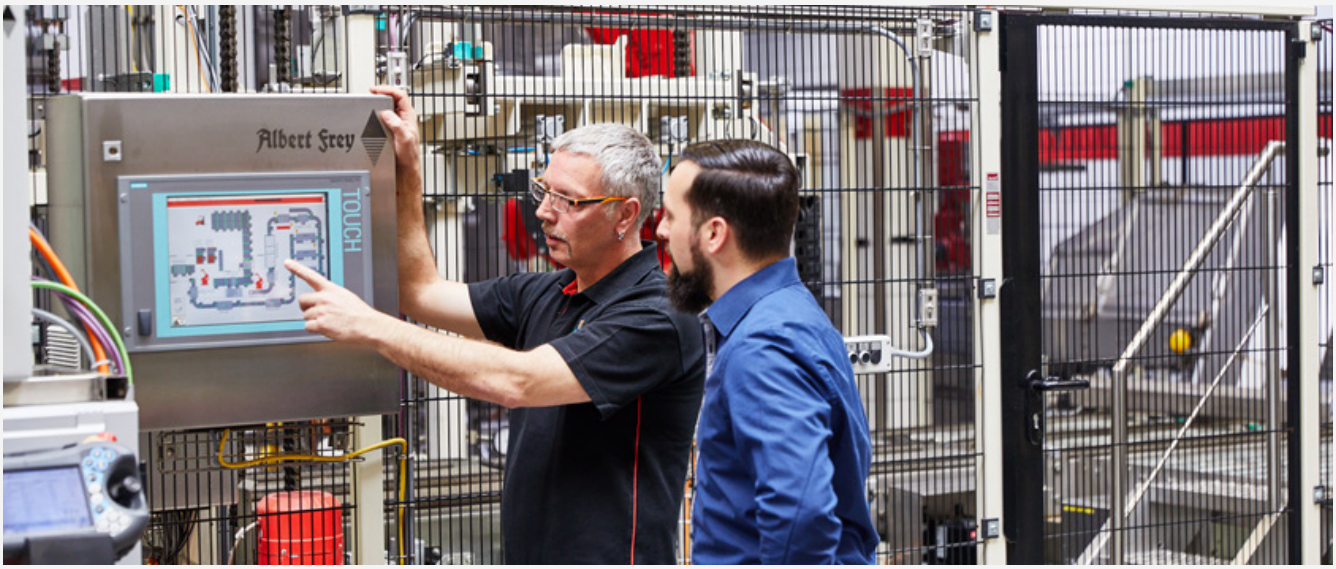
In 3 Schritten zur Netzwerksegmentierung

So integriert man schnell und einfach netzwerkseitig seinen Produktionsbereich

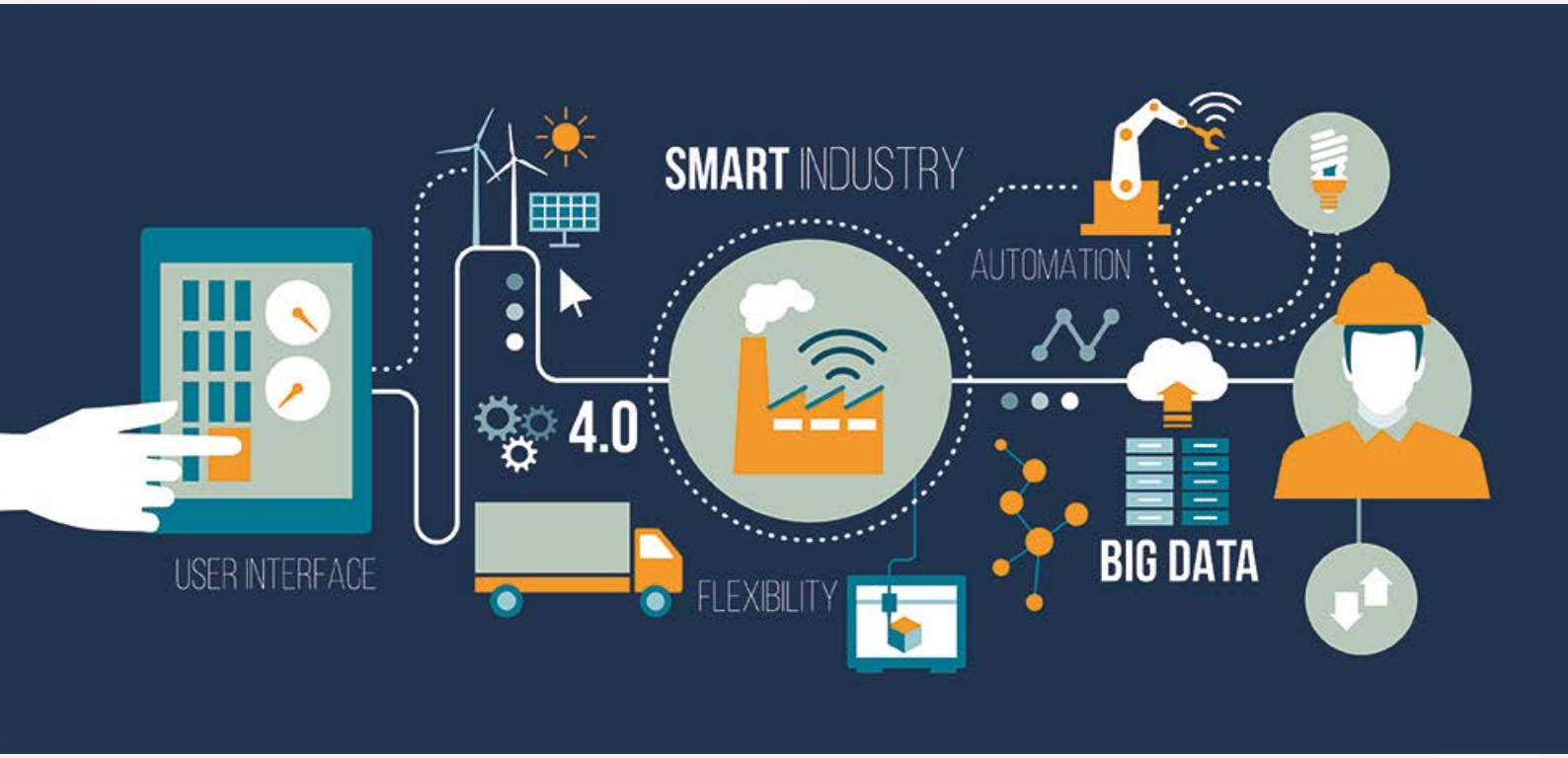
Ein Leitfaden

HWI
wir integrieren IT



INHALTSVERZEICHNIS

Warum gerade die Netzwerksegmentierung so wichtig ist!



Digitale Transformation, Industrie 4.0, Smart Factory – diese Buzzwords haben alle etwas gemeinsam: Mehr Daten, mehr Kommunikation und damit verbunden die Notwendigkeit eines zuverlässigen Netzwerkes. Die fortschreitende Vernetzung von Produktionsanlagen birgt aber auch Risiken – Störungen und Angriffe können sich ungebremst ausbreiten. Ein segmentiertes Netzwerk ist eine wichtige Voraussetzung, um diese Risiken einzuschränken und damit die Anforderungen an die Digitalisierung zu erfüllen. Wahrscheinlich ist Ihnen das bewusst, dennoch ist Netzwerksegmentierung eine Investition, die viele scheuen.

Dabei ist ein ordentlich segmentiertes Netzwerk grundlegend nichts Neues – es gehört zu einem intelligenten Netzwerkdesign dazu, ist sozusagen Best-Practice und Industrie-Standard.

In der IT gilt das schon seit es Netzwerke gibt. Durch die Vernetzung von Produktionsnetzwerken wird es nun auch in der OT (Operational Technology) zur Triebfeder. Im Produktionsbereich können wir uns Ausfälle nicht leisten – Verfügbarkeit ist das oberste Ziel. Es kommt zu einer Verschiebung der Schutzziele:

- Für die IT-Abteilung steht als wichtigster Wert zuallererst die Sicherheit und Vertraulichkeit der Daten, gefolgt von der Integrität und Echtheit der Daten, während am Ende erst die Verfügbarkeit dieser Daten steht.
- In der OT verhält sich das traditionell umgekehrt: Mit oberster Wichtigkeit wird hier die Verfügbarkeit der Daten betrachtet, danach kommen Integrität und Vertraulichkeit.

Um Gefahren zu minimieren und die Gewährleistung der Schutzziele sicherzustellen, ist die Schaffung einer standardisierten Sicherheitsstruktur notwendig. Die Netzwerksegmentierung ist neben dem Asset Management und der Absicherung der Fernzugriffe die grundlegende technische Maßnahme zur Schaffung einer solchen Sicherheitsstruktur auf Basis der Norm IEC 62 443.

Vorteile einer Netzwerksegmentierung

Segmentierte Netzwerke sollten als Basis für die Umsetzung von IT / OT-Projekten gesehen werden und dienen der Optimierung von Automationsprozessen.

HWI TIPP: Diese Vorteile entstehen durch die Netzwerksegmentierung

- **Mehr (Zugangs-)Kontrolle:** Klare Definition von Berechtigungen für Netzwerkteilnehmer.
- **Verbesserte Sichtbarkeit:** Im Assessment werden alle Netzwerkteilnehmer dokumentiert.
- **Erhöhte Sicherheit:** Kontrolle und Sichtbarkeit sind Verstärker für die Sicherheit.
- **Schutz der User:** Durch die Einschränkung von Zugang und Kommunikation, können User-Fehler vermieden werden.
- **Vereinfachte Fehlerbehebung:** Durch das Wissen über alle Netzwerkteilnehmer und ein logisches Design können Fehler schneller und einfacher behoben werden. Außerdem wird durch die erhöhte Sichtbarkeit des Datenstroms das Troubleshooting von Verbindungen einfacher.
- **Kommunikationsbeziehungen aufzeigen:** In einem segmentierten Netzwerk können Kommunikationsbeziehungen einfacher dargestellt und nachvollzogen werden. Ebenfalls können sie z.B. durch Firewalls kontrolliert werden.
- **Schadens-/ Störungsbegrenzung:** Im Falle eines Angriffs oder einer Störung bspw. durch einen Broadcast-Sturm ist nicht das gesamte Netzwerk betroffen.
- **Höhere Performance:** Weniger Verbindungen erhöhen die Performance.
- **Ermöglichung von gemischten Umgebungen:** Ein homogenes Netzwerk ist nicht immer möglich, in einem segmentierten Netzwerk ist es jedoch einfacher, verschiedene Hersteller und Komponenten zu mischen.
- **Verbesserung des Monitorings:** Durch die Übersicht über alle Netzwerkteilnehmer wird auch das Monitoring einfacher.
- **Mehrwert für Anlagen- und Lebenszyklusmanagement:** Das Wissen über die Verwendung, den Status und die Anlagen im Netzwerk bietet einen deutlichen Mehrwert
- **Konformität und Compliance:** Ein normkonformes Netzwerk kommt nicht ohne Segmentierung aus.

Bedrohungen für das Produktionsumfeld – Warum ist IT-Sicherheit auch für meine Industrieanlage relevant?

Wieso besteht überhaupt die Gefahr vor Ausfällen im Produktionsumfeld? Ist es nur der erhöhte Vernetzungsgrad, der es Angreifern einfacher macht in mein Netzwerk einzudringen? Nicht nur, denn es gibt auch andere Faktoren, die eine große Rolle spielen:

- (Unsichere) IT-Standardtechnologien (z.B. Router, Switche) im Industrieumfeld, die nicht auf den Einsatz in der Industrie ausgelegt sind.
- Bestandsanlagen haben meist eine Laufzeit von 15-30 Jahren und waren nie darauf ausgerichtet an ein Netzwerk angeschlossen zu werden. Sie laufen häufig auf veralteten Betriebssystemen. Update- und Patchmanagement gibt es nicht.
- Die IT im Automatisierungsumfeld wurde nicht professionalisiert. Datenerfassungssysteme, Fernwartung etc. wurden in die Netzwerkinfrastruktur integriert – ohne Konzept und Dokumentation.
- Hersteller der Industriesysteme verwenden eigene Technologien, die für die normale Office-IT unbekannt sind und damit den Zugang erschweren.

Das Ergebnis ist eine vernetzte Anlagenlandschaft,

- ohne Konzept und eine klare Übersicht,
- der es an Sicherheit und Skalierbarkeit fehlt,
- ohne Standardisierung, auf Grund der Vielzahl an herstellereigenen Systemen,
- die Angriffe nicht abwehren kann,
- in der sich Angreifer und Fehler einfach ausbreiten können und
- die auch bekannte Schwachstellen aufweist durch das Fehlen von Patches.

Einige dieser Punkte kommen Ihnen vielleicht bekannt vor – eventuell weist Ihre Anlagenlandschaft ähnliche Merkmale auf. Digitalisierungsprojekte auf dieser Grundlage durchzuführen ist nicht ratsam – erst die Schaffung einer Sicherheitsstruktur kann für eine reibungslose digitale Transformation sorgen.

Weidele, M. (2020, Mai 12). Der große Industrial Security Guide: Ein komprimierter Leitfaden für Einsteiger, Abgerufen 15. November 2020, von https://www.sichere-industrie.de/industrial-security-guide/

Normengrundlagen: IEC 62 443

Die Normenreihe IEC 62 443 hat sich in den letzten Jahren zu einem Standard für Industrial Control Systems entwickelt. Die IEC 62 443 leitet sich aus der ISO 27001 ab und befasst sich mit der IT Security im Produktions- und Automatisierungsbereich. Die Netzwerksegmentierung spielt dabei in verschiedenen Bereichen immer wieder eine Schlüsselrolle. Als Standardfamilie ist die Norm sehr umfangreich und komplex, deshalb konzentrieren wir uns nun nur auf das Relevante für die Netzwerksegmentierung.

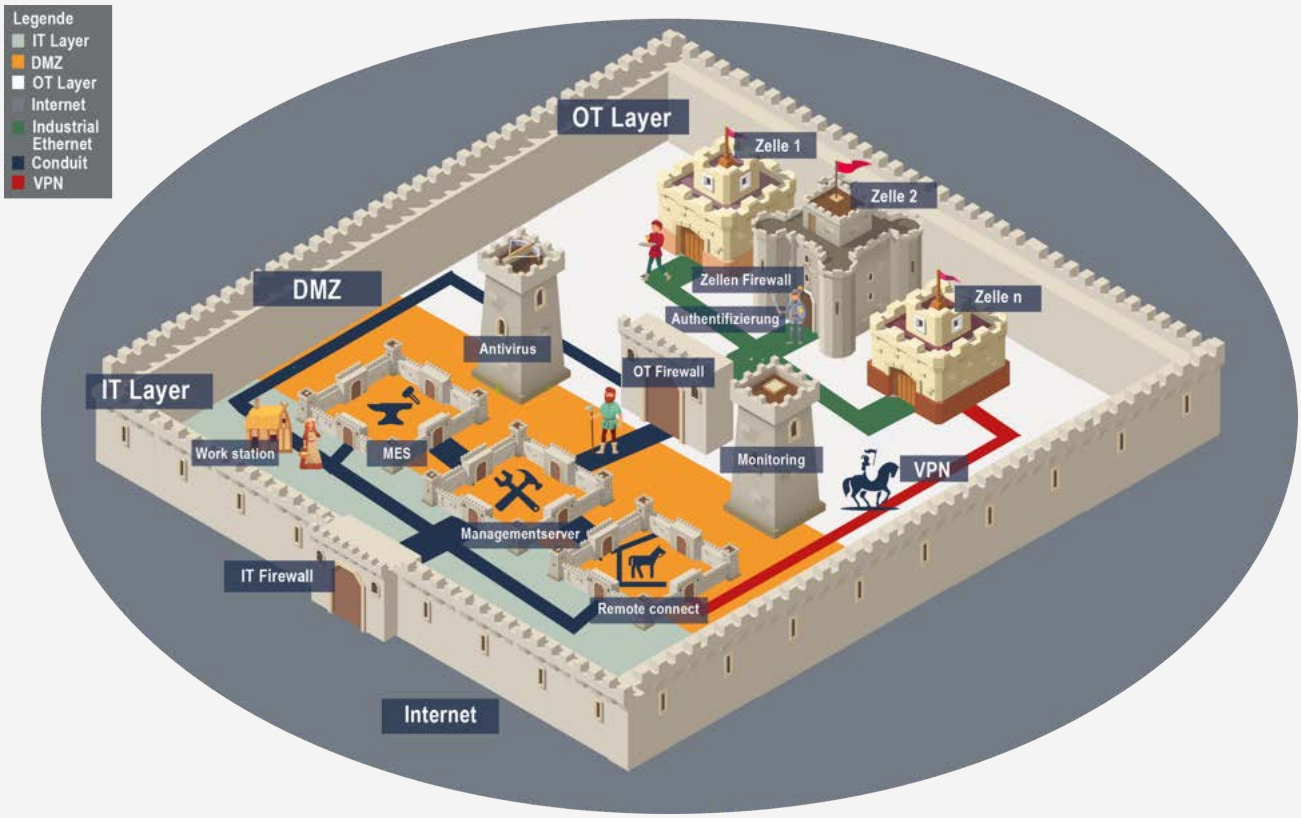
Physische Trennung IT <-> OT	• Defense-in-Depth • Ein definierter und kontrollierter Übergang • Resiliency & Business Continuity
Zones & Conduits	• Bildung von Security-Zonen auf Basis der Risikoabschätzung • Definierte Übergänge zwischen Security-Zonen • Zonenübergreifene Kommunikation einschränken
Single-homed-Assets	• Auflösung von Dual-homed-Assets • Definierte und kontrollierte Übergänge
Zellen	• Verfügbarkeit • Resiliency & Business Continuity

Grundlage ist der **„Defense-in-Depth“** Ansatz, welcher von der physischen Trennung zwischen IT und OT ausgeht. Dadurch wird ein kontrollierter und definierter Übergang geschaffen. Seinen Ursprung eigentlich im Militär, hat dieser Ansatz das Ziel, sicherzustellen, dass ein Angreifer (in unserem Fall ein Störfall) sich nicht durch das Aushebeln einer einzigen Maßnahme ungehindert ausbreiten und Schaden anrichten kann. Durch „gestaffelte Verteidigung“, also mehrere Maßnahmen, die auf dieselben Angriffsvektoren wirken, kann das Netzwerk geschützt werden. Ein wichtiger Bestandteil dieses Konzeptes sind **Zonen und Übergänge.**

Diese Sicherheitszonen werden auf Basis einer **Risikoabschätzung** (Threat-Risk-Assessment) erstellt. Eine Sicherheitszone stellt ein Security Level dar, und die jeweiligen Assets in der Zone haben einen bestimmten Schutzbedarf oder ein bestimmtes Risiko. Mittels Beurteilung des Asset-Werts, Bedrohung und Schwachstellen, wird das Risiko und nach Umsetzung entsprechender Maßnahmen, das Restrisiko ermittelt.

Das Defense-in-Depth Konzept kann man sich wie eine Burg vorstellen. Dort gibt es verschiedene Bereiche (Zonen), wie etwa das Handwerksviertel, oder die Schatzkammer, in denen verschiedene Personengruppen (Assets), bspw. der Schmied oder der Burgherr, leben. Beide Zonen haben sowohl unterschiedliche Schutzziele, als auch individuelle Zugangsberechtigungen.

Angenommen der Schmied muss einen Dienst für den König erbringen und dafür in die Schatzkammer (Zone), so benötigt er eine Zugangsberechtigung und muss auf dem Weg von seiner Schmiede bis zur Schatzkammer beim Gang durch die verschiedenen Viertel kontrolliert werden auf "den König gefährdende Mitbringsel". Er wird außerdem auch beobachtet von einer Wache auf einem Turm (Monitoring) und einer zweiten Wache mit Pfeil und Bogen (Antivirus), die schnell eingreifen kann, wenn sie etwas Verdächtiges sieht. Der Schmied muss also verschiedene Barrieren (Übergänge) durchdringen. Diese Barrieren besitzen abhängig von Ihrer Wichtigkeit ein unterschiedlich hohes Sicherheitslevel und müssen dementsprechend abgesichert werden. Vor der Schatzkammer tritt er dann bspw. auf eine Wache und muss sich und seinen Dienst ausweisen (Authentifizierung).



Geiger, M. (2018, Mai 15). Zones & Conduits: Das Schutzkonzept aus der IEC 62443 einfach erklärt, Abgerufen 15. November 2020, von https://www.sichere-industrie.de/zones-conduits-das-schutzkonzept-aus-der-iec-62443-einfach-erklaert/
Schulz, T. (2020) Cybersicherheit Für vernetzte Anwendungen in der Industrie 4.0 (1.Aufl.). Vogel Communications Group

Gäbe es lediglich ein Viertel, in dem sich alle Bewohner aufhielten, führte das zu einem unübersichtlichen Chaos, ohne die Möglichkeit Besitztümer zu schützen. So ähnlich würde es sich in einem unsegmentierten Netzwerk verhalten. Erst durch die Schaffung von Zonen und Übergängen wird zonenübergreifende Kommunikation eingeschränkt und Assets innerhalb der Zonen können geschützt werden.

In unserem Netzwerk würden wir also zunächst zwischen dem IT-Layer und dem OT-Layer unterscheiden. In der Burg befinden sich IT- und OT-Layer im Innern der Burg, sind aber voneinander getrennt durch Wege, Mauern, Tore und Wachen - einer Vielzahl an Kontrollmechanismen. Außerhalb der Burg befindet sich das unsichere Internet, welches durch das Burgtor (Firewall) nur kontrolliert hereingelangt. Als Übergang zwischen den beiden Hauptbereichen IT und OT befindet sich die demilitarisierte Zone (DMZ), in welcher sich Dienste befinden - z.B. Schmied, Handwerker, Stall, Türme mit Wachen - (MES, Managementserver, Remote Control, Monitoring), die von beiden Bereichen in Anspruch genommen werden.

Im nächsten Abschnitt werden wir uns die einzelnen Bereiche des Netzwerks und der Burg genauer anschauen sowie auf Basis der Grundprinzipien der IEC 62 443 unser Netzwerk segmentieren und schützen.

In 3 Schritten zur Netzwerksegmentierung

Nachdem wir die Grundlagen verstanden haben, widmen wir uns nun der eigentlichen Segmentierung unseres Netzwerkes. Um ein Produktionsnetz zu segmentieren, ist es wichtig, die Prozesse in der Automation zu verstehen. Es reicht nicht aus, die IT-Standards für die Segmentierung eines Office-Netzes zu verwenden. Wie das gelingt erklären wir nun in 3 Schritten.

1.Schritt: Das Assessment

Der erste Schritt für eine erfolgreiche Netzwerksegmentierung ist ein „Assessment" des Netzwerks. Wir untersuchen also unser Netzwerk und stellen uns folgende Fragen:

- Wie sieht der zugrundeliegende Automationsprozess aus?
- Welche Assets gehören zu welchem Automationsschritt?
- Welche Netzwerkteilnehmer gibt es?
- Welcher Netzwerkteilnehmer kommuniziert mit wem?
- Was muss geschützt werden?

Wenn wir nicht genau wissen, welche Netzwerkteilnehmer im Netzwerk existieren, sind unsere ergriffenen Maßnahmen nicht effizient oder schlagen sogar fehl. Deshalb sind Informationen von elementarer Bedeutung. Als Grundlage dafür eignet sich ein **Anlagenerfassungsblatt** und eine **Anleitung zur Erstellung einer Kommunikationsmatrix**. Als Faustregel gilt: Umso besser und aussagekräftiger das Assessment ist, desto reibungsloser läuft die Netzwerksegmentierung. Dieser erste Schritt sollte deshalb nicht unterschätzt werden.

Doch wo fängt man an?

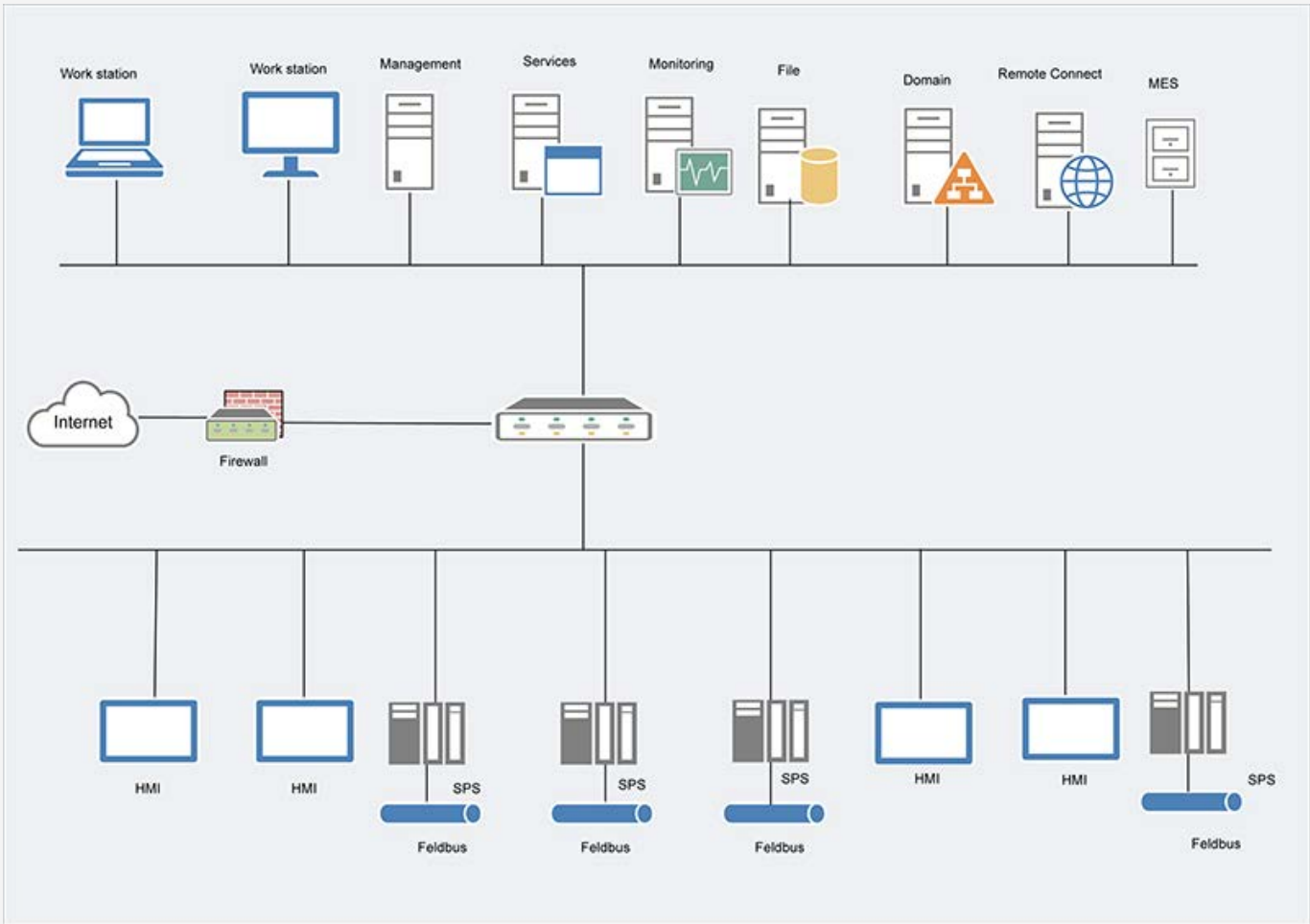
HWI TIPP für eine Vorgehensweise zum Assessment

- **Definieren Sie einen Lead als Projektverantwortlichen** und bringen Sie alle beteiligten Personen zusammen, um ein Verständnis für das Vorhaben zu schaffen. Fragen müssen im Vorfeld definiert werden und die wichtigsten Informationen aus den Gesprächen sollten mitgenommen werden.
- **Nutzen Sie Dokumentation, die schon da ist.** Als Tool zur Dokumentation eignet sich z.B. „Visio" für den schnellen Start und die Aufnahme der Informationen aus den Gesprächen und aus den bestehenden Dokumentationen. Informationen lassen sich aus Visio in ein .csv Format exportieren und in Datenbanken einpflegen.
- Die Verwendung von automatisierten **Tools** (z.B. Anomalieerkennung) ist erst ratsam, wenn das Netzwerk segmentiert ist, da sie erst dann am besten funktionieren.

Anlagenerfassungsblatt: https://hwi-it.de/anlagenerfassungsblatt/
Anleitung zur Erstellung einer Kommunikationsmatrix: https://hwi-it.de/netzwerkaufnahme-leicht-gemacht/

Der Netzplan zur Visualisierung des Netzwerks

Das Ergebnis eines ordentlichen Assessments sollte ein Netzplan sein. Dieser hilft das ganze Netzwerk zu visualisieren und die Gegebenheiten zu erfassen. In einem Automationsnetz finden wir häufig Elemente wie Steuerungen, Engineeering Stationen, SCADA Systeme, etc. Ein fertiger Netzplan könnte so aussehen:



Durch den Netzplan verstehen wir die Prozesse im Netzwerk und die Abhängigkeiten untereinander noch besser. Für die Segmentierung ist dieser Schritt deshalb besonders wichtig.

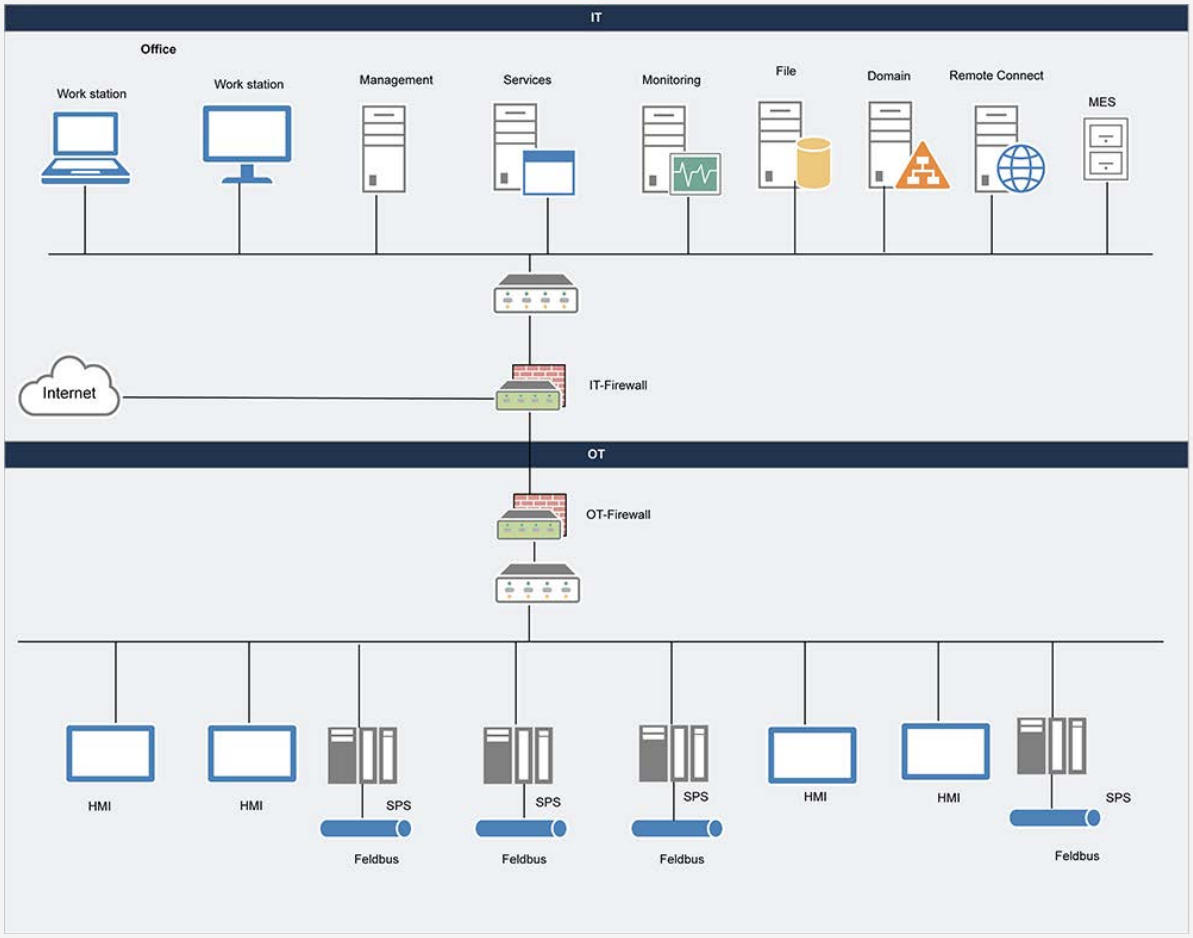
2. Schritt: Die Planung

Nachdem wir den Netzplan fertiggestellt haben, können wir nun mit der eigentlichen Segmentierung beginnen. Hier gehen wir nach der Norm IEC 62 443 Schritt für Schritt vor.

Physische Trennung von IT und OT

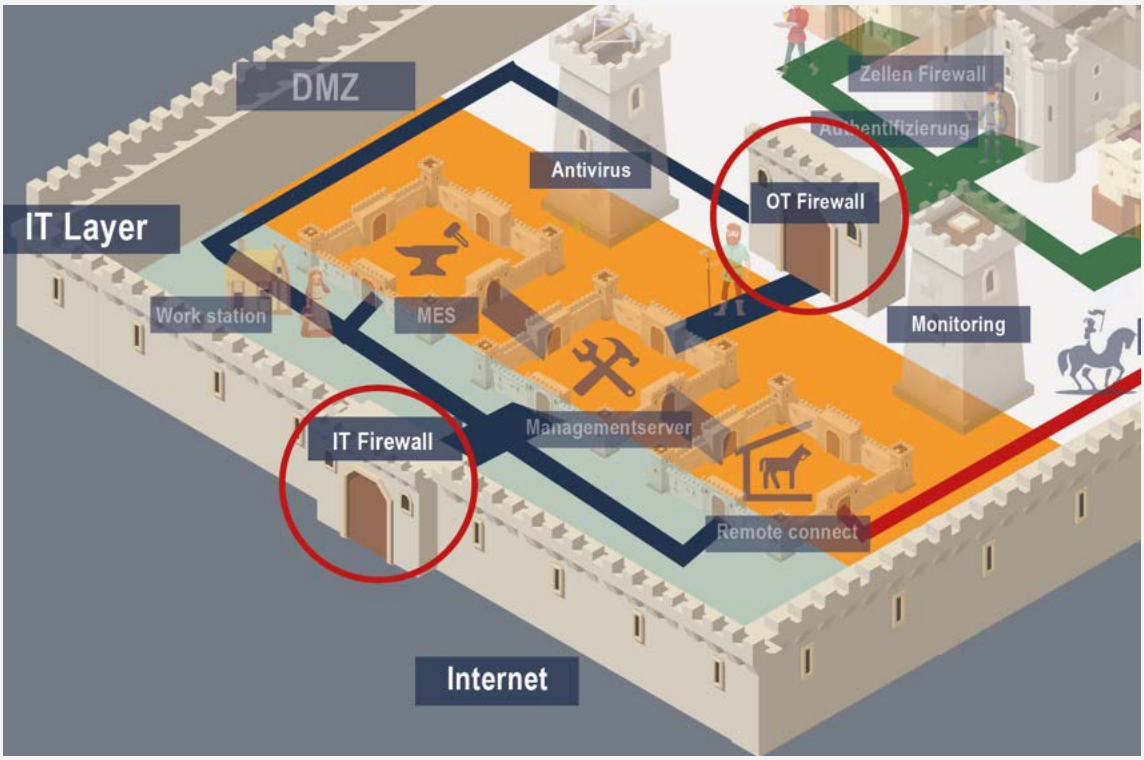
Unser erster Schritt ist die physische Trennung zwischen den beiden Layern IT und OT. Dieser Schritt ist essenziell. Ziel ist es dabei die Nord-Süd Kommunikation zwischen dem IT und OT Layer unter Kontrolle zu bringen. Dafür verwenden wir Firewall-Funktionalitäten, die die zuvor ermittelten Kommunikationsbeziehungen von und nach IT-Welt steuern aber auch verhindern und minimieren, vor allem in Bezug auf unbekannte / ungewollte Kommunikation. Vorteile von Firewall- Funktionalitäten an dieser Stelle sind u.a.:

- höhere Performance durch minimierte Kommunikation
- vereinfachtes Troubleshooting
- minimierte Verbreitung von unerwünschter Kommunikation



Die Firewall-Trennung führt außerdem dazu, dass die Geräte dem OT-Layer zugeordnet werden und dadurch ein unabhängiger Betrieb des gesamten OT-Layers, aus System- Geräte- und Organisationssicht, möglich wird. Die Aufteilung des Verantwortungsbereichs und der autonome Betrieb sind entscheidende Vorteile, die durch die Segmentierung entstehen. Wie unabhängig ein Betrieb sein soll, entscheiden die Anforderungen z.B. an Datenflüsse. Die Zusammenarbeit zwischen IT und OT ist daher wichtig, auch wenn wir eine physische Trennung vornehmen.

Wenn wir nochmal auf unsere Burg-Analogie zurückkommen, entsprechen die Firewall-Funktionalitäten den Mauern und Toren in der Burg, die die verschiedenen Bereiche voneinander trennen - z.B. das Nobelviertel (OT) vom Handwerksviertel (IT) und außerdem wird die Burg nach außen abgesichert mit einem Tor vor unkontrolliertem Eindringen (Internet).



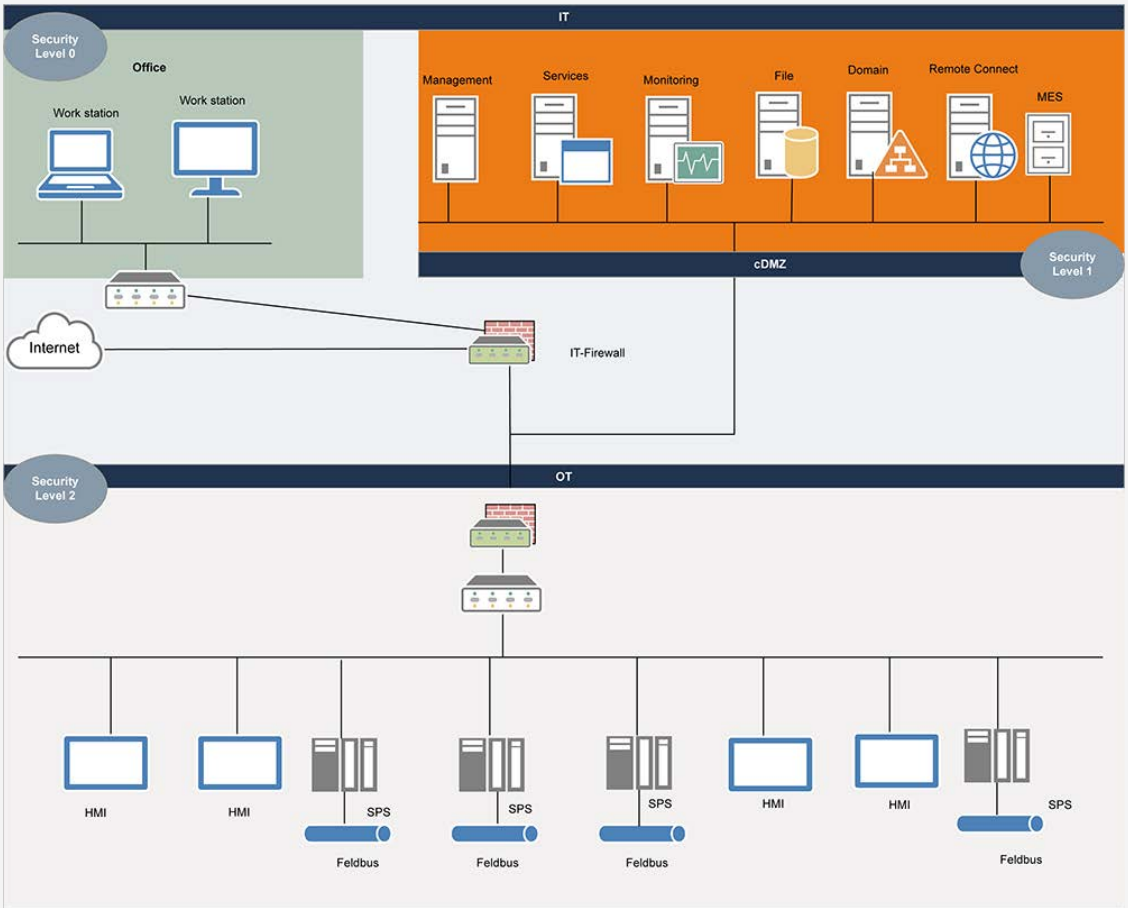
Zonen und Übergänge

Nachdem wir IT und OT physisch getrennt haben, müssen wir uns als nächstes mit Zonen und Übergängen beschäftigen. Wie bereits zu Beginn erwähnt, sind Sicherheitszonen und Übergänge eine Grundlage der Norm. Mithilfe einer Risikoabschätzung werden die Sicherheitszonen definiert. Eine Sicherheitszone stellt ein Security Level dar, und die jeweiligen Assets in der Zone haben einen bestimmten Schutzbedarf. Die Übergänge wirken als Kontroll- und Sicherheitsmaßnahmen und die Security-Level müssen sich laut der Norm durch einen Übergang verändern.

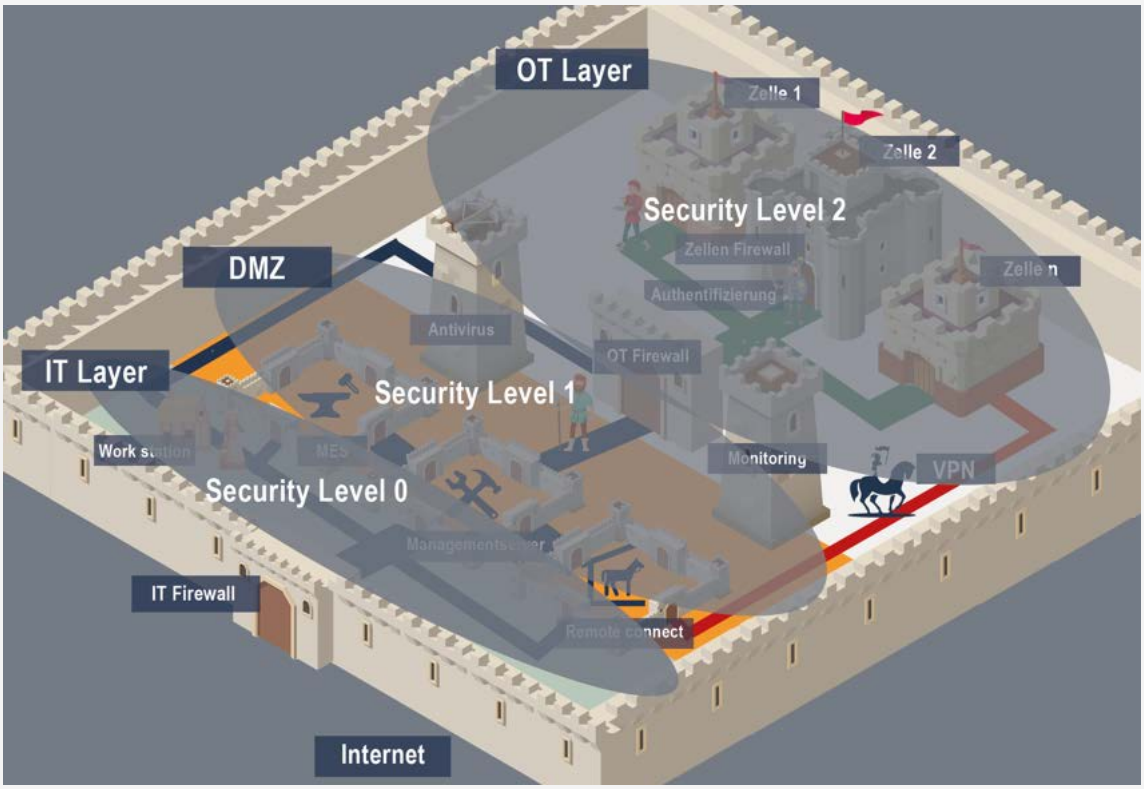
HWI TIPP zur Bestimmung von Zonen und Übergängen

- Den gesamten **OT-Layer mit einem höheren Security Level als den IT-Layer** bewerten. Zum Beispiel:
  IT-Layer = Security Level 0
  OT-Layer = Security Level 2
- Damit nehmen wir an, dass der OT-Layer unsicherer ist, und einen höheren Schutzbedarf benötigt. Diese Annahme ist durchaus legitim, wenn wir betrachten, welche Komponenten mit welchen Laufzeiten im OT-Layer vorhanden sind.
- Dazwischen schaffen wir einen **Übergang**, den wir **Corporate DMZ** (cDMZ= Demilitarisierte Zone) nennen, mit dem Security Level 1

Die cDMZ ist ein sehr wichtiges Konzept für die Konvergenz zwischen IT und OT und den echten IT-Betrieb im Automationsbereich. Mit der Einteilung in drei Sicherheitslayer haben wir uns sehr viel Arbeit abgenommen, denn eine Definition des Risikos für jedes einzelne Asset im Netzwerk ist wenig praktikabel und handhabbar. Dadurch würden wir uns selbst im Assessment ausbremsen. Denn auch während eines Netzwerksegmentierungsprojektes muss das Produktionsnetz verfügbar sein – die Produktion muss in der Lage sein zu produzieren. Mit der einfachen Definition der cDMZ nehmen wir uns hier deshalb einiges an Arbeit ab und schaffen einen Bereich für spätere IT-Betriebsmodelle.



Bezogen auf die Burg befindet sich der IT-Layer am Eingang der Burg und der OT-Layer im hinteren Teil der Burg – sozusagen der wichtigste Bereich der Burg (z.B. die Schatzkammer), den es unbedingt zu schützen gilt. Beide Bereiche sind durch einen Übergang (DMZ) voneinander getrennt – in diesem Bereich befinden sich verschiedene Dienste, die von beiden Bereichen in Anspruch genommen werden (Schmied, Stall, Handwerker). Dieser Bereich verknüpft also beide Viertel miteinander und ermöglicht einen kontrollierten Übergang vom IT-Layer zum OT-Layer.



Single-homed Assets

Single-homed Assets sind essenziell für einen stabilen Netzwerkbetrieb. Doch was verbirgt sich eigentlich dahinter? Achtung: Single-homed Assets dürfen auch weiterhin über zwei Netzwerkkarten verfügen, diese dürfen allerdings nicht mehr an unterschiedliche Security Levels angebunden sein. In der Praxis sähe das so aus, dass ein Device auf Security Level 2 in den Layer 2 spricht und gleichzeitig in den Layer 0. Dadurch würden wir unser zuvor erstelltes Konzept der Sicherheitsmaßnahmen untergraben. Es ist aber durchaus möglich mehrere Geräte zu haben mit mehreren Netzwerkkarten, die in mehrere Maschinennetze konfiguriert sind. Hier hilft uns im nächsten Schritt das Prinzip der Zellenbildung.

HWI TIPP zu Single-homed Assets

- Eine Zellenfirewall, die eine Zelle und die Netze dahinter trennt bzw. schützt, gilt aus Sicht des Netzwerks als Single-homed Asset.

In unserer Burg gilt eine Wache, die ein Viertel und die Bereiche dahinter schützt, als „Single-homed asset“, denn sie verhindert, dass ein Viertel aus einer Sicherheitszone unkontrolliert für eine andere Sicherheitszone geöffnet ist.

Zellen

Für die Zellenbildung gibt es keine einheitliche Vorgehensweise, dadurch gehört es auch zu einem komplexen Schritt des Segmentierungsprozesses. Laut Norm ist hier die Basis das Sicherheitslevel. Hier gibt es allerdings einige Stolpersteine, die man vermeiden sollte. Ein Beispiel: Wir haben in unserem OT Netzwerk drei Windows XP PC's, die einen Internetanschluss benötigen - an dieser Stelle das Synonym für „unsicher". Die PC's haben den gleichen Schutzbedarf und sind demnach auf dem gleichen Sicherheitslevel – z.B. Level 4. Man könnte sie also in einer Zelle zusammenziehen. Aus Sicht der IT ist das eine sehr legitime Vorgehensweise – aus Sicht der OT ist es aber kaum umzusetzen. Denn damit würden wir die Komponenten netzwerktechnisch aus Ihren Prozessschritten reißen. Die Folge wäre eine enorme Arbeit im Troubleshooting und eine unnötige Komplexität – die sich negativ auf die Sicherheit auswirkt.

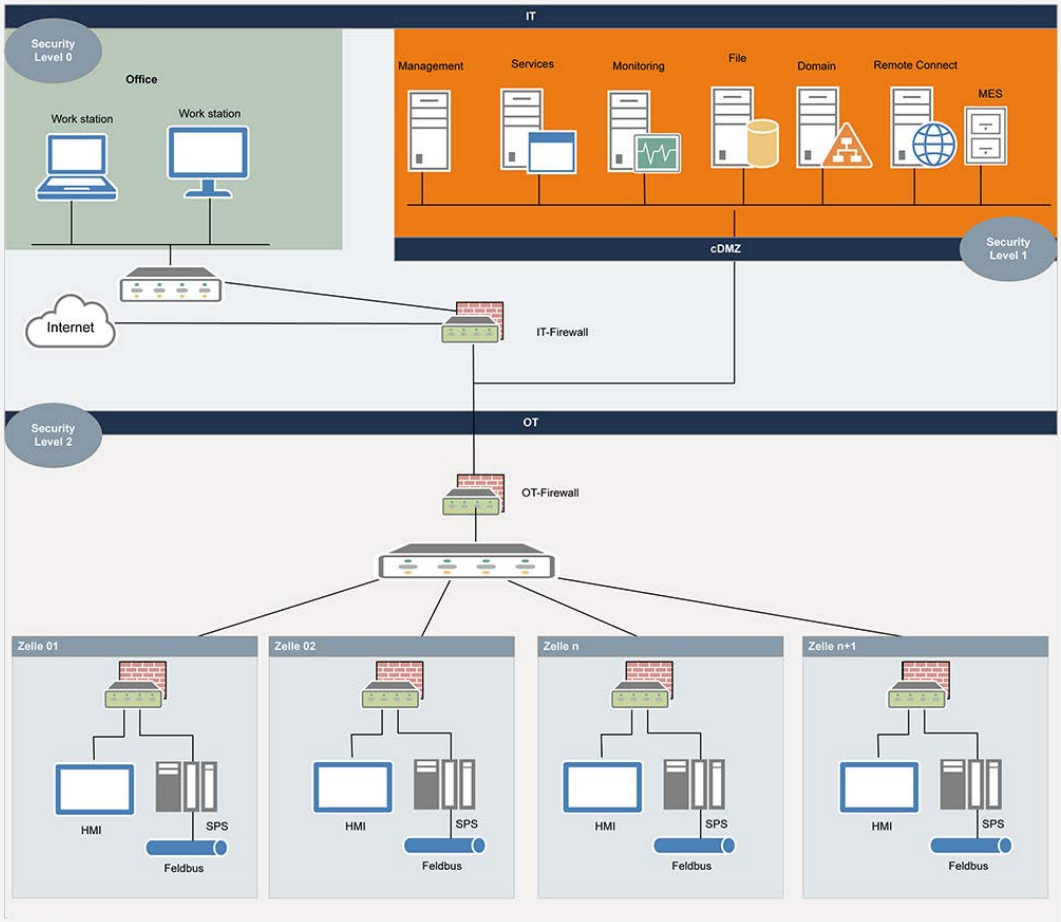
Aber wie sollten wir bei der Zellenbildung dann vorgehen?

Mögliche Vorgehensweisen:

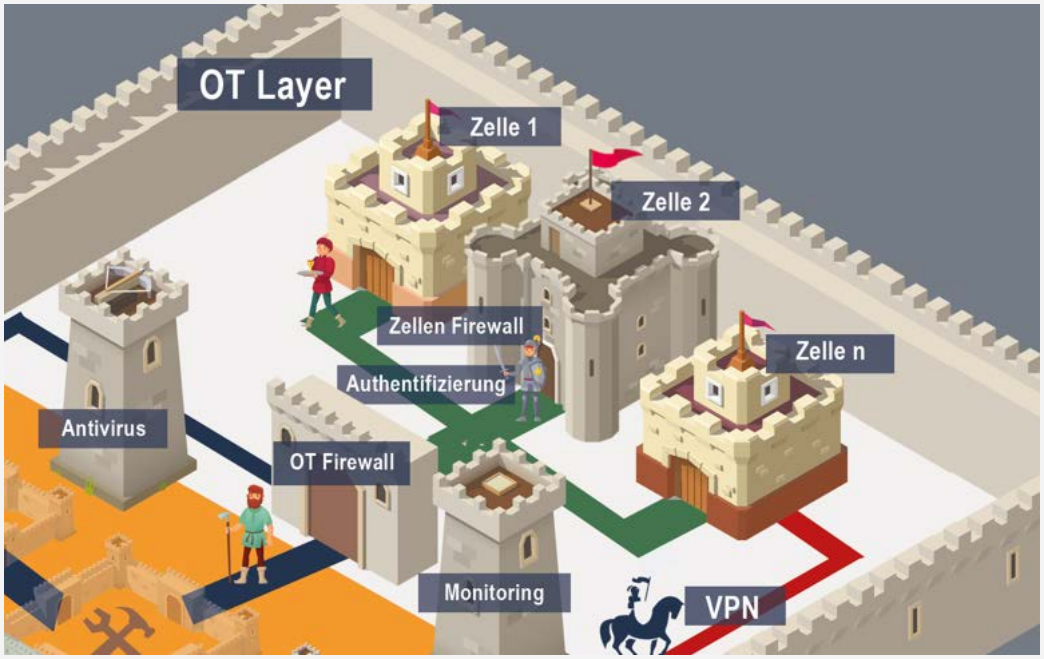
- Nach funktionaler Gruppierung: zusammenhängende Teile der Anlage werden in Zellen segmentiert
- Nach Zusammenführung von Überwachungs- und Steuerungselementen (z.B. alle HMI's in einen Bereich inklusive Controller)
- Nach Zugriffen: Ähnliche Zugriffsarten auf ähnliche Datenbanken oder Historians
- Nach Fernwartungszugängen (z.B. Fernwartungszugang nur in einen Zellenbereich möglich)
- Nach eingesetzten Protokollen (Gerade bei Performance relevant)
- Nach der Wichtigkeit für den Geschäftsprozess

HWI TIPP zur Definition von Zellen

- Immer passend zur Anlagenstruktur segmentieren, denn dadurch wird die Komplexität niedrig gehalten
- Einzelne Prozessschritte bilden Zellen
- Dann High-Potentials (bspw. Windows XP PC's mit Internetanschluss) ansehen
- Hinterfragen von Kommunikation (Ist ein Internetanschluss an einem PC in der Produktion notwendig?)
- Schaffung von gesonderten Sicherheitsmaßnahmen, z.B. durch Firewall vor einem Gerät, Netzwerkdiode oder Maßnahmen auf dem Gerät selbst



In unserer Burg befinden sich die Zellen im hinteren Teil - dem Nobelviertel. Hier wohnt der Burgherr mit seiner Familie und in separaten Gebäuden (Zellen) die Angestellten. Der Thronsaal ist beispielweise die wichtigste Zelle mit dem höchsten Schutzbedarf - hier ist zusätzlich zum Tor noch eine Wache vorhanden. Über einen "Geheimweg" (VPN) kann dem Burgherr schnell und unkompliziert ein Pferd zur Verfügung gestellt werden. Dieser Weg führt vom Stall (in der DMZ) direkt zu einer Zelle im Nobelviertel.



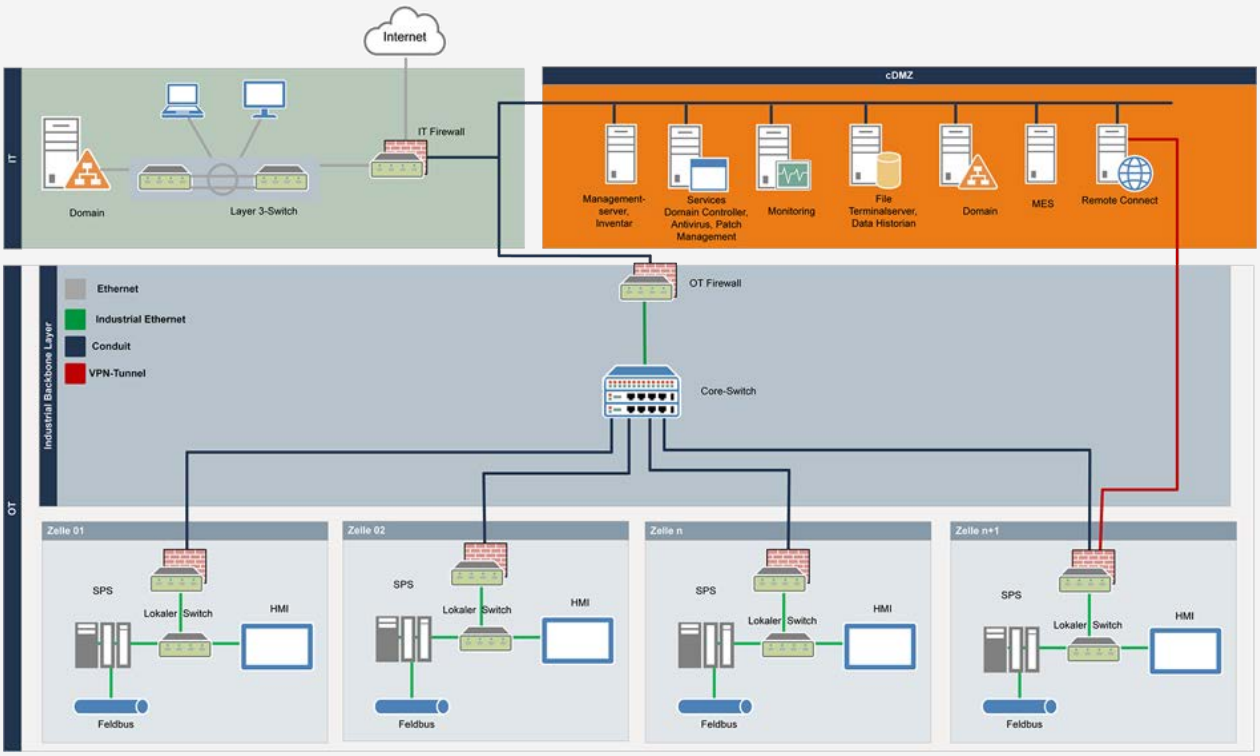
Mehrwert der Zellenbildung:
Durch die physische Trennung von IT und OT haben wir die Nord-Süd Verbindung kontrolliert, mit der Zellenbildung kontrollieren wir nun die Ost-West Verbindung. Laut der Norm steht Verfügbarkeit an erster Stelle. Um diese gewährleisten zu können, schaffen wir mit der Zellenbildung eine Risikoeingrenzung bzw. Schadensbegrenzung. Für jede Zelle wird eingeschätzt, wie kritisch sie für andere Prozessschritte ist, und was passieren würde, wenn eine der Zellen fehlt. Ziel ist es, dass der Produktionsprozess durch den Ausfall einer Zelle nicht beeinträchtigt wird.

Zwei grundsätzliche Prinzipien werden durch die Kontrolle der Nord-Süd Verbindung und Ost-West Verbindung geschaffen:

1. **Least Privilege** (Standard in der IT-Security): Die wichtigste Maßnahme bei höchstem Integritätsbedarf ist, die Rechte möglichst weit einzuschränken, d.h. es wird nur Zugriff genehmigt, wo er benötigt wird, denn das Nicht-Vorhandensein von Kommunikation ist der beste Schutz und sorgt für eine geringe Angriffsfläche bzw. ein geringes Störungspotenzial im Netzwerk.
2. **Least Route:** Der schnellste Weg von einem Asset zum anderen: Minimale Verzögerung bei der Datenkommunikation trägt insbesondere in einem Echtzeitnetz zu einer geringeren Auslastung der Übertragungswege und Kommunikationswege bei.

3. Schritt: Umsetzung

Das Ergebnis der Segmentierung muss nun in den Netzstrukturplan überführt und umgesetzt werden. In unserem Beispiel haben wir die einzelnen Zellen nach Prozessschritten segmentiert. Der fertige Netzplan sieht so aus:



In einer Zelle können dabei auch mehrere Produktions-Firewalls vorhanden sein, wenn es z.B. mehrere Maschinennetze gibt bzw. High-Potential-Assets, die es zu trennen gilt. Alle Zellen werden über automationsnahe Komponenten (bspw. ein eigener Switch pro Zelle) geführt, die dann in einem Industrial Security Backbone zusammenlaufen. Die Datenpakete der einzelnen Zellen werden kontrolliert in Richtung IT transferiert und gewährleisten so die Vernetzung mit der IT.

Nach der Umsetzung der Segmentierung sehen wir nochmal den **deutlichen Mehrwert der cDMZ** in der Kommunikation zwischen IT und OT:

- Sie ermöglicht die Umsetzung der Konzepte: Defense-in-Depth, Least Privilege und Least Route
- Eine strukturierte und kontrollierte Kommunikation wird vom Office Netz in den Automationsbereich bis zur Maschine (und umgekehrt) umgesetzt
- Eine klare Definition der Security Level und Abgrenzung untereinander
- Die Schaffung eines robusten Industrial Backbone, welcher die Zellen als Access Teilnehmer sieht
- Das Ermöglichen des Engineerings aus diversen Netzen bis an jede Maschine, sofern die Kommunikation erlaubt ist

Ein weiterer Vorteil ist, dass in der cDMZ das Vier-Augen-Prinzip vorherrscht, d.h. es gibt keine Kommunikation mehr, ohne, dass der jeweils andere Bereich (IT oder OT) Bescheid weiß und Konfigurationen vornimmt. Dort wo eine Konfiguration nicht möglich ist, bzw. wo eine Kommunikation zwischen den Sicherheitslayern unterbunden werden muss, kann die cDMZ verwendet werden, um IT-Komponenten zu platzieren, die in andere Netzwerke zugreifen können (z.B. Proxy Server, Edge-Computing Devices).

Generell ist jede Netzwerksegmentierung individuell und anlagenspezifisch durchzuführen. Dennoch sind die Schritte, die wir durchgeführt haben, ein wichtiger Bestandteil jedes Segmentierungsprojektes. Sie können wie folgt zusammengefasst werden:

- Kategorisierung auf Basis von Sicherheitslevels
- Erstellung einer Zellenstruktur, die jederzeit um weitere Zellen erweitert werden kann
- Erstellung der cDMZ als Bereich, in dem Komponenten für verschiedene Use Cases platziert werden können.

Ausblick: Was ist nach der Segmentierung zu beachten?

Unser Netzwerk ist nun ordentlich segmentiert, aber was dann?

Nach der Segmentierung ist vor dem Betrieb.

Mit der Umsetzung der Segmentierung ist es noch nicht getan. Wichtig ist jetzt die Entwicklung eines Betriebskonzeptes. Denn durch die Segmentierung ist einiges an neuer Hardware hinzugekommen, die verwaltet werden muss. Fragen wie -

- Wer hält die Hardware aktuell?
- Wer ist zuständig für Troubleshooting?
- Wer prüft Sicherheitslücken?
- Wer überwacht die Kommunikation im Produktionsnetzwerk?
- Wer ist für die Bereiche verantwortlich?
- Ist der Betriebsverantwortliche für die einzelnen Prozessschritte auch gleichzeitig verantwortlich für die Zelle?

- müssen unbedingt geklärt werden. Es wird definitiv eine Verschiebung von Betriebsverantwortung geben und gegebenenfalls auch Tätigkeiten in Feldern, wo es sie vorher nicht gab. Aus diesen Gründen sind Betriebskonzepte wichtig in der Organisation und in der Technik.

Was unbedingt vermieden werden sollte, ist nur ein reiner Austausch der Hardware und diese wie gehabt 10-15 Jahre laufen zu lassen. Denn so würden wir die Probleme, die wir eigentlich lösen wollten, nur verschärfen. Deshalb ist mit der Netzwerksegmentierung auch ein guter Zeitpunkt den Betrieb zu organisieren und festzulegen. Nachdem die Basis geschaffen wurde, sollte auch IT-Sicherheit in die Automation integriert werden. IT-Sicherheit muss ganzheitlich betrachtet werden und ist durch die Netzwerksegmentierung und die Einbeziehung des gesamten Netzwerkes nun noch besser möglich.

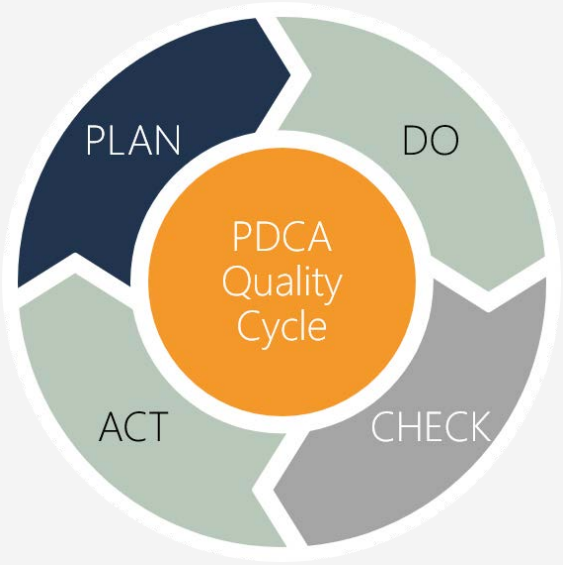
Durch die Umsetzung von IT-Sicherheits-Maßnahmen sichern wir uns gegen die anfangs erwähnten Bedrohungen für das Produktionsumfeld ab und gewährleisten die Schutzziele der Produktion:

1. Verfügbarkeit der Produktionsdaten
2. Datenintegrität
3. Vertraulichkeit von Informationen

Sicherheit ist aber kein statischer Zustand, der anhält, wenn er einmal erreicht wurde. Durch die Weiterentwicklung von Geschäftsprozessen, Infrastrukturen, rechtlichen Rahmenbedingungen und das Auftreten von neuen Schwachstellen ist es zwingend notwendig, IT-Sicherheit dauerhaft aufrechtzuerhalten und kontinuierlich zu verbessern. Eine mögliche Vorgehensweise, die auch die IEC 62 443 vorschreibt, ist der „Plan-Do-Check-Act" (PDCA)-Zyklus. Innerhalb dieses Zyklus sollten Bedrohungen und Auswirkungen eines potentiellen Angriffs fortlaufend bewertet werden und dann mit entsprechenden Maßnahmen darauf reagiert werden.

1. Planen (Anforderungen und Risiken)
2. Ausführung (Realisierung)
3. Prüfen (Messung und Validierung)
4. Anpassen (Verbesserung)

Durch die Anwendung dieses kontinuierlichen Verbesserungsprozesses erhält unser Netzwerk immer den bestmöglichen Schutz.



Über HWI IT

Als IT-Integrator hilft HWI IT Unternehmen komplexe IT-/OT-Projekte umzusetzen, Know-how aufzubauen und ihre Wettbewerbsfähigkeit zu stärken, durch die (cyber-) sichere Integration von IT in Automationsprozesse.
Durch unser umfangreiches Know-how im Bereich Netzwerk und unser Verständnis für Automationsprozesse in der Industrie gelingt es uns die Sicht der IT und der OT zu verknüpfen, die Lücke zu schließen und für beide Bereiche die perfekte Lösung zu finden.

Mit diesem Leitfaden wollten wir Ihnen einen Einblick in die Netzwerksegmentierung geben. Damit sind sie ausgerüstet für die ersten Schritte Ihres Segmentierungsprojektes. Sollten Sie dennoch Unterstützung bei der Umsetzung benötigen, helfen wir Ihnen gerne weiter! Wir freuen uns über Ihre Kontaktaufnahme.

Das sagen unsere Kunden

„Inzwischen haben wir ein neues Netzwerkkonzept implementiert, was bessere Perfomance bietet, die Zugriffe absichert, die Office-IT anbindet, die Virtualisierung sicherstellt und uns letztlich zukunftssicher macht."
Adriano Pederiva (Leiter Automatisierung, Badische Staatsbrauerei Rothaus AG)

„Die konkreten Handlungsempfehlungen auf Basis der IEC Norm 62443 haben uns hinsichtlich Strategie und Technologie weit vorangebacht."
Roland Siefermann (Leiter System- und Netzwerkadministration, Progress-Werk Oberkirch AG)

„Durch die Zusammenarbeit mit HWI IT, denken wir bei Anforderungsgrößen nicht mehr in Systemen, sondern in Prozessen."
Matthias Bürkle (Production Operations Technics, Biologische Heilmittel Heel GmbH)

Impressum

HWI IT GmbH
Im Kreuzfeld 2
79364 Malterdingen
https://hwi-it.de/
info@hwi-it.de

Registergericht: Amtsgericht Freiburg
Registernummer: HRB 713674

Geschäftsführung:
Holger Wiedel

Redaktionell verantwortlich:
Christina Ho

Version 1.0