GI-SECMGT

ICS - Security: Wer macht's und was muss gemacht werden?

Werner Metterhausen

von zur Mühlen'sche GmbH, BdSI

Sicherheitsberatung - Sicherheitsplanung - Rechenzentrumsplanung

Bonn, Berlin, Wien

Alte Heerstr. 1
53121 Bonn
Tel. +49 228 96293-0
Fax +49 228 96293-90
www.vzm.de

VON ZUR MÜHLEN-GRUPPE:

- **VON ZUR MÜHLEN´SCHE GmbH**
- **RZ-Plan - Mit Planung zur Sicherheit.**
- **Sicherheits-Berater - Sicherheit durch Information.**
- **SIMEDIA - Sicherheit entsteht durch Wissen.**

Geschäftsbereiche der VON ZUR MÜHLEN-Gruppe

Ein starker Verbund!

MIT SICHERHEIT MEHR SICHERHEIT®

Kennzahlen zur VON ZUR MÜHLEN-Gruppe

- **3 Gesellschaften**
  - VON ZUR MÜHLEN'SCHE (VZM) GmbH, BdSI
  - SIMEDIA GmbH – Seminare, Kongresse, Lehrgänge
  - TeMedia Verlags GmbH – Sicherheits-Berater
- **40 Mitarbeiter**

  Spezialisten unterschiedlicher Disziplinen mit komplexem übergreifendem Expertenwissen:
  - Architekten, Bauingenieure
  - Nachrichten- und Elektroingenieure, Haustechniker
  - Brandschutzsachverständige
  - Informatiker
- **1972**
  - VZM-Gründung als Einmannunternehmen durch Rainer von zur Mühlen
  - Heute in der Sicherheitsberatung über die längste Erfahrung verfügend

MIT SICHERHEIT MEHR SICHERHEIT®

Unsere Leistungsschwerpunkte

Sicherheitsberatung

Risiko- und Schwachstellenanalysen, Gutachten, Audits, Machbarkeitsstudien, Konzepte und Strategien, Management-Beratung, Coaching – von der Kurzkonsultation bis zum komplexen Großprojekt, z.B.

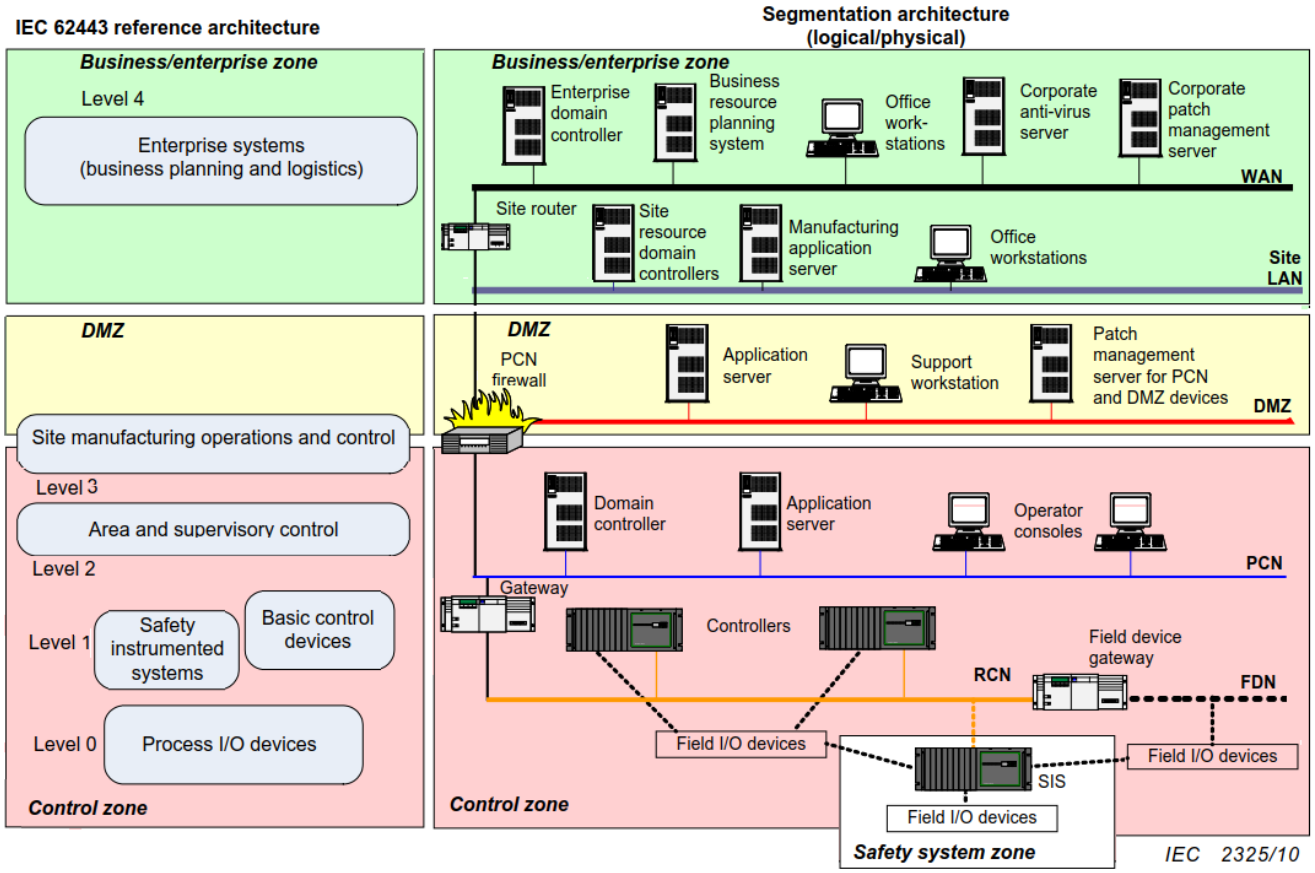
- Bauherrenberatung
- Objektschutz
- Informationssicherheit
- Business Continuity-, Notfall- und Krisenmanagement
- Werkschutz
- Expat Security
- …

MIT SICHERHEIT MEHR SICHERHEIT®

Problem

- ICS sind Teil einer „Anlage“ (Haus, Schiff, Kraftwerk usw.).
- Die Sicherheit von ICS (Industrial Control Systems) konfrontiert Hersteller und Betreiber mit einer „neuen Lage“.
- Wer Anlagen bauen kann, ist noch lange kein Experte für „Cyber-Security“. Liefert er eine sichere Anlage?
- Der Betreiber der Anlage muss die Anlage abnehmen und anschließend im Betrieb die Risiken der Anlage beherrschen. Ist er genügend „Cyber-Security-Experte“?

ICS



MIT SICHERHEIT MEHR SICHERHEIT®

These

- **{Cybersecurity | IoT-Security | ICS-Security} ist ein kulturelles / organisatorisches Problem**

Aus der „fast noch IT“-Welt

- Videoüberwachung und revisionsfeste Protokollierung mit 800 Kameras.

  800 Cams + Videoserver + NAS + …

- Kunde benötigt neues Release der Videoserver.

- Releasewechsel der Server erfordert Firmware-Update der Kameras.

- Der Hersteller / Anbieter wird mit Anforderungen konfrontiert, die er nicht „auf dem Zettel“ hat:

  Videokameras wartet man tagsüber

  vs.

  2-Schichten Betrieb revisionsfest dokumentieren

Kunde A

- **Mehrere Anlagen zur thermischen Abfallverwertung (Strom, Dampf)**

- **Zentrale Verwaltung mit üblicher IT-Landschaft**

MIT SICHERHEIT MEHR SICHERHEIT®

ICS im richtigen Leben (Strategie Kunde A):

Solange ihr mit eurer Büro-IT aus unserer Anlage rausbleibt, ist hier alles sicher.

- Interpretierbar als strenge Anwendung der ISO 27002 13.1.3:

13.1.3 Trennung in Netzwerken

Maßnahme

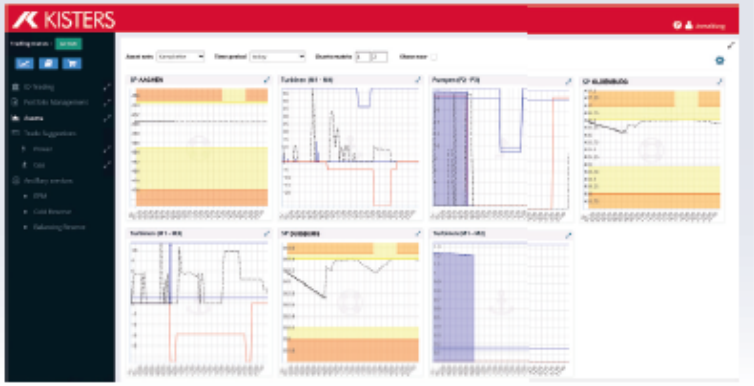
Informationsdienste, Benutzer und Informationssysteme sollten in Netzwerken gruppenweise voneinander getrennt gehalten werden.

Anleitung zur Umsetzung

Eine Methode zum Sicherheitsmanagement in großen Netzwerken besteht in deren Trennung in separate

Realität (Kunde A)

Handelsvorschläge für einen optimalen Stromhandel



Übersicht über die Assets (Turbinen, Pumpen, Kraftwerke ...)

Funktionen und Technik des Intraday-Cockpits

- Direkte Anbindung an die Börse (ComXerv-API)
- Direkte Anbindung an PFM-Systeme (z.B. BelVis PFM, eRisk) und Optimierungssysteme (z.B. ResOpt) mit durchgängigem Datenfluss
  - Kein Zeitverlust
  - Automatische Rückführung der abgeschlossenen Deals in das PFM-System (portfolio-/asset-scharf)
  - Direkte Aktualisierung der eigenen Handelsposition
- Übersicht der einzelnen Anlagen (Assets)
- **Live-Monitoring** der Handelspositionen und komfortable Live-Übersicht der Marktsituation
- Einfaches Einbinden von zusätzlichen externen Informationen und Daten, z.B. Marktinformationen, Prognosen, Wetterinformationen, Handelseinschränkungen usw.
- Zertifiziert durch die EPEX SPOT

Kunde A

- **Ein wenig tiefer geschaut:**
- **Die IT ist etwas beleidigt und hat kein ICS-Security Budget**
- **Die Produktion (die Anlagen) hat kein Personal und kein Budget für ICS Betrieb und ICS Security**

Kunde B

- Bau und Betrieb von Anlagen zur Wärme-/Kälteerzeugung
- Die IT von Kunde B ist „Office-IT“
- Die Beschaffung aller Anlagenkomponenten incl. ICS lag bei den vier Niederlassungen

Niederlassungs-IT

- JumpServer: RDP Zugriff auf Windows-Server 2008
- ca. 30 Accounts
- Div. remote-access-Produkte
- Erreichbar: + 2000 „Anlagen“

- Win 2008 Patches? – Alle??
- Win 2008 Antivirus? – Kostenfreies Produkt

Aus der Nähe:

- **Auf Jumpserver vier Verzeichnisse (Regionen)**
- **Pro Verzeichnis viele Unterverzeichnisse**
  z.B.: `47506-KUNDENNAME-HE`
- **Darin Link auf die remote access Software**
- **Wie meldet sich der Mitarbeiter an?**

Denken Sie das Undenkbare!

Kunde C

- **Weltweit agierender Konzern (Bau und Betrieb von Energietechnik)**
- **Thema ICS Security seit 2008**
- **Konzernweite ICS Security Policy**
- **Weitere Dokumente zum Thema in konzerntypischer Fülle**
- **Anweisung landesspezifische ICS Richtlinie in Kraft zu setzen (2015)**

Richtlinien-Exegese:

- Die vom Konzern übernommene Reihenfolge der Kapitel erscheint eher zufällig
  Anlage = Planung – Errichtung - Betrieb
- Excel samt Excel Vorlage als Vorgabe zum Configuration- und auch Change Management ist weder zeitgemäß noch angemessen.
- Es werden Vorgaben gemacht, die fast den Vorgaben der Office IT entsprechen (Benutzermanagement, Passworte, WLAN, etc)
- Klug, auch Schlüssel-Personen in das Thema Obsoleszenz einzubringen

Zielgruppe der Richtlinie

- **Projektleiter / Anlagentechniker**

- **Die Vorstellung im Cyberland:**
  - Predictive maintenance
  - Ressourcenoptimierung

- **Die Realität in Neuland:**
  - Meldung per SMS
  - Rein in den Kombi und los zum Kunden

Einschätzung ICS Security 2019

- **Es gibt viel zu tun!**
- **Zuständigkeit für ICS klären**
- **ICS Security muss sich Inspiration bei der IT suchen (ISO 27k, ITIL, …)**
- **Es bleibt spannend!**

MIT SICHERHEIT MEHR SICHERHEIT®

Werner Metterhausen

von zur Mühlen'sche GmbH, BdSI

Sicherheitsberatung - Sicherheitsplanung - Rechenzentrumsplanung

Bonn, Berlin, Wien

Alte Heerstr. 1
53121 Bonn
Tel. +49 228 96293-0
Fax +49 228 96293-90

www.vzm.de