MALAXIT
The Power of Networking

IT Security Standards in der Strombranche – eine Auswahl

Die folgenden Bereiche / Funktionsblöcke können in dedizierten physischen oder logischen Zonen sein, müssen dies aber nicht:

Das **Internet** ist unabdingbar, typischerweise werden auch einige Cloud Services genutzt.

In der **Office-IT** Umgebung befinden sich die klassischen Applikationen für die Büroautomation: Email, SAP usw.

In der **Business-OT** Umgebung befinden sich die SCADA Umgebung und die Business- Applikationen. Dies beinhaltet in der Regel auch den Leitstand.

In den **Unterwerken** befinden sich die Komponenten welche die Schalter ansteuern und die Leistungen und Flüsse messen.

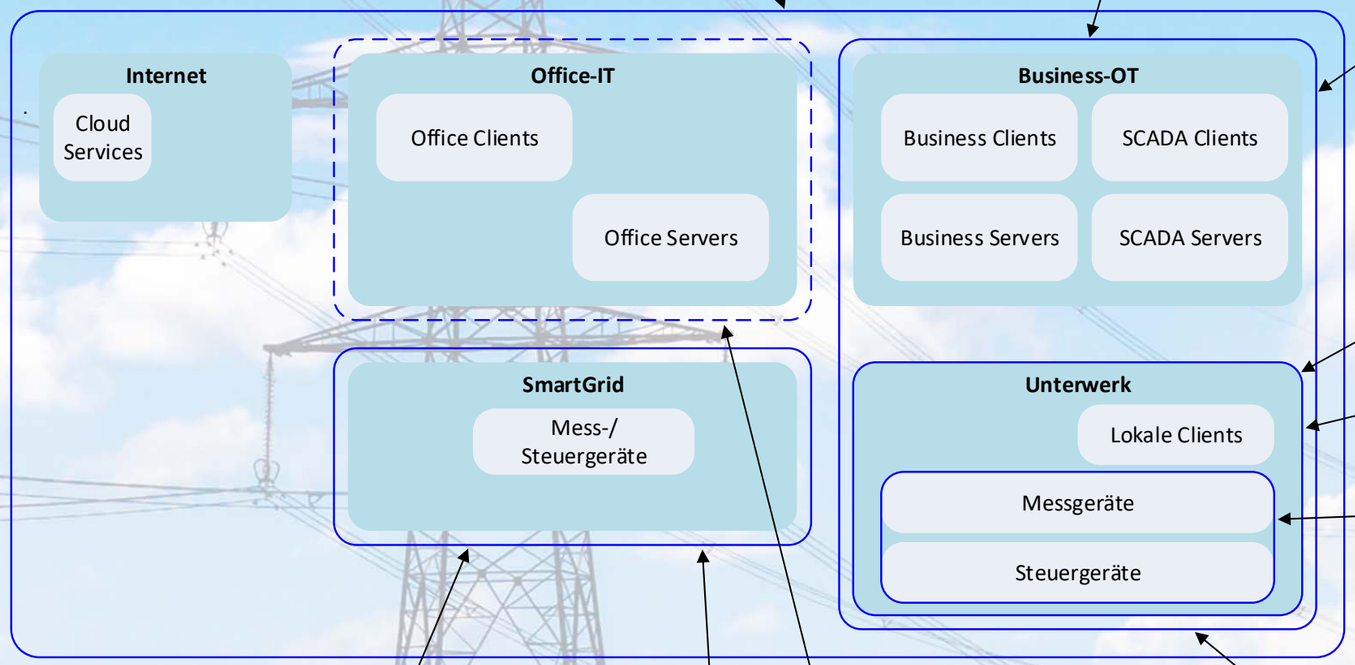
In der **SmartGrid**-Umgebung befinden sich die Infrastruktur und die Netzwerke / Verbindungen für Smart-Meters sowie die entsprechenden kleineren Anschlüsse.

ISO 27001/27002
Definiert ein Set von Policies und Massnahmen die in der IT implementiert werden sollen um die Sicherheit und Verfügbarkeit sicherzustellen.
Seit der Version 2013 wird auch das Involvement vom Firmen Management (Ebene CEO) und dessen Commitment vorausgesetzt und geprüft.
Der Standard ist allgemein, nicht spezifisch auf die Energie-Branche ausgerichtet.

ISO 27019
Baut auf ISO 27002 auf. Für SCADA- und Umsysteme werden zusätzliche Policies und Massnahmen definiert und bestehende vertieft.
Es wird nicht zuletzt auch auf IEC 62351 für die Implementation verwiesen.

NERC-CIP v5
Dieser US-Standard fokussiert auf die kritischen Systeme.
Grundlage für die Prozesse und Anleitungen bildet die Klassifizierung der Systeme in Kritikalitäts- Stufen. Es werden Massnahmen und Policies vorgeschrieben, welche für diese so klassifizierten Systeme definiert und umgesetzt werden müssen.

Hauptfokus des auf Stromversorger ausgerichteten Standards ist die OT Umgebung.



IEEE C37.240-2014
Cyber Security Massnahmen für Systeme in Unterwerken und für Substation Automation.
Der Standard baut auch auf NISTIR 7628 auf, ist aber eher eine Übersicht der Massnahmen die getroffen werden sollten.

IEEE 1402
Beschreibt die Anforderungen für physische und elektronische Security von Unterwerken.
Der Standard ist auf die Strombranche ausgerichtet, aber leider schon arg angegraut (letzter Update 2008).

IEEE 1686
Security Standard für IEDs (Intelligent Electronic Devices).
Dies ist eine Richtlinie, welche Cyber Security Anforderungen ein IED erfüllen soll.
Der Standard ist eher eine Hilfe zur Evaluation von IEDs, weniger eine Architektur- Richtlinie.

IEC 62351
Beschreibt umfassende Anforderungen für die Security:
- Daten Integrität / Unverfälschbarkeit (Integrity)
- Vertraulichkeit (Confidentiality)
- Verfügbarkeit (Availability)
- Unabstreitbarkeit (non-Repudiation)

Der Schwerpunkt liegt im OT Bereich, es sind aber auch Aspekte im IT Bereich in begrenztem Rahmen vorhanden.
Dies ist einer der wenigen Standards die auch auf die **Architektur** eingehen (62351-10).

ISO 30101
Beschreibt detailliert die Anforderungen an SmartGrid-Sensoren und -Netzwerk. Security wird nur am Rande behandelt.

NISTIR 7628
Beschreibt die logischen Interfaces der SmartGrid Infrastruktur und wie diese Interfaces und Verbindungen geschützt werden müssen (Cyber Security).
Dies beinhaltet die Anbindung an zentrale Systeme.

Ein mögliches Vorgehen:
Implementierung von ISO 27001/27002 über die gesamte Infrastruktur.
Anschliessend Vertiefung im OT Bereich auf der Basis von IEC 62351.
Als nächster Schritt Erarbeitung der Details im SmartGrid Bereich auf der Basis von ISO 30101.

Herausforderung: Eingliedern der bestehenden Systeme die nicht für Cyber Security entwickelt wurden.

Wir haben Erfahrung mit verschiedenen Standards. Gerne erarbeiten wir auch mit Ihnen zusammen das Vorgehen zur Umsetzung eines Standards und begleiten Sie dabei.

Kontaktieren Sie uns!

Malaxit AG
Länziweg 1
5034 Suhr

+41 62 842 48 70
info@malaxit.ch