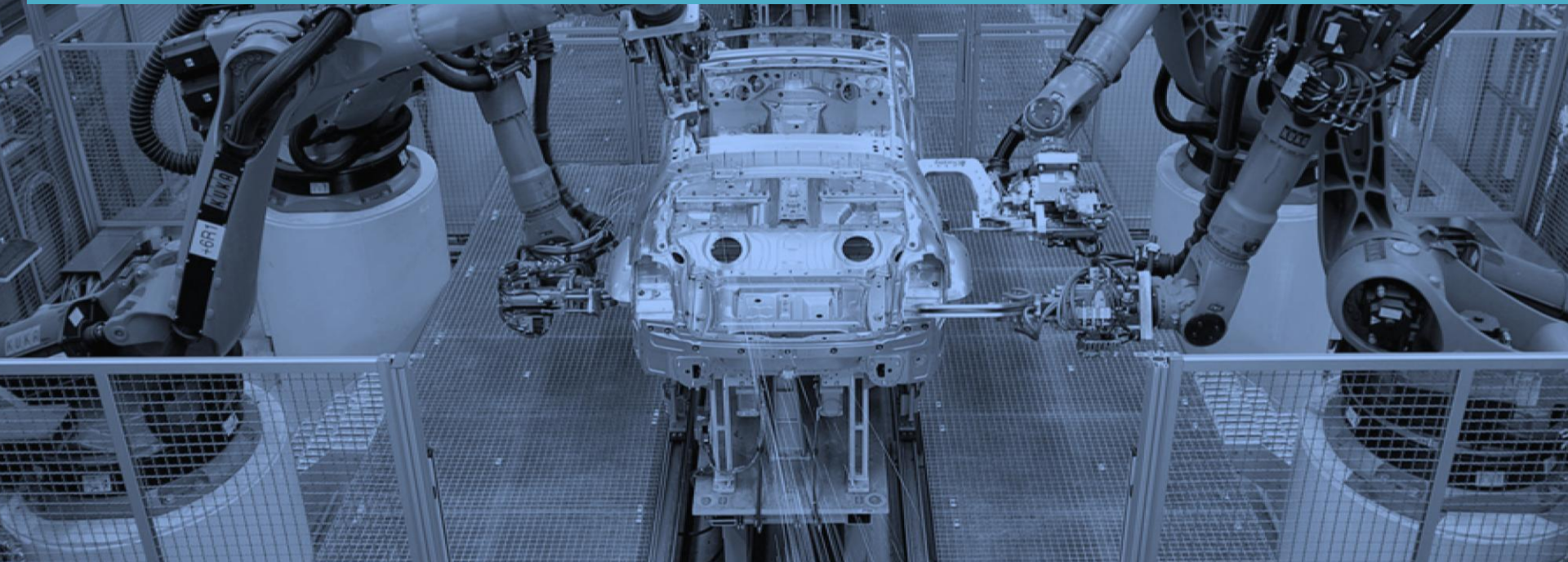


Stuxnet zum Frühstück Industrielle Netzwerksicherheit 2.0

Stuttgart und München



Gefahrenpotentiale

Gefahrenbereich	Bedeutung heute Rang	Prognose Rang	Schäden	
			Rang	ja, bei
Irrtum und Nachlässigkeit eigener Mitarbeiter	1	2	1	49%
Malware (Viren, Würmer, Trojanische Pferde)	2	1	4	35%
Software-Mängel/-Defekte	3	5	2	46%
Hardware-Mängel/-Defekte	4	6	3	45%
unbefugte Kenntnissnahme, Informationsdiebstahl, Wirtschaftsspionage	5	3	7	12%
unbeabsichtigte Fehler von Externen	6	7	5	30%
Hacking (Vandalismus, Probing, Missbrauch, ...)	7	4	8	12%
höhere Gewalt (Feuer, Wasser, ...)	10	11	9	12%
Sabotage (inkl. DoS)	11	10	11	10%

Ist die totale IT-Sicherheit möglich ?

Verfügbarkeit

Sicherheit

Erreichbarkeit

Authentifizierung

Performance

Authorisierung

Einfachheit

Accounting

Managebarkeit

Integrität

Vielfältigkeit

Vertraulichkeit



Ist IT-Sicherheit ohne technische Massnahmen möglich ?

Menschen

Maschinen

Weisungen

Firewall

Checklisten

IPS/IDS

Richtlinien

NAC

Standards

SecureMail

Vorschriften

AntiVirus/SPAM

Ausführungsbestimmungen

VPN



Achtung !

Bezüglich Sicherheit gibt es grundsätzlich keine Unterschiede zwischen «grossen» und «kleinen» Netzwerken !

Das generelle Sicherheitsbedürfnis und somit die Komplexität der gewählten Massnahmen ist von Netzwerk zu Netzwerk unterschiedlich.

Sicherheits- Strategie



Die Strategie legt zukünftige Ziele der IT sowie die lang- und mittelfristigen Handlungsvorgaben zu ihrer Erreichung innerhalb einer Planungsperiode fest

- Risikoanalyse, Risikokategorien bilden, geeignete & zweckmässige Massnahmen treffen
- Sicherheitsleitlinie (Security Police) erstellen

Sicherheitsrichtlinie (Security Policy)

IT- Systemen, insbesondere von IT-gestützten Geschäftsprozessen, muss insgesamt vermieden beziehungsweise kurzfristig kompensiert werden können. Der Schutz aller IT-gestützten Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung ist von strategischer Bedeutung für unser Unternehmen.

Die unten aufgeführten Ziele und Massnahmen bezwecken, sind aber nicht allein darauf beschränkt, die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sowie die Rechenschaftspflicht des Einzelnen hinsichtlich der Nutzung von Informationen zu regeln und sicherzustellen.

2.0 Übergreifende Ziele

- 2.1 Unsere Daten und unsere IT- Systeme in allen technikabhängigen und kaufmännischen Bereichen werden in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstandszeiten toleriert werden können. Fehlfunktionen und Unregelmässigkeiten in Daten und IT-Systemen sind nur in geringstem Umfang und nur in konkreten Ausnahmefällen akzeptabel (Integrität). Die Anforderungen an die Vertraulichkeit der Daten haben ein normales, an Gesetzeskonformitäten orientiertes Niveau. Einzig für Daten der Geschäftsleitung und für gewisse projektspezifische Daten gelten maximale Anforderungen an die Vertraulichkeit.
- 2.2 IT- Sicherheitsmassnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT- Systemen stehen. Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden.
- 2.3 Alle Mitarbeiter des Unternehmens halten die einschlägigen Gesetze wie das Strafgesetzbuch, das Betriebsverfassungsgesetz, das Handelsgesetzbuch, das Sozialgesetzbuch, die Gesetze zur Regelung zum Datenschutz und das Gesetz gegen den unlauteren Wettbewerb sowie alle vertraglichen Regelungen ein. Negative finanzielle und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstösse sind zu vermeiden.

Risikopotential Mensch

Das schwächste Glied in der Kette: Risikofaktor Mensch !

- Social Engineering
- Human Firewall



Materialwahl

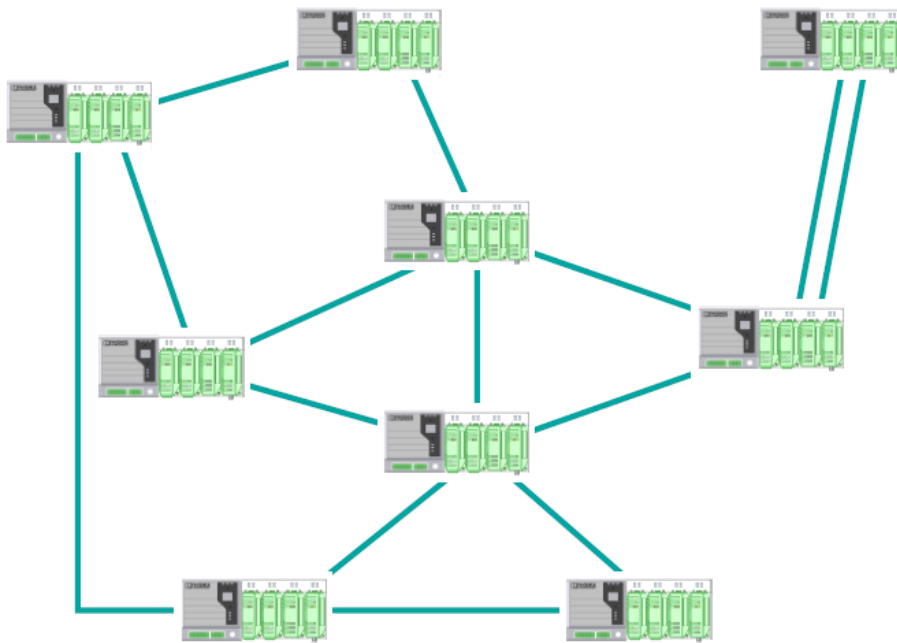
Sicherheitsrelevante Planung, Konzeption, Realisierung & Unterhalt
Nur den Anforderungen entsprechende aktive und passive Komponenten einsetzen !



Wieso Industriekomponenten ?

	Büro- Netzwerk	Industrie- Netzwerk
Installation	<ul style="list-style-type: none"> • Feste Grund-installation im Gebäude (UKV) • Variabler Geräteanschluss an Standardarbeitsplätzen • Überwiegend sternförmige Verkabelung 	<ul style="list-style-type: none"> • Anlageabhängige Verkabelung und Kabelführung • Feldkonfektionierbare Steckverbinder bis IP 67 • Redundante Verkabelung, häufig Ringstrukturen
Daten	<ul style="list-style-type: none"> • Grosse Datenpakete • Mittlere Netzverfügbarkeit (STP/RSTP) • Hauptsächlich azyklische Datenübertragung • Kein Echtzeitverhalten notwendig 	<ul style="list-style-type: none"> • Kleine Datenpakete • Sehr hohe Netzwerkverfügbarkeit (MRP) • Hauptsächlich zyklische Datenübertragung • Echtzeitverhalten z.T. notwendig
Umwelt	<ul style="list-style-type: none"> • Normaler Temperaturbereich • Wenig Staub, Feuchtigkeit und Erschütterungen • Kaum mechanische und chemische Belastungen • Geringe EMV-Belastung 	<ul style="list-style-type: none"> • Erweiterter Temperaturbereich • Staub, Feuchtigkeit und Erschütterungen möglich • Gefahr durch mechanische Beschädigung oder chemische Belastung • Hohe EMV-Belastung

Topologie: Spanning Tree Protokoll



Medienredundanz

Auflösung von Schleifen im Netzwerk

Beliebig vermaschte
Netzwerkstrukturen möglich

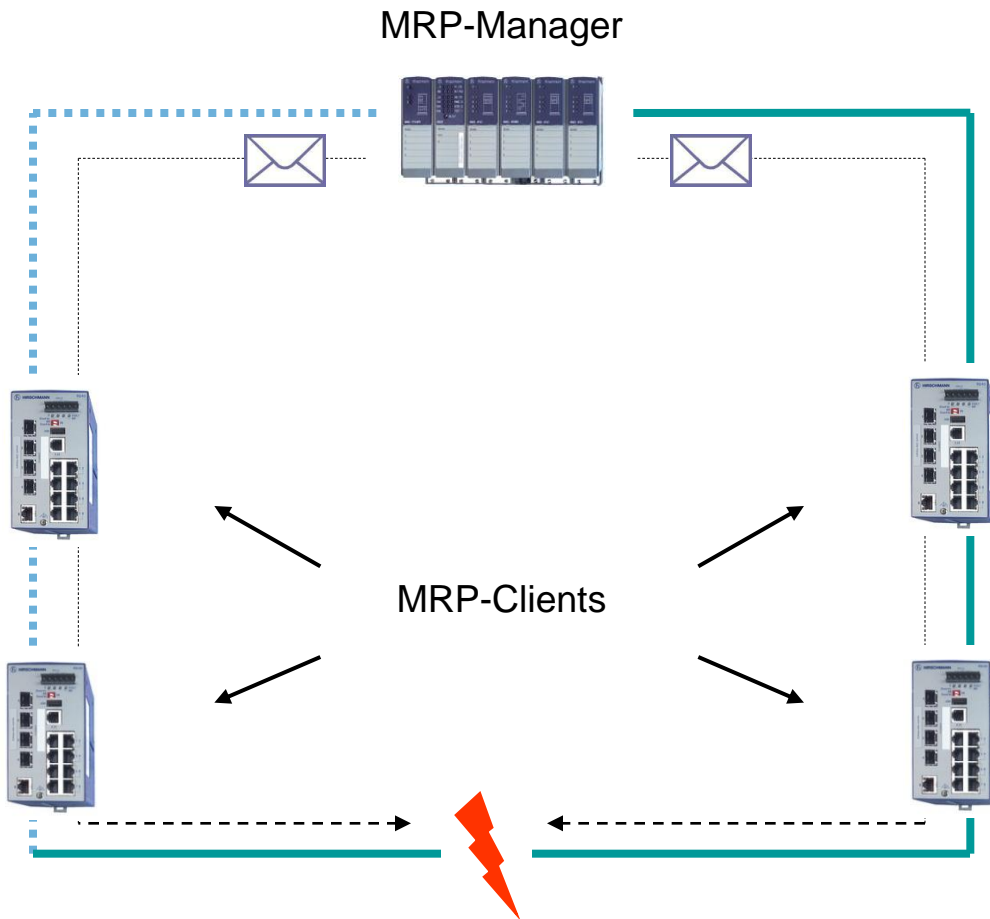
Erzeugung einer logischen
Baumstruktur

Reduzierung der Umschaltzeit durch
RSTP

Umschaltzeiten (abhängig von der
Netzwerkgrösse, STP: 30 - 90 s, RSTP:
< 2 s bis max. 7s)

Standards: IEEE 802.1D (STP); IEEE
802.1W (RSTP)

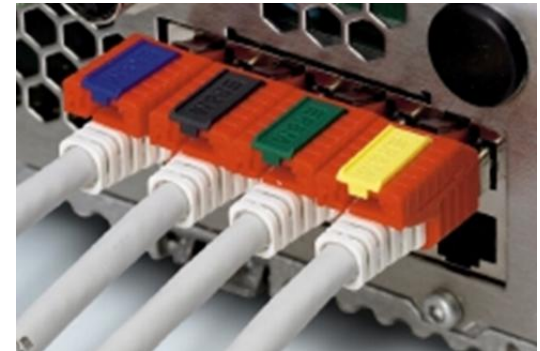
Topologie: Media Redundanz Protokoll



- Standardisiertes Medienredundanzprotokoll
- Hochverfügbare Netzwerke
- geeignet für kritische Automatisierungsanwendungen
- Keine vermaschten Topologien
- Weniger komplex als RSTP
- Reine Ringstrukturen
- Umschaltzeiten: < 200 ms

Layer 1: Bitübertragungsschicht

Schutz gegen irrtümliches, unbeabsichtigtes und/oder unautorisiertes Lösen einer Verbindung



Layer 1: Bitübertragungsschicht

Schutz gegen irrtümliches und/oder unbeabsichtigtes, unautorisiertes Erstellen einer Verbindung.

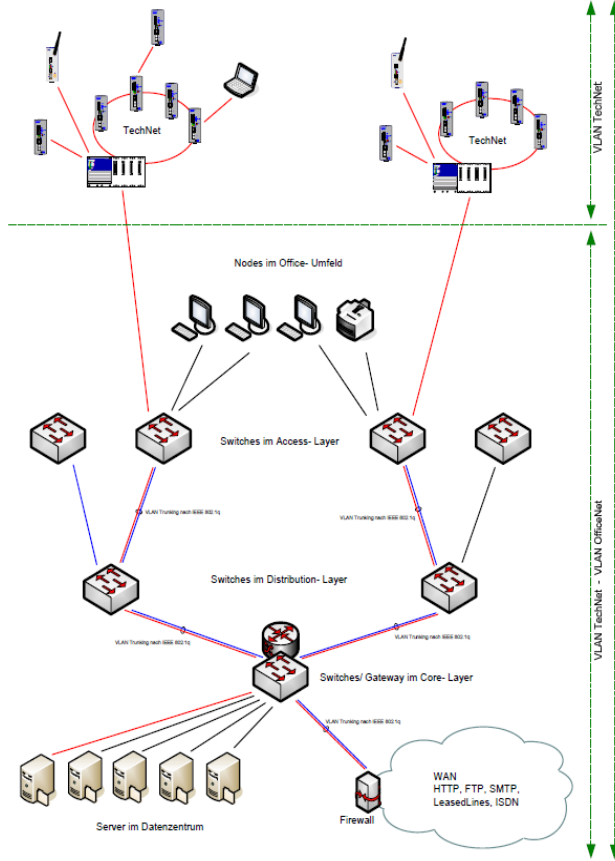
Modul	Port	Name	Port an	Verbindungsfehler weitermelden	Automatische Konfiguration	Manuelle Konfiguration	Link/ Aktuelle Betriebsart	Manuelles Cable-Crossing (Auto. Konfig. aus)	Flusskontrolle
1	1		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	100 Mbit/s FDX	unsupported	<input checked="" type="checkbox"/>
1	2		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>
1	3		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>
1	4		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>
1	5		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>
1	6		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>
1	7		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>
1	8		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>

Modul	Port	Port Status	Erlaubte MAC-Adressen	Aktuelle MAC-Adresse	Erlaubte IP-Adressen	Aktion
1	1	enabled		00:00:00:00:00:00		portDisable
1	2	enabled		00:00:00:00:00:00		portDisable
1	3	enabled		00:00:00:00:00:00		portDisable
1	4	enabled		00:00:00:00:00:00		portDisable
1	5	enabled		00:00:00:00:00:00		none
1	6	enabled		00:00:00:00:00:00		none
1	7	enabled		00:00:00:00:00:00		none
1	8	enabled		00:00:00:00:00:00		none

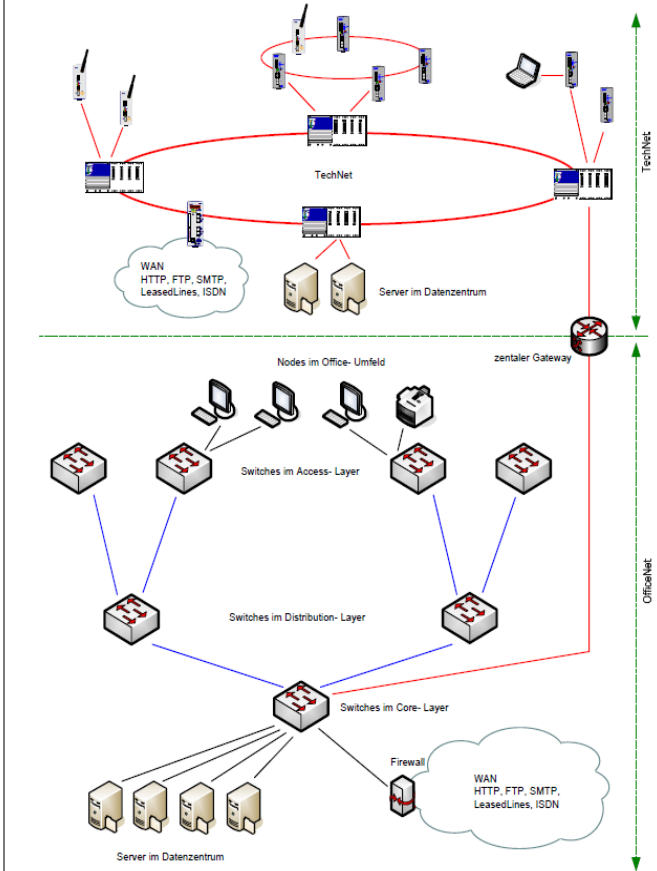
Layer 2: Sicherungsschicht

Logische Gruppierung von Netzwerkgeräten oder Benutzer, die nicht auf ein physikalisches Segment beschränkt ist.

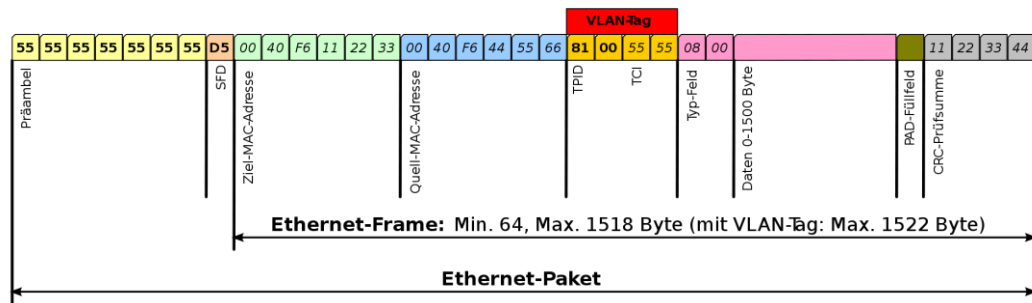
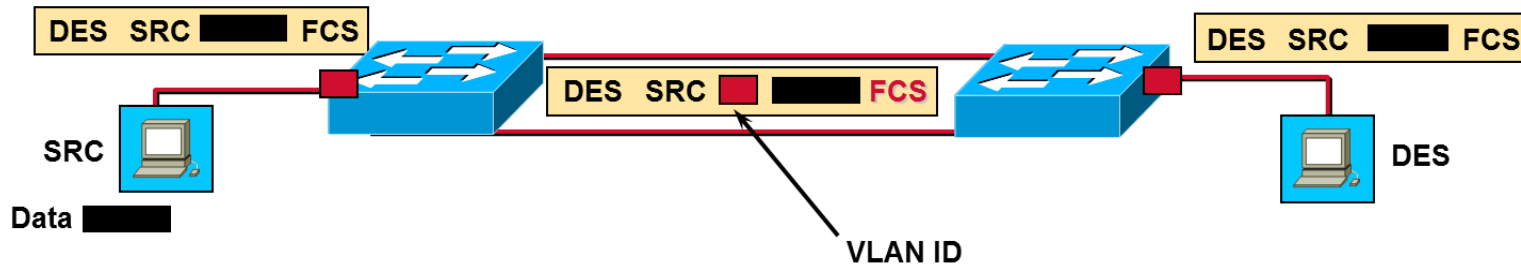
Lösungsansatz 1



Lösungsansatz 2



Layer 2: Sicherungsschicht



Technische Umsetzung eines VLAN-Konzepts

Layer 3: Vermittlungsschicht



Router transportiert Datenpakete aufgrund von eindeutigen Anweisungen von einem Netzwerk zum andern (Layer 3, bzw. IP-Adressen) und blockiert Broadcasts.

Layer 4/5: Transportschicht

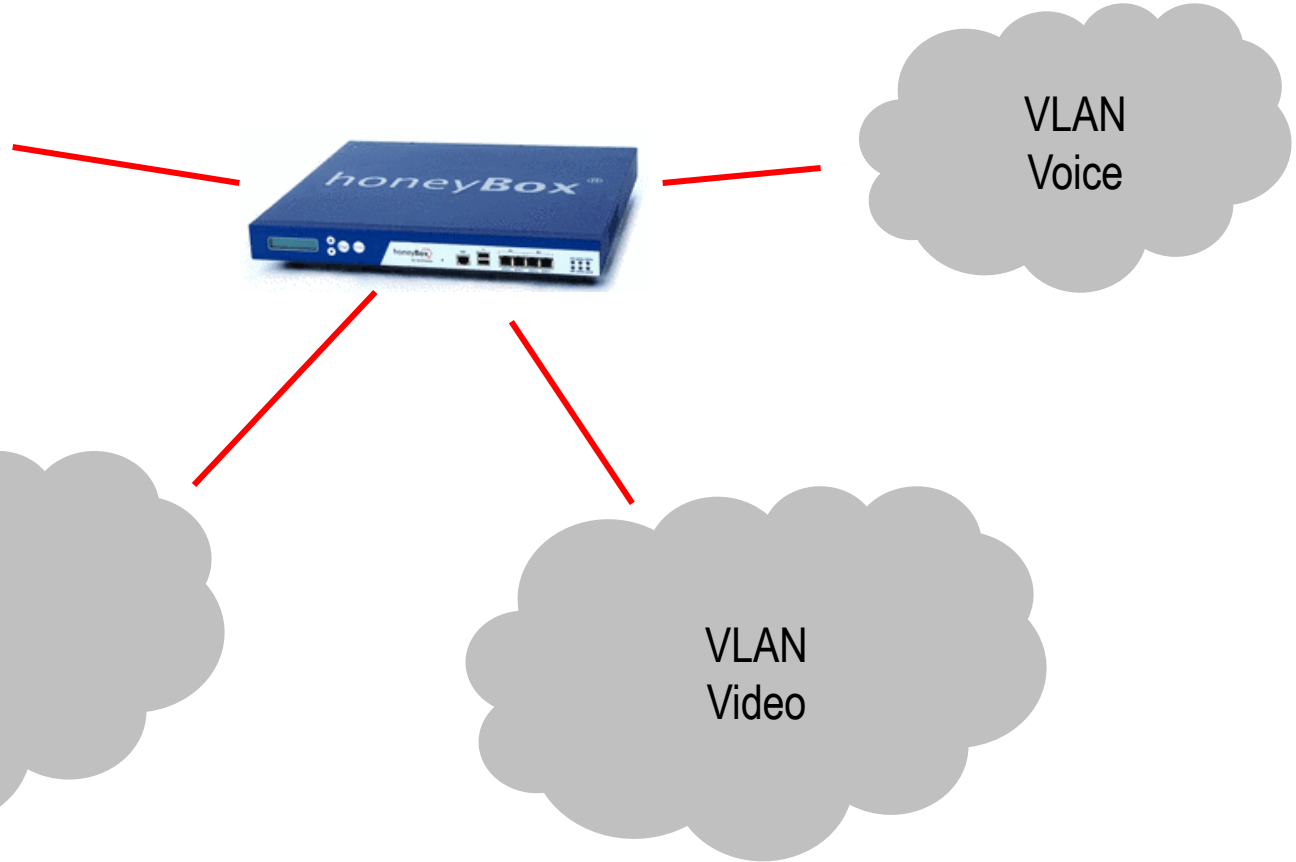
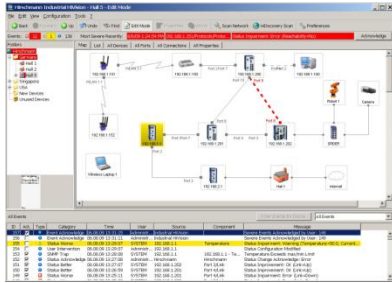


Alle Daten von internen Netzwerk nach aussen und umgekehrt müssen durch die Firewall (keine Hintertüren).

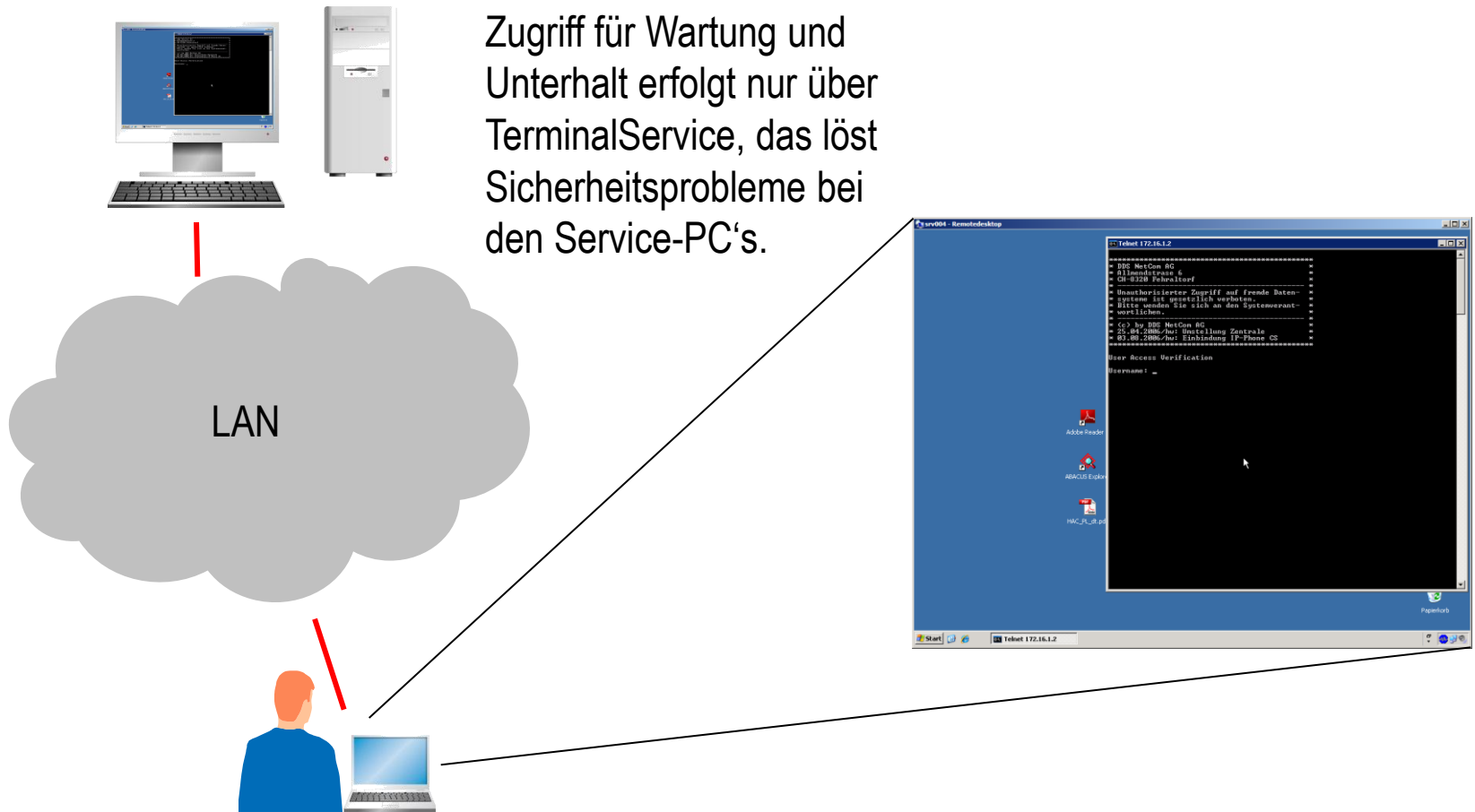
Es werden ausschliesslich autorisierte (Auf der Grundlage eines Sicherheitskonzepts) festgelegte Verbindungen zugelassen.

Die Firewall selbst ist immun gegen Angriffe (ist unsichtbar).

Layer 7: Anwendungsschicht



Layer 7: Anwendungsschicht



Zusammenfassung

Layer 1

Netzwerktopologie bestimmen

Netzwerk physikalisch gegen Nachlässigkeit und Irrtum schützen

Layer 2

Netzwerk durch virtuelle Netzwerke VLAN segmentieren (1 VLAN pro Risikogruppe)

Layer 3

Segmentierte Netzwerke verbinden, Broadcast's verhindern, Netzwerkadressen verbergen



Zusammenfassung

Layer 4 / Layer 5

Datenverbindungen zwischen verschiedenen Netzwerken zentral definieren, authentifizieren und autorisieren.

Layer 7

Netzwerke passiv schützen, indem schlecht gesicherte Systeme simuliert werden, die Angriffe melden.

Wartungsverbindungen immer über TerminalServices realisieren.



Besten Dank.

Besten Dank für ihre Aufmerksamkeit.

YELLO NetCom GmbH & Co. KG
Birkenallee 115-117
48432 Rheine
Telefon 05971 / 961 76-0
Telefax 05971 / 961 76-25
rheine@yello-net.de
hanspeter.weingartner@dds.ch

