Der Hersteller hat Zugriff auf meine Daten
    - Ist die Verschlüsselungslösung auch sicher?
    - Können die Geheimdienste mitlesen?
    - Wo befindet sich das Gateway (GeoIP)?
    - deutscher oder zumindest europäischer Anbieter?
- **Gefahr, dass hauseigene Daten auf fremden Servern landen**
  - Prinzipiell kann der Betreiber des zentralen Servers (Gateways) auf die zwischen Client und Host ausgetauschten Daten zugreifen
  - dieser Umstand sollte gerade bei Fernwartung in datenschutzrechtlich sensiblen Bereichen berücksichtigt werden
- Stellt **höhere Anforderungen an Sicherheit und Datenschutz**

Fernzugriff über MyCloud

- Dieser Ansatz wird seit Snowden immer interessanter
- „Cloud-basiertes Fernwartungsportal in eigener Cloud“
  - ermöglicht einfachen und sicheren Fernzugriff
  - ganz ohne aufwendige VPN-Konfiguration
  - ansonsten identisches Prinzip zur cloudbasierten Variante
- **Das zentrale Gateway gehört zu meiner Unternehmens-IT.** Daraus folgt:
  - Ich bin für die Datensicherheit selbst verantwortlich
  - Ich muss keinem Hersteller wie z. B. bei „Teamviewer“ vertrauen
  - Standort: entweder in meinem Unternehmen oder angemietet beim Hoster

- Beispiellösung: Siemens AG, *SINEMA Remote Connect*

Siemens AG, SINEMA Remote Connect

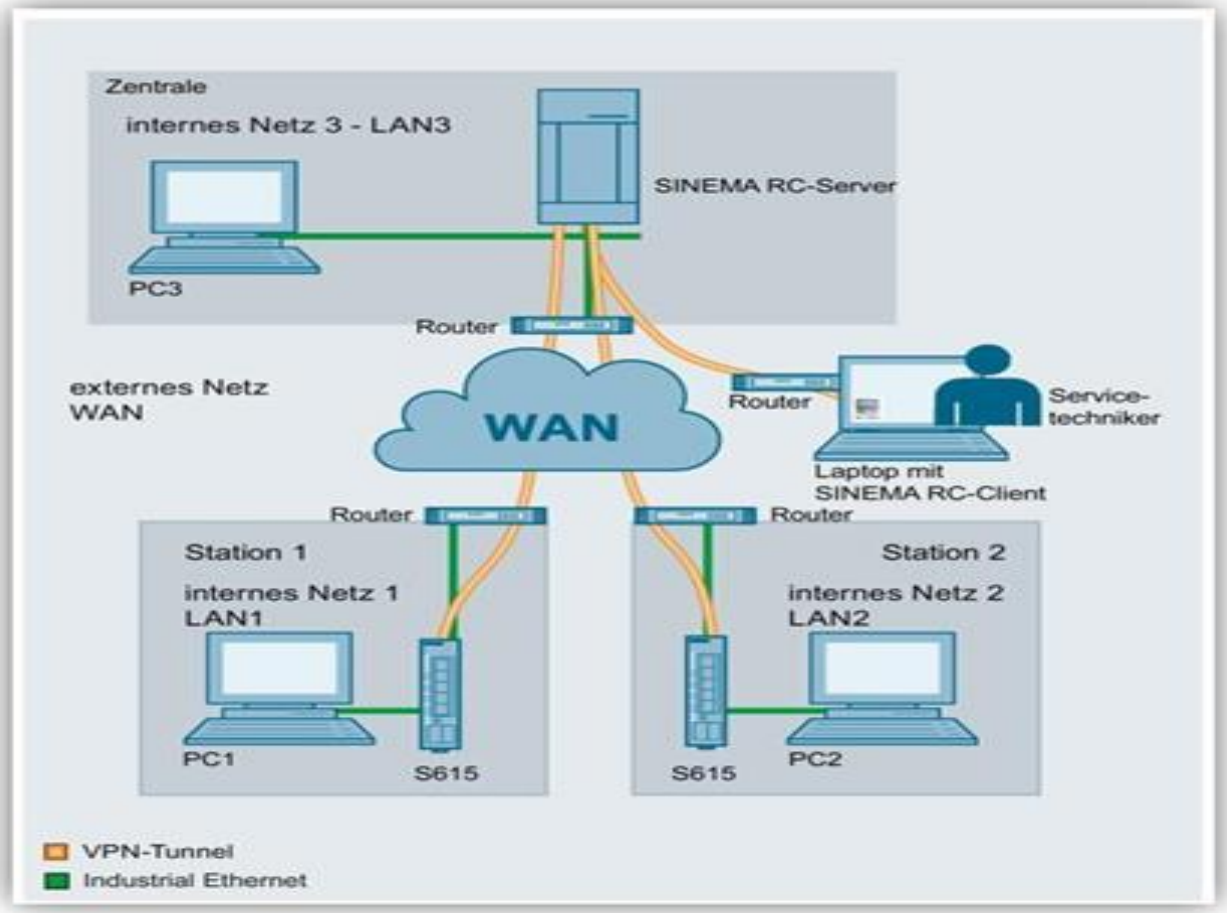


Bild: Siemens AG

Vorteile – Fernzugriff über MyCloud

- Ich muss niemanden mehr vertrauen und bin selbst für die Sicherheit verantwortlich
- Ansonsten die gleichen Vorteile wie bei der Cloud-basierten Lösung

Nachteile – Fernzugriff über MyCloud

- Technische Kenntnisse zur sicheren Administration des Gateways erforderlich
- Habe ich genügend Kenntnisse?

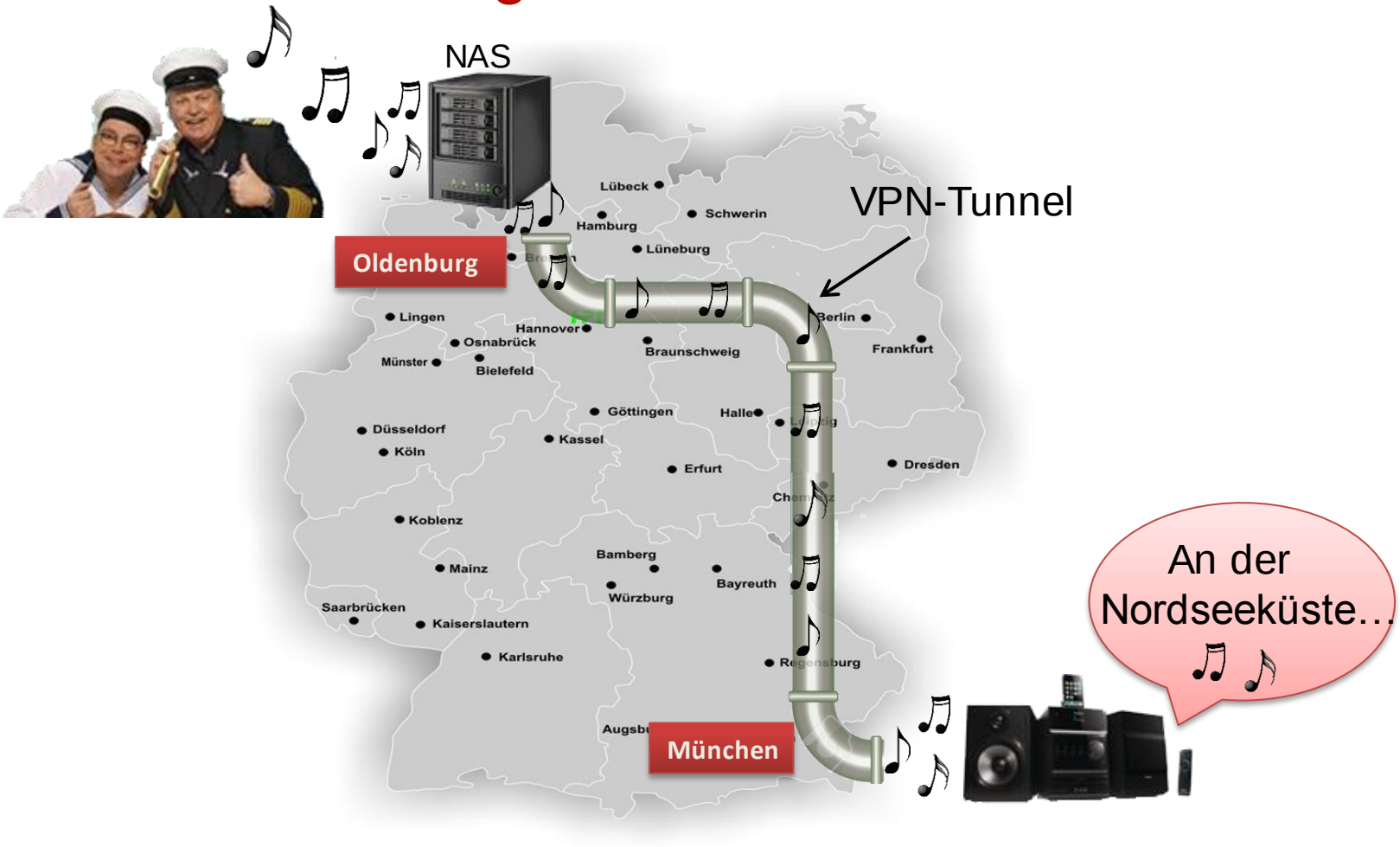
Fernzugriff über Virtual Private Network (VPN)

- **Ermöglicht sichere Anbindung an das Unternehmensnetzwerk** über ein unsicheres Netzwerk, wie dem Internet, durch Aufbau eines sog. VPN-Tunnels

- **VPN-Tunnel** bietet einen **gesicherten Kommunikationskanal über ein unsicheres Netzwerk** hinweg
  - Das Mitlesen der Kommunikation ist nicht möglich
  - Die Kommunikation zwischen zwei Teilnehmern wird verschlüsselt

- **VPN wirkt wie lokales Arbeiten im Firmennetz**

Klaus & Klaus sicher „getunnelt“



Sicherheit durch Einsatz von VPN

- **Sicherheit hängt ab ...**
  - vom gewählten VPN-Verfahren,
  - von der Authentifizierungsmethode,
  - von den verwendeten „Schlüsseln“ (Schlüsselmaterial)
  - von der Schlüssellänge

- **Anmerkungen zu VPN**:
  - Komplexes Thema, erfordert tiefergehende theoretische Kenntnisse für die Inbetriebnahme und Fehlersuche.
  - Dennoch, der „Tunnelbau“ und Produktlösungen werden immer einfacher!

- **Tipp**: VPN bei Surfen über Hotspot verwenden
  - VPN-Technik sollte auch bei Netzzugang über öffentliche WLANs (Hotspots) aus Sicherheitsgründen verwendet werden

VPN - Verfahren

- IPSec
- SSL-VPN (OpenVPN)
  .....
- L2TP over IPSec
- PPTP ← nicht verwenden, da unsicher

- Anmerkung:
  VPN-Server und VPN-Client müssen das selbe Verfahren beherrschen.
  Dennoch sind bei IPSec Inkompatibilitäten nicht ausgeschlossen

Vorteile – Fernzugriff über VPN

- Bietet sicheren Fernzugriff auf alle möglichen Ressourcen über das Internet
- Ermöglicht arbeiten wie im lokalen Netzwerk
- die Universallösung
  - Nach Aufbau des VPN-Tunnels kann ich auf sämtliche Ressourcen im internen Netz zugreifen
  - Sämtliche Protokolle (HTTP, HTTPS, SMB/CIFS, ...) können durch den Tunnel transportiert werden
  - Einschränkungen („Tunnelverkehr“) über die Unternehmensfirewall regeln
- Trotz Komplexität des Themas werden die angebotenen Lösungen für den Anwender immer einfacher

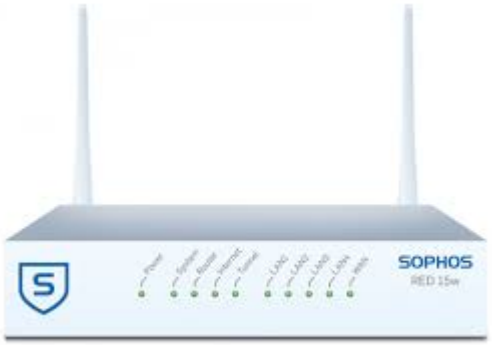
- Anmerkung: auch Cloud-basierte Lösungen setzen VPN ein

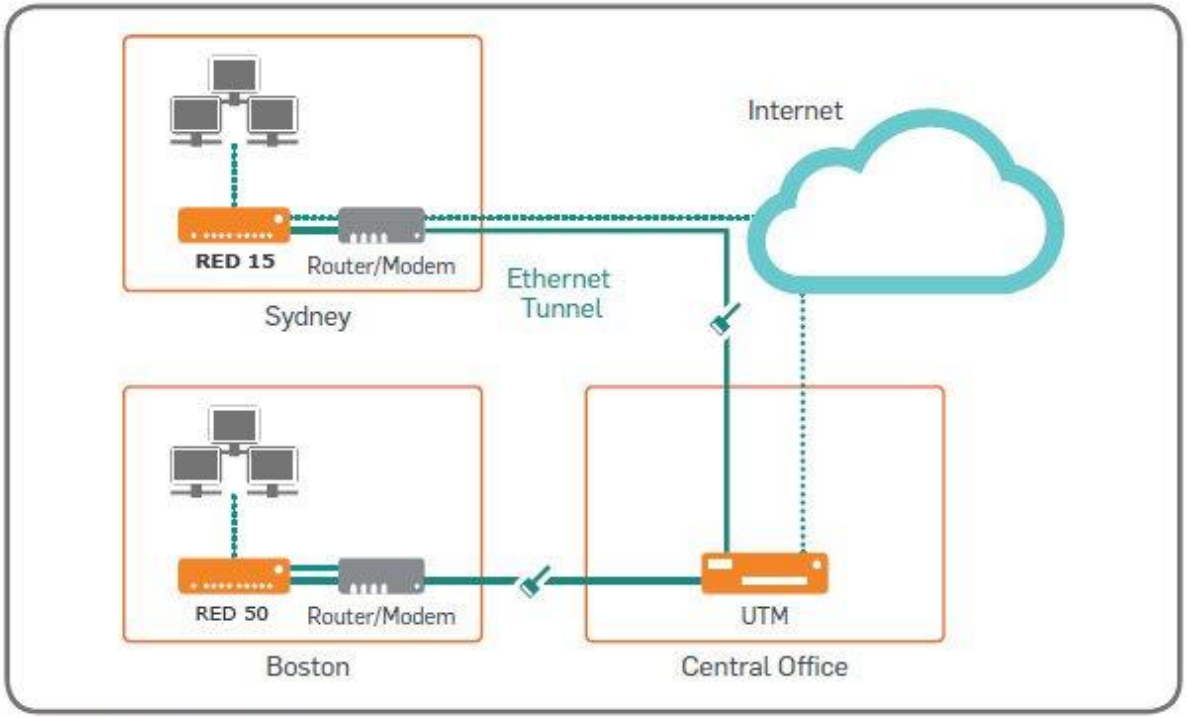
Nachteile – Fernzugriff über VPN

- Sehr komplexes Thema
- VPN ist nicht VPN - Unterschiedliche Verfahren, auch gleiche Verfahren teilweise zueinander inkompatibel
- VPN heißt nicht automatisch sicher
- VPN und Firewall
  - Eventuell keine VPN-Verbindung aus Hotel, beim Kunden, etc. möglich
- Bewertung der Sicherheit überfordert den Laien
- Unter Umständen aufwendige VPN-Konfiguration

Fernzugriff mit herstellerspezifischen Lösungen

- Beispiel: Sophos Remote Ethernet Device (RED)





Deployment scenario of Sophos RED

Quelle: Sophos

Vorteile herstellerspezifischer Lösungen

- Teilweise einfach zu implementieren
- Sichere Verfahren
- Preislich interessant
- Remote Access - und Standortvernetzungs-Lösungen möglich

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

3. Welcher Lösungsansatz eignet sich für welches Problem, einige Beispiele...

Kategorisierung der Ressourcen (Geräte und Daten)

- Typ 1: **Fernzugriff auf Windows-Rechner**
  - PC oder Notebook
  - Fernbedienung des Windows-Rechners erwünscht
- Typ 2: **Fernzugriff auf Geräte mit Weboberfläche**
  - Auf diesen Systemen läuft ein Webserver
  - Der Zugriff erfolgt über einen Webbrowser durch Eingabe der IP-Adresse und Port-Nummer, z. B. https://192.168.1.8:5003
  - Über die Weboberfläche wird das Gerät konfiguriert und verwaltet
  - Beispiele: Fritz!Box, IP-Kamera, Synology-NAS, Digitalstrom-Server
- Typ 3: **Fernzugriff auf „mobiler Kleintierzoo“**
  - Hier läuft kein Webserver bzw. spezieller Serverdienst für Remote Control
  - Zugriff zu Wartungs- und Unterstützungszwecken

Kategorisierung der Ressourcen

- Typ 4: **Fernzugriff auf sonstige Geräte**
  - Hier läuft kein Webserver bzw. spezieller Serverdienst für Remote Control
  - Zugriff für Bedienung, Wartung und Konfiguration
  - Beispiel: Bedienung Comfort Panel
- Typ 5: **Fernzugriff auf Unternehmensdaten**
  - z. B. freigegebene Ordner auf NAS (Netzwerkfestplatte) / Windows-Share
  - allgemein Datenserver (Fileserver)
  - SMB/CIFS-Protokoll
- Typ 6: **Fernzugriff auf das Unternehmensnetzwerk**
  - Ermöglicht den Zugriff auf alle Ressourcen im Netzwerk

Fernzugriffslösung für Kategorie

Typ	Kategorie	Fernzugriffslösung
1	Fernzugriff auf Windows-Rechner	Viele Möglichkeiten: – Erste Wahl → Teamviewer – RDP-Protokoll → Remote Desktop (Bordmittel) – VNC-Protokoll → VNC-Server und VNC-Client erforderlich – --> Zusätzlich dann die Portweiterleitung – Windows-Fernsteuerung mit heise-Konzept http://www.heise.de/netze/tools/fernwartung
2	Fernzugriff auf Gerät mit Weboberfläche	a) Portweiterleitung und Kommunikation über http-Protokoll b) Portweiterleitung und Kommunikation über https **c) VPN** d) opt. cloudbasierte bzw. MyCloudbasierte Lösung

Fernzugriffslösung für Kategorie

Typ	Kategorie	Fernzugriffslösung
3	Fernzugriff auf „mobiler Kleintierzoo“	Ideal mit Teamviewer, also Cloudbasierter Ansatz
4	Fernzugriff auf sonstige Geräte	z.B. Comfort Panel a) VNC-Protokoll, VNC-Server auf Panel installieren und konfigurieren, VNC-Client auf Tablet, Smartphone oder Notebook b) Danach Portweiterleitung einrichten oder noch besser c) Über **VPN**-Tunnel d) Herstellerspezifische Lösung

Fernzugriffslösung für Kategorie

Typ	Kategorie	Fernzugriffslösung
5	Fernzugriff auf Unternehmensdaten	Bitte nur über **VPN**-Tunnel!!
6	Fernzugriff auf das Unternehmensnetzwerk	Remote Access über **VPN** (host to site)

4. Gefährdungen durch Fernzugriff

Die Top-10-Bedrohungen 2016 laut BSI

1. Social Engineering und Phishing
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Infektion mit Schadsoftware über Internet und Intranet
4. **Einbruch über Fernwartungszugänge ← 4. Platz**
5. Menschliches Fehlverhalten und Sabotage
6. Internet-verbundene Steuerungskomponenten
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Extranet und Cloud-Komponenten
9. (D)Dos-Angriffe
10. Kompromittierung von Smartphones im Produktionsumfeld

Anmerkung: Angaben beziehen sich auf industrielles Umfeld

Gefährdungen durch Fernzugriff

- Allgemein:
  - Fernzugriff macht IT-Systeme anfällig, erst recht, wenn sie via Internet stattfindet
- **Sabotage**
  - Ausfall oder Einschränkung der Funktionsfähigkeit wichtiger Systeme
  - Verfälschung von Daten
- **Verlust von Daten = Datenklau**
- **Spionage**
  - Verlust der Vertraulichkeit wichtiger Unternehmensdaten
  - Kundendaten und andere sensible Unternehmensdaten sind ein häufiges Ziel von Cyberattacken
    - Forschungs- und Entwicklungsergebnisse, Strategiepapiere, Einzelheiten von Verträgen, Angebote und Preiskalkulationen, die Korrespondenz mit Geschäftspartnern, Informationen über die Besonderheiten der Unternehmens-IT, Zugangsdaten

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

5. Sicherheitsmaßnahmen zur Absicherung des Fernzugriffs

Unkoordinierte „Insellösungen“ vermeiden

Ein ganzheitliches Konzept ist erforderlich!

Wichtigster Faktor und gleichzeitig größte Schwachstelle ist der Mensch.

Erfordert organisatorische, infrastrukturelle, personelle, technische und Notfall-Maßnahmen.

Das schwächste Glied in der Kette bestimmt die IT-Sicherheit.

Bedenken Sie jedoch:

„Organisatorische Mängel lassen sich nicht mit Technik erschlagen“

Allgemeine Maßnahmen (Regeln)

- **Bei Fernwartung, Fernadministration, etc.**
  - Fernzugriff muss von Innen initiiert werden
  - Fernzugänge nur für die Zeit der Wartung öffnen
  - Fernwartung protokollieren
  - Nur einen Nutzer pro Account verwenden
- **Nicht mehr benötigte Zugänge sperren**
- Anlagenbetreiber sollten die **Standardpasswörter des Herstellers ändern**

Organisatorische Maßnahmen

- **Risikoanalyse**
- **Richtlinien für Diebstahl oder Verlust** des mobilen Endgeräts
- **Maßnahmen, wenn ein Mitarbeiter ausscheidet**
- **Regelungen Fernzugriff für Mitarbeiter**
- **Regelungen Fernwartung durch Dritte (Externe)**
- **Datenklassifizierung**
- **Sensibilisierung der Mitarbeiter**

Technische Maßnahmen

- **Sichere Netzwerkarchitektur**
  - **Netztrennung in Sicherheitszonen**
    - Min. 3: **internes Netz** (= vertrauenswürdig), demilitarisierte Zone (**DMZ =** für Dienste und Anwendungen, die aus dem Internet erreichbar sind), **Außenanbindungen** (= **Internetanbindung** sowie andere nicht vertrauenswürdige Netze)
    - Zonenübergänge müssen abgesichert und kontrolliert werden
  - **Segmentierung der Netzwerke**
    - Client-Server Segmentierung
    - Endgeräte-Segmentierung im internen Netz
    - DMZ-Segmentierung
      - Zugriffspunkte für die Fernwartung gehören in eine von anderen Netzen getrennte demilitarisierte Zone (**DMZ**)
    - Trennung Gerätegruppen bzw. Mandanten auf Netzwerkebene

Technische Maßnahmen

- **Grundlegende Absicherung des Internetzugangs**
  - Sicherheitsgateway (Unternehmensfirewall) erforderlich
- **Absicherung der Kommunikation durch Firewalls**
  - regelt, dass Servicemitarbeiter nur diejenigen Komponenten erreichen sollen, die sie für ihre Arbeit benötigen
- **Netzzugangskontrolle**

Anforderungen an mobile Endgeräte

- **Zugangsschutz**
- **Erfolgreiche Authentifizierung** erforderlich
  - gegenüber Endgerät und dem Unternehmensnetz
- **Verschlüsselung der Daten**
  - Sicherheit und Diebstahlschutz
- **Regelmäßige Sicherung der Daten** auf dem mobilen Endgerät
  - Wo? Im Unternehmensnetzwerk
- **Schutz der Vertraulichkeit muss gewährleistet sein**

- Weiterhin**: Bei Diebstahl oder Verlust**
  - Fernzugriff des betroffenen Benutzers / Gerätes durch das Unternehmen kurzfristig sperren

Fernzugriffsverbindung

- **Absicherung eingehender Kommunikation vom Internet in das interne Netz**
  - Nur von vertrauenswürdigen IT-Systemen via Internet
  - Gegenstelle (VPN-Gateway) steht in DMZ
  - **Sichere Authentisierungsverfahren** verwenden.
  - **Sicher verschlüsseln** (per SSH oder VPN-Tunnel)
    - Ziel: Kommunikationsverbindung zwischen Endgerät und Unternehmensnetz vor unbefugtem Mitlesen schützen
    - Einsatz eines kryptografisch gesicherten VPN
    - AES mit Schlüssellänge von mindestens 192 Bit

Anmerkungen:

- Die Liste der Maßnahmen ist nicht vollständig
- Die aufgeführten Maßnahmen können Gefährdungen nicht völlig ausschließen, führen aber zu einem akzeptablen Restrisiko

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

6. Fazit

Zusammenfassung und Bewertung

- **Fernwartungs- bzw. Fernzugriffszugänge auf Daten, IT-Systeme und Maschinen lassen sich sicher betreiben**
- Für die Sicherheit ist alles vorhanden: **Sichere Technologien** und **Produkte**
- **VPN** bietet sicheren Fernzugriff auf alle möglichen Ressourcen, ist aber komplex
- Im Trend liegen **Cloud-basierte Lösungen**, die größtenteils VPN-Technik einsetzen
- **Voraussetzungen**, damit „Sicherer Fernzugriff“ umgesetzt wird:
  - die Fragen der Sicherheit in das Unternehmen integrieren
  - Experten für die Lösungen beauftragen
  - Richtige Produktauswahl
  - Das richtige Schlüsselmaterial und eine ausreichende Schlüssellänge für die Verschlüsselung wählen

Vielen Dank für Ihre Aufmerksamkeit