KRIKO Engineering GmbH

Automation, Drives & Industrial IT

# NETZWERK-SICHERHEIT IM INDUSTRIELLEN UMFELD

Das vorliegende Dokument dient als praxisnaher Leitfaden zur Netzwerksicherheit im industriellen Umfeld. Es werden nur ausgewählte, in der OT-Umgebung praxiserprobte Mechanismen vorgestellt. Die Bandbreite an möglichen weiteren Sicherheitskonzepten ist weitaus größer.

# INHALT

# EINFÜHRUNG

Cyberangriffe auf kritische Infrastrukturanlagen, Sicherheitslücken in Regierungs-IT-Systemen, Datenpannen aller Art. Schlagzeilen wie diese zieren fast täglich Seiten der Pressedienste im In- und Ausland. Die wirtschaftlichen Folgen für die betroffenen Unternehmen sind teils gravierend.

In einer Umfrage des Bundesamtes für Sicherheit in der Informationstechnik (BSI) von 2019 an IT-Sicherheitsexperten in der Wirtschaft, gaben 87 % der von Cyber-Angriffen betroffene Unternehmen an, dass es dadurch zu Betriebsstörungen und -ausfällen kam (Vgl. Cyber-Sicherheits-Umfrage –Cyber-Risiken & Schutzmaßnahmen in Unternehmen, 2019, S.13). Zugangspunkte für Angriffe sind meist Geräte in IT-Netzwerken.

Bei Anlagen mit hohem Automatisierungsgrad besteht gleichzeitig eine immer größere Notwendigkeit des Zusammenwachsens von IT- und OT-Netzen. In diesem Kontext spielt die OT-Netzsicherheit im industriellen Umfeld eine immer größer werdende Rolle.

Eine sorgfältige Konzeptionierung und Planung des physikalischen Netzes und der Sicherheitsmechanismen sind entscheidend für die spätere Netzsicherheit und Verfügbarkeit der Anlageninfrastruktur. Kriko unterstützt im gesamten Prozess von der Beratung über die Planung, bis hin zur Umsetzung.

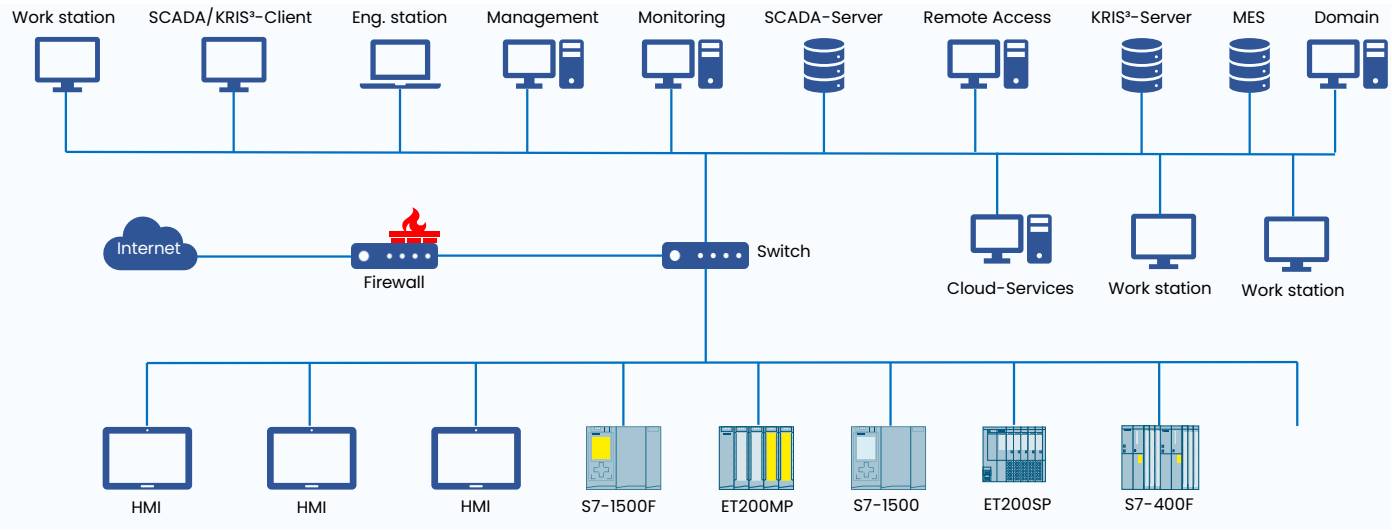
# SEGMENTIERUNG DER NETZWERK-ARCHITEKTUR

Zu Beginn einer jeden Sicherheitsbetrachtung eines Netzwerkes steht die physikalische und logische Betrachtung der Netzaufteilung. In einer Bestandsaufnahme wird geprüft, welche Gliederungen und Segmentierungen von Netzwerkteilnehmern es bereits gibt, um hieraus Maßnahmen ableiten zu können. Die Anforderungen an eine physikalische Netzaufteilung werden unter anderem in den Systemanforderungen der in diesem Bereich führenden Norm ISA/IEC-62443-3-3 FR 5 „Eingeschränkter Datenfluss" beschrieben. Hierbei werden Systemanforderungen an Automatisierungssysteme in Abhängigkeit derer zuvor klassifizierten Security Levels SL1-SL4 (geringes bis hohes SL) gestellt.

In der Anforderung SR5.1 RE 1 als eine Anforderung ab SL2 heißt es beispielsweise:
„Das Automatisierungssystem muss die Fähigkeit haben, automatisierungstechnische Netze von nicht-automatisierungstechnischen Netzen physikalisch abzuteilen und kritische automatisierungstechnische Netze von anderen automatisierungstechnischen Netzen physikalisch abzuteilen." Folgende Schritte beschreiben die praxisnahe Umsetzung dieser und weiterer normativen Anforderungen anhand eines fiktiven Beispiel-Netzes. Es muss berücksichtigt werden, dass die Anforderungen an OT-Netzwerke je nach Branche, Größe des Betriebes und Sicherheitsbewusstsein des Betreibers variieren können und die folgenden Möglichkeiten zu Netz-Segmentierung nur beispielhaft sind.

## Ausgangssituation

Die beispielhafte Ausgangssituation wäre ein heterogenes Netz, in welchem sich IT- und OT-Arbeitsstationen, Komponenten zur netzweiten Bereitstellung von Diensten wie Domain oder Remote Access, sowie Automatisierungskomponenten befinden. Folgende Abbildung zeigt beispielhaft den Netzplan einer solchen Konstellation. Bei dieser Anordnung ist keinerlei physikalische Trennung innerhalb des Netzes vorgesehen.Dies ist eine Konstellation, die in historisch gewachsenen Anlagennetzwerken noch teilweise angetroffen wird, wenn bei der schrittweisen Umrüstung von Feldbustechnik auf Industrial Ethernet Komponenten kein anlagenweites Gesamtkonzept erarbeitet wurde.



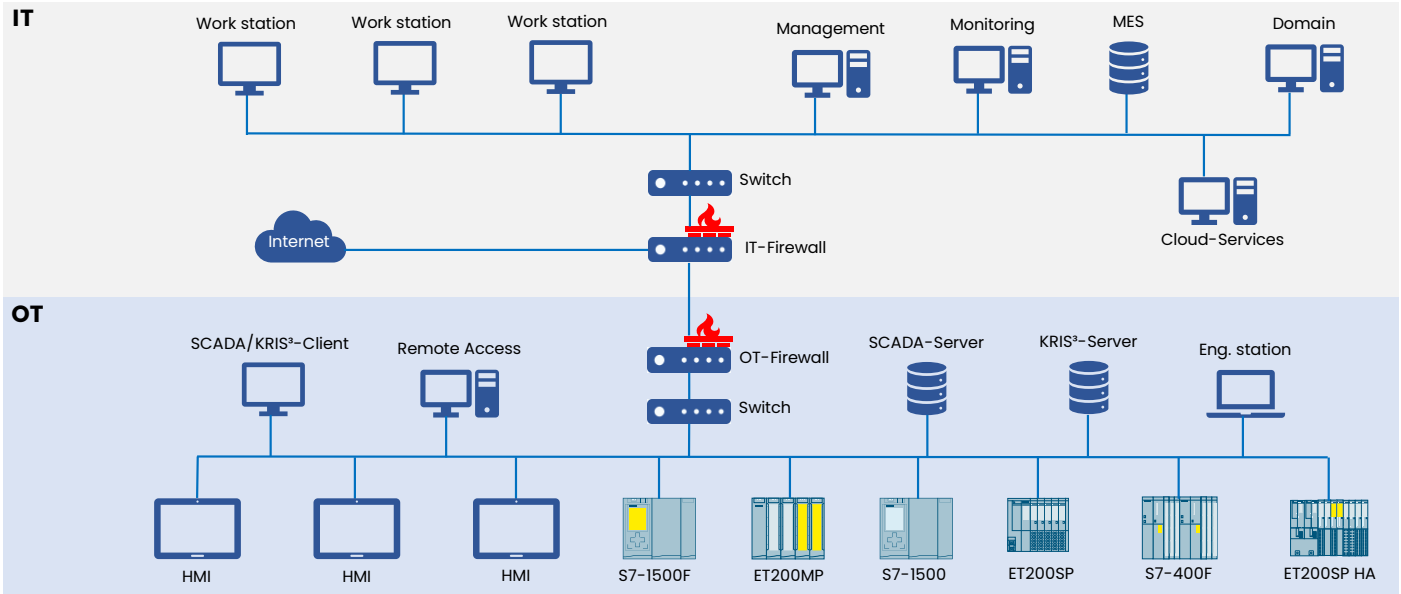
## Trennung von IT und OT

Um den Anforderungen der IEC-62443 hinsichtlich Netzwerksegmentierung gerecht zu werden, müssen im ersten Schritt automatisierungstechnische Netze von nicht-automatisierungstechnischen Netzen logisch abgeteilt werden. Hierzu wird eine Unterteilung in IT- und OT-Netz vorgenommen.

Weiter fordert die ISA/IEC-62443-3-3 SR5.2 (SL1-SL4): „Das Automatisierungssystem muss die Fähigkeit haben, die Kommunikation an Zonengrenzen zu überwachen und zu kontrollieren […]“ und SR5.2 RE 1 (SL2-SL4) „Das Automatisierungssystem muss die Fähigkeit bieten, Netzverkehr von vornherein abzulehnen und ihn nur in Ausnahmefällen zuzulassen.“

Um dieser Anforderung gerecht zu werden, wird die Trennung über hardwarebasierte Next-Generation-Firewalls auf IT- und OT-Seite vorgenommen. Hierbei ist der Grundgedanke, dass ein jedes Netzsegment sich selbst vor ungewollter Kommunikation schützt. Per Whitelisting werden nur gewünschte und dokumentierte Kommunikationsbeziehungen zugelassen.

Die Anbindung an das Internet erfolgt auf der weniger kritisch angesehenen IT-Seite, sodass die gesamte Kommunikation von und zum OT-Bereich an der OT-Firewall kanalisiert wird.
Die folgende Abbildung zeigt den Netzplan nach der Trennung.



## Einführung einer DMZ

Eine weitere Anforderung der ISA/IEC-62443-3-3 in SR5.1 RE 2 (SL3-SL4) besagt „Das Automatisierungssystem muss die Fähigkeit bieten, ohne eine Verbindung zu nicht automatisierungstechnischen Netzen Netzdienste bereitzustellen in automatisierungstechnischen Netzen […].“

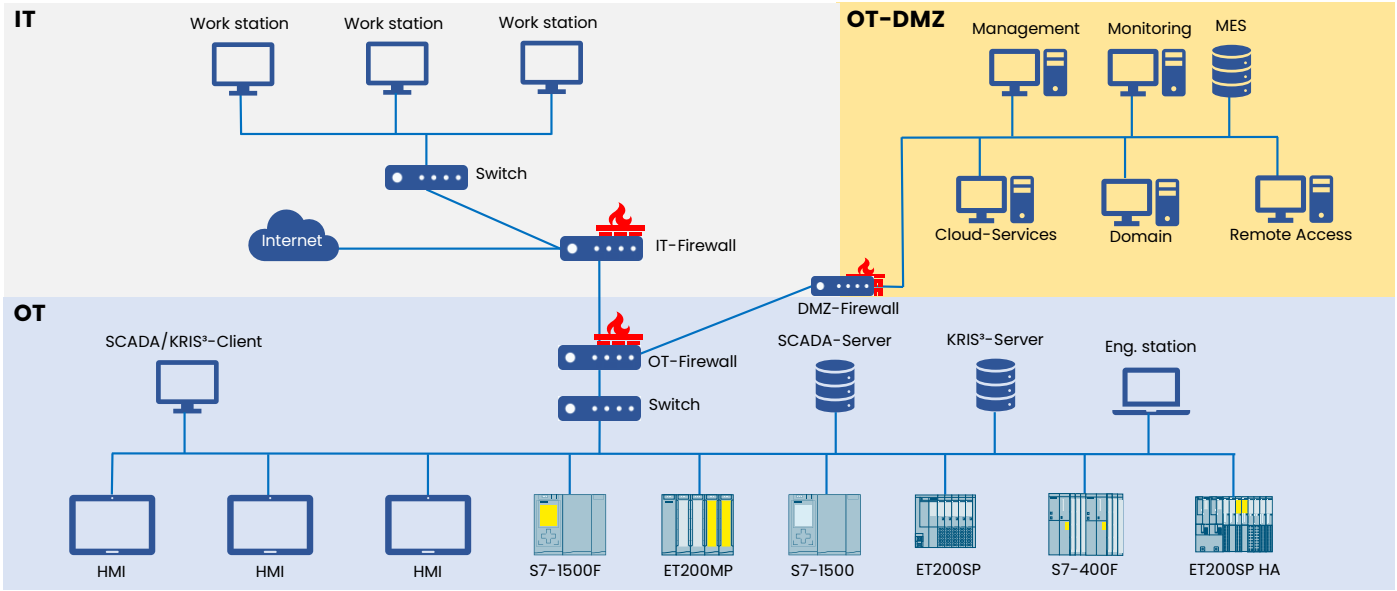
Wie können Dienste wie Fernzugriff, MES, Cloud Services, Netzwerkmanagement, Webserver, Fileserver, Antivirus-Server etc. ohne direkte Verbindung zwischen IT-Netz und OT-Netz in der OT-Umgebung verfügbar gemacht werden? Die Lösung hierfür ist das Schaffen einer weiteren Sicherheitszone, der sogenannten DMZ (demilitarisierten Zone).

Alle Komponenten, die Verbindungen in andere, nicht vertrauenswürdige Netze herstellen, werden physikalisch getrennt von IT und OT in ein separates Netzwerk überführt.
Eine DMZ kann in der Praxis auf zwei verschiedene Art und Weisen erstellt werden:

1. An einer einzelnen Firewall wird ein separater physikalischer Port mit eigenem VLAN genutzt, an dem die DMZ errichtet wird. Der Traffic von und zur DMZ wird überwacht.

2. Sicherer ist es, zwei physikalisch getrennte Firewalls zu nutzen, eine auf DMZ-Seite und eine auf der OT-Seite. Bestenfalls sind die Firewalls von zwei verschiedenen Herstellern, sodass Sicherheitslücken noch unwahrscheinlicher werden.

Die nachfolgende Abbildung zeigt das Schaffen einer DMZ in der Beispiel-Netz-Konfiguration.

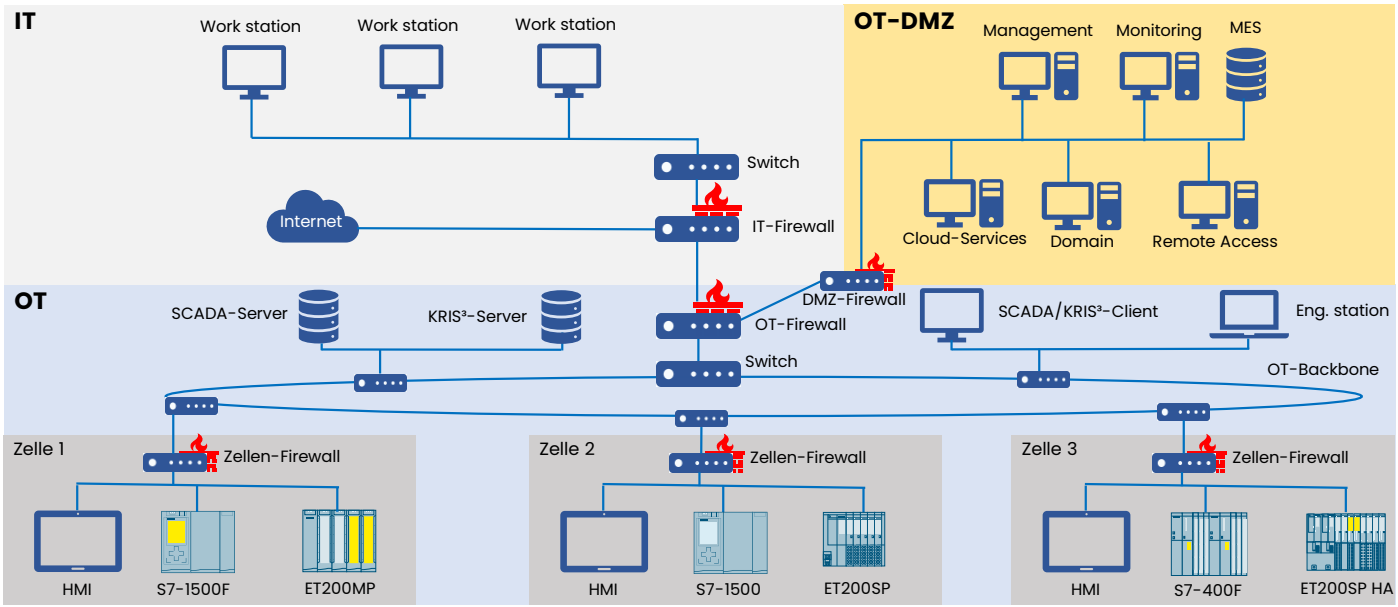


## Bilden von Zellen

Die nächste Anforderung der ISA/IEC-62443-3-3 in SR5.1RE3(SL4) besagt „Das Automatisierungssystem muss die Fähigkeit bieten, kritische von nicht kritischen automatisierungstechnischen Netzen logisch und physikalisch zu isolieren."

Die geforderte Isolierung wird über die Bildung sogenannter Zellen organisiert. Der ein- und ausgehende Datenstrom einer jeden Zelle wird durch eine Zellen-Firewall kontrolliert. Innerhalb der Zellen sind alle gängigen Bustopologien denkbar.

Die folgende Abbildung zeigt die Zellenbildung anhand des Beispiel-Netzes:




Für die Segmentierung auf Zellebene innerhalb eines OT-Netzes gibt es einige Ansätze, die anlagenspezifisch betrachtet werden müssen. Kriterien zur Bildung von Zellen können sein:

**Funktionale Beziehung**
Mehrere Maschinen derselben Produktionslinie können eine Zelle bilden.

**Echtzeitbedürfnisse**
Bei hohen Anforderungen an Latenz oder Taktsynchronität zwischen automatisierungstechnischen Komponenten, müssen sich diese Komponenten in derselben Zelle befinden.

**Funktionale Sicherheit**
Kritische Anwendungen im Sinne der funktionalen Sicherheit, die zu Schaden von Personal oder Maschinen führen können, erfordern eine Trennung anderer nicht-kritischer Anwendungen.

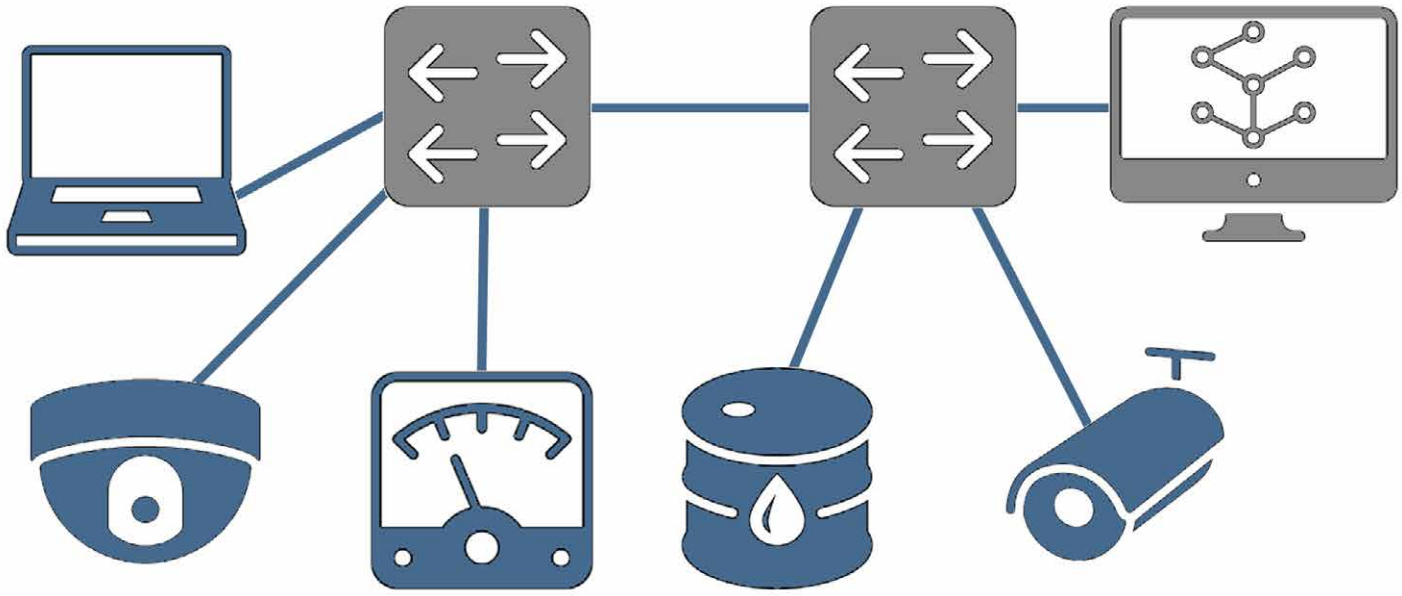
**Risiko**
Geräte, die als kritisch im Sinne der IT-Sicherheit angesehen werden (bspw. Rechner mit veralteten Betriebssystemen) können in dieselbe Zelle gruppiert werden, um ein- und ausgehende Datenströme kontrollieren zu können.

# SCHUTZ DER NETZWERK-INFRASTRUKTUR

**Die Basis eines jeden Netzwerks bilden die darin eingesetzten Geräte. Der erste Schritt auf dem Weg zu einem sicheren und damit hochverfügbaren Netz ist der Schutz der eigentlichen Netzwerkinfrastruktur. Die nachfolgend vorgestellten Mechanismen dienen der Regulierung von Zugriffen auf einzelne Teilnehmer.**

## VLANs

VLANs (Virtual Local Area Networks) bieten die Möglichkeit, unabhängige Netzwerke auf derselben physikalischen Basis zu erstellen. Geräte in einem VLAN erkennen standardmäßig keine Geräte in anderen VLANs.
So ist es möglich, ein Netzwerk logisch zu segmentieren. Beispielsweise können Management-Zugriffe auf die Netzwerkinfrastruktur, Client-Server-Zugriffe im OT-Netz und Anlagenkommunikation zu Automatisierungsgeräten komplett voneinander getrennt und der Datenverkehr je VLAN priorisiert werden. Die Netzwerkinfrastruktur für eine solche Segmentierung und Priorisierung bieten entweder gemanagte Layer-2 Switche mit einer oder mehreren zentralen Firewalls, oder im einfachsten Fall Layer-3 Switche.



## User Management

In vielen Betrieben ist es nach wie vor übliche Praxis, Standardpasswörter und gemeinsame Log-Ins für mehrere Mitarbeitende zu nutzen. Oft sind die Passwörter auch noch frei zugänglich. Dies führt dazu, dass einer der effektivsten Schutzmechanismen in der Netzwerksicherheit, die Zugriffskontrolle, seine Wirkung nahezu verliert. Zudem wird die Nachverfolgbarkeit von Tätigkeiten einzelner Benutzer durch Log-Files oder Audit-Trails hierdurch ausgehebelt.
Wie aber dieses Problem lösen, bei vielen verschiedenen Geräten und Systemen in einem Netzwerk? Ein Benutzer je Mitarbeitenden für jeden Netzwerkteilnehmer mit entsprechenden Password Policies definieren? Das ist kaum möglich und nicht praktikabel, kostet Zeit und ist fehleranfällig. Würden neue Mitarbeitende eingestellt werden, so müssten alle entsprechenden Geräte umkonfiguriert werden.

Es besteht also die Notwendigkeit, User Management von einer zentralen Stelle aus zu tätigen. Eine Lösung stellt ein zentraler Domain-Server mit zentraler Authentifizierung aller Geräte per LDAP (Lightweight Directory Access Protocol) dar. So können Benutzergruppen und deren Rechte zentral verwaltet werden. Alle Mitarbeitenden können sich mit ihren Zugangsdaten nur auf denen ihnen erlaubten Geräten mit dem ihnen zugewiesenen Rechten anmelden.
Dies erhöht nicht nur die Sicherheit, für die Mitarbeitenden entfällt so auch das leidige Thema der Passwortlisten, da sie ein User und Passwort per Single-Sign-On für alle Geräte und Systeme nutzen.

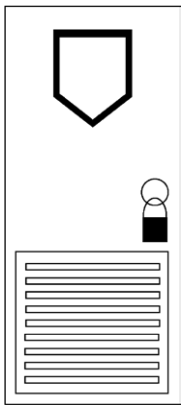
| User | Role | Password |
|---|---|---|
| Mark | Operator | ***** |
| David | Auditor | ***** |
| admin | Administrator | ***** |
| user | Guest | ***** |

# STEUERUNG INTERNER NETZWERKZUGRIFFE

**Nachdem der Schutz vor unautorisierten Zugriffen auf die Netzwerkinfrastruktur praktikabel umgesetzt wurde, kann nun das Einbringen von Netzwerkteilnehmern innerhalb eines Netzwerks betrachtet werden. Die folgenden Methoden dienen zur Sicherung des Netzwerks vor unerlaubten Zugriffen durch Geräte, die sich bereits innerhalb einer Organisation befinden.**

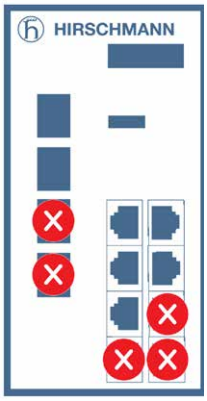
## Physikalische Verriegelung

Um unerlaubte Zugriffe auf das Netzwerk zu verhindern, ist eine sehr einfache und besonders effektive Methode die physikalische Verriegelung der Netzwerkschränke durch abschließbare Türen.



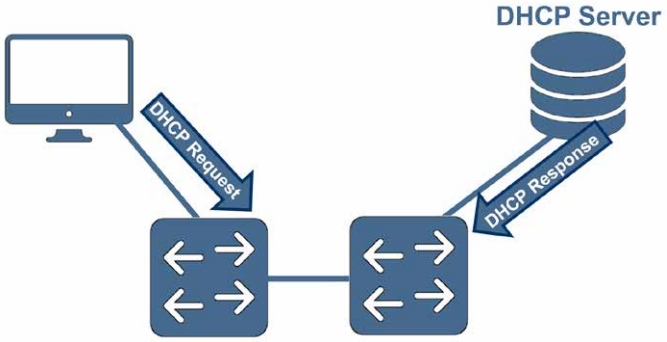
## Deaktivierung ungenutzter Ports

Das Einbringen von unerwünschten Geräten in ein Netzwerk ist eines der häufigsten Szenarien, die gewollt oder ungewollt zu Netzwerkproblemen führen. Um den unkontrollierten Wildwuchs eines Netzwerkes und böswillige Attacken von unerwünschten Geräten zu verhindern, werden alle ungenutzten Ethernet-Ports an Netzzugangspunkten wie Switchen deaktiviert.




## DHCP-Server

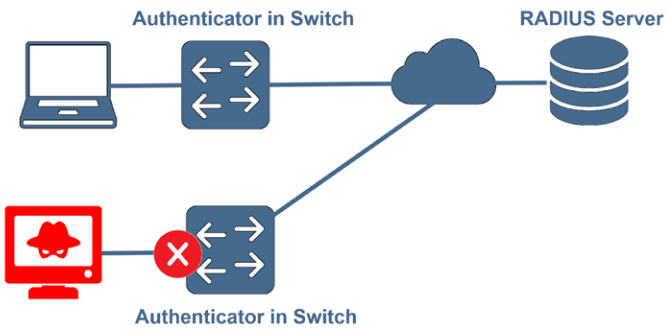
Wird ein externes Gerät temporär ins Netzwerk integriert, besteht die Gefahr, dass es zu IP-Adresskonflikte mit anderen Netzwerkteilnehmern kommen kann. Um dies zu verhindern, können an Netzzugangspunkten auf speziell definierten Service-Ports eine automatische Zuweisung einer ungenutzten IP-Adresse innerhalb eines definierten DHCP-Adressbereichs durch einen zentralen DHCP-Server erfolgen.




## Port-basierte Netzwerkzugriffskontrolle

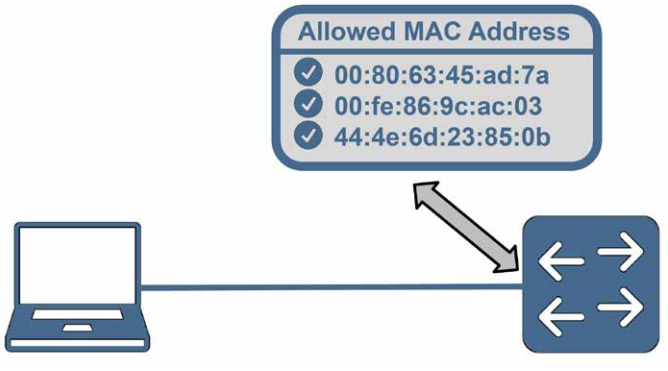
Manchmal ist es notwendig, externe Geräte temporär ins Netzwerk zu integrieren. Ein Beispiel hierfür könnte der Service-Laptop eines Wartungstechnikers einer Maschine im Anlagennetz sein. Hierzu können spezielle Service-Ports an den Netzzugangspunkten definiert werden.

Bei Anschluss an einem solchen Service-Port wird per zentraler Authentifizierung mit den Benutzerdaten des Service-Technikers im Netzwerk entschieden, ob und welchen Netzwerkzugriff der Benutzer erhält oder nicht. Die Definition, welche Benutzergruppen auf welche Geräte und VLANs mit welchen Protokollen zugreifen dürfen, geschieht in der Konfiguration der Firewall. Die Definition der Benutzer und Benutzergruppen erfolgt an einem zentralen Domain-Controller und werden per LDAP auf das gesamte Netzwerk ausgerollt.
So können an zentraler Stelle die Netzwerkzugriffsrechte des Service-Technikers nach Beendigung seines Einsatzes wieder entzogen werden.



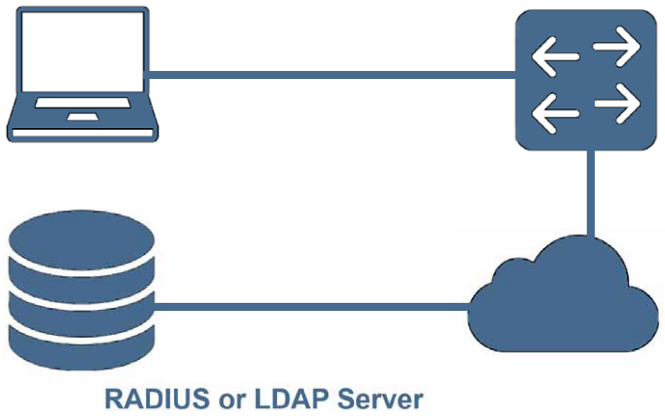

## Port-Sicherheit per MAC-Filterung

Werden ungenutzte Ports deaktiviert und der Zugriff an Service-Ports reguliert, so besteht immer noch die Gefahr des Aussteckens eines aktiven Netzwerkteilnehmers und Einbringen eines unerwünschten Gerätes. Um dieses Szenario zu unterbinden, können jedem Port eines Netzzugangspunktes eine feste MAC-Adresse zugewiesen werden, welche mit der des angeschlossenen Gerätes übereinstimmen muss. Datenpakete an diesem Port, die nicht von dieser MAC-Adresse kommen, werden verworfen. Auf diese Weise ist sichergestellt, dass keine unerwünschten Geräte an nicht deaktivierten Ports von Switchen kommunizieren dürfen.




## Port-Sicherheit per RADIUS-Server

Gerade bei virtualisierten Plattformen und großen OT-Netzwerken ist die MAC-Filterung unpraktikabel, da bei redundanten Host-Systemen MAC-Adressen virtueller Maschinen sich nicht immer am selben physikalischen Ort befinden. Außerdem muss jeder zur MAC-Filterung beteiligte Switch entsprechend parametriert werden, was die Verwaltung stark verkompliziert.
Die Lösung auf diese und viele weitere Probleme bietet ein zentraler RADIUS-Server, wie beispielsweise Microsoft NPS (Network Policy Server). Dieser stellt eine zentrale Authentifizierungsstelle für Netzwerkzugriffe dar. Hierüber können Geräte von zentraler Stelle über eine Authentifizierung per Benutzerdaten, Zertifikat oder MAC-Adresse in das zum Gerät passende VLAN integriert werden. So stehen auch in physikalisch flexiblen Netzwerken jedem Gerät nur die Ressourcen und Services zur Verfügung, für die das Gerät vorgesehen ist.



# KONTROLLE DES DATENVERKEHRS

**Wurde das Netzwerk gegen ungewollte Zugriffe geschützt, so kann in einem weiteren Schritt der Datenverkehr kontrolliert werden. Dieser weitere Sicherheitsaspekt beinhaltet die Steuerung, Analyse und das Monitoring von Datenpaketen zur Laufzeit.**

## Netzwerk-Traffic steuern

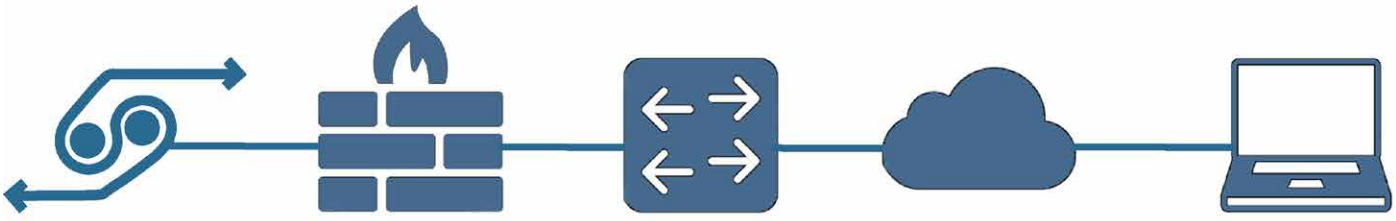
Wurde ein Netz intelligent per VLANs logisch segmentiert, so kann überlegt werden, in welchen Fällen eine VLAN-übergreifende Kommunikation notwendig ist. Hierzu gehören beispielsweise der Fernzugriff zum OT-Netz aus einem IT-Netz oder einer DMZ, die Datenweiterleitung an eine Cloud, die Kommunikation zu MES und ERP-Systemen, sowie Authentifizierungsanfragen an einen externen LDAP-Server etc.

Diese Zugriffe werden per Standard durch eine zentrale Firewall verhindert. VLAN- und netzübergreifende Zugriffe müssen dann explizit per Firewall-Regeln zugelassen werden. In dieser Zugriffssteuerung wird nicht nur über Quell- und Zielangabe definiert, wer zu wem kommunizieren darf, sondern auch per Application-Control (Freigabe nur bestimmter Protokolle), was kommuniziert werden darf.

## Netzwerk-Zugriffe analysieren

Die von Kriko eingesetzten Firewalls besitzen die Möglichkeit, den Datenverkehr auf netzübergreifenden Verbindungen in Hinblick auf mögliche Bedrohungen zu analysieren. Hierzu gehören Dienste wie Antivirus, Intrusion Prevention, Application Control, Web Filtering, Antispam und viele mehr.

Die Firewalls werden über einen sicheren Kanal an das Internet angebunden, um die aktuellen Viren- und Bedrohungs-Definitionen zu kennen. So können sie Bedrohungen über zuvor freigegebene Verbindungen von außen wirksam sperren, bevor sie Schaden anrichten können.



## Netzwerk-Monitoring

Als strategischer Partner der Firma Paessler bietet Kriko seinen Kunden mit dem Tool PRTG ein mächtiges Netzwerkmonitoring.
Von zentraler Stelle aus werden die benötigten Bandbreiten der Geräte und Anwendungen definiert und geprüft. Datenbanken im Netzwerk werden überwacht, Statistiken zu Anwendungen im Netzwerk werden erstellt.

Alle Server, Clients, Netzwerkinfrastrukturgeräte, Steuerungen und sonstige Netzwerkteilnehmer können in Echtzeit auf deren Erreichbarkeit, Verfügbarkeit, Kapazität und Zuverlässigkeit überwacht werden. Netzwerktopologien werden automatisch erkannt und auf Änderung überwacht.
Mit diesen und vielen weiteren Möglichkeiten ist das Netzwerk-Monitoring ein zentraler Pfeiler zur aktiven Erhöhung der Netzsicherheit und -verfügbarkeit.



Quellen:

Bundesamt für Sicherheit in der Informationstechnik: Cyber-Sicherheits-Umfrage –Cyber-Risiken & Schutzmaßnahmen in Unternehmen, 2019, S.13

Bundesamt für Sicherhiet in der Informationstechnik : ICS- Security-Kompendium Version 1.23

Hirschmann by Belden Electronics GmbH: Network Security in the Hirschmann Operating System, 2020

HI Solutions AG , VDMA : Security in Automation - Profilierung von IT-Sicherheitsstandards für den Maschinen- und Anlagenbau

Paessler AG: https://www.paessler.com/de/prtg-enterprise-monitor, 2022

Siemens AG 2019: Industrial Communication in Food & Beverage

Siemens AG 2021 : Sichere industrielle Netzwerkarchitektur

## Über die KRIKO Engineering GmbH

**KRIKO Engineering ist Ihr Partner für Automatisierung, Antriebstechnik und industrielle IT – regional im Südwesten verwurzelt, aber auch weltweit tätig. Als unabhängiges Ingenieurbüro verfügen wir über 30 Jahre Erfahrung in der Umsetzung von Energie- und Automatisierungsprojekten im industriellen Umfeld – von der Beratung über die Planung bis zu Inbetriebnahme und Service. Auf Bewährtes setzen und gleichzeitig mit viel Elan neue Wege beschreiten, sind die Grundprinzipien unserer Arbeit.**

**Wir steuern Maschinen oder gesamte Produktionsanlagen und schaffen eine effiziente und hochverfügbare Infrastruktur, wie z.B. IT-Netzwerke oder Medienversorgung, für Ihre optimalen Produktionsbedingungen. Neben dem Bau von Neuanlagen, sind wir vor allem im Bereich des Retrofit tätig. Denn auch Bestandsanlagen müssen den aktuellen Anforderungen hinsichtlich hoher Energieeffizienz, Qualität, Flexibilität, Verfügbarkeit und Sicherheit gerecht werden. Durch unser über 20 Jahre hinweg weiterentwickeltes Prozessinformationssystem KRIS³ und unser IT- und Netzwerk-Know-how sind wir zudem Lösungsanbieter für Digitalisierung und Industrie 4.0**

## ANSPRECHPARTNER


**Felix Steinkuhl**
Technischer Vertrieb
Projektleitung

+49 761 40078 45
felix.steinkuhl@kriko.com

**Daniel Secci**
Informationstechnik

+41 61 68324 82
+49 761 40078 55
daniel.secci@kriko.com

KRIKO Engineering GmbH
Automation, Drives & Industrial IT

**Deutschland**
Merzhauser Straße 120
79100 Freiburg
Tel. +49 761 40078 0

**Schweiz**
Riehenring 175
4058 Basel
Tel. +41 61 68324 80