Wider den Blackout

Sicherheit für kritische Infrastruktur nach ISO 27001 und 27019

Dr. Friedrich Neurauter (TINETZ)

14. Information-Security-Symposium, Wien 2018

Inhalt / Agenda

I. Einleitung / Vorstellung

II. Umsetzungsprojekt ISO 27001 + 27019 TINETZ

III. Herausforderungen: IT- vs. OT-Sicherheit

IV. Erkenntnisse / Fazit / Lessons Learnt

V. Zusammenfassung / Ausblick

Dr. Friedrich Neurauter

- TINETZ-Mitarbeiter seit März 2014
- Ausbildung: Informatiker (UIBK)

03/2014	• Smart Meter Security (projektweit)
10/2016	• Informationssicherheitsmanager (unternehmensweit)

TINETZ-Tiroler Netze GmbH

- 100%ige Tochtergesellschaft der TIWAG-Tiroler Wasserkraft AG (Landesenergieversorger)
- Größter Verteilnetzbetreiber Tirols (> 500 MA)
- Auftrag:
  - Betrieb und Ausbau eines qualitativ hochwertigen und hochverfügbaren Stromnetzes
  - Integration von neuen, innovativen Technologien in den Netzbetrieb (Smart Meter etc.)

Assets und deren Absicherung

Zentrale Netzleitstelle

45 Umspannwerke, 4100 Trafost.
11.500 km Leitungen

Smart Meter
(ca. 220.000)

- Zentrale Betriebsführung (Leits
- Fernüberwachung und -steu
- Systemausfälle können gravie
- Aufkommen spezifischer Malware: In ashOverride
- Hohes Sicherheitsniveau notwendig

Einführung eines ISMS
nach ISO 27001 + 27019

Inhalt / Agenda

I. Einleitung / Vorstellung

II. Umsetzungsprojekt ISO 27001 + 27019 TINETZ

III. Herausforderungen: IT- vs. OT-Sicherheit

IV. Erkenntnisse / Fazit / Lessons Learnt

V. Zusammenfassung / Ausblick

Umsetzungsprojekt ISO 27001 + 27019

- **Projektziele**
  - Einführung eines ISMS nach ISO 27001 / ISO TR 27019
    - Die ISO TR 27019 beinhaltet für einzelne Kontrollziele EVU-spezifische Implementierungsempfehlungen
  - Geltungsbereich „Gesamt-TINETZ“ (alle Standorte, UWs)
- **Rahmenbedingungen**
  - Aufbauend auf Vorprojekt (Gap-Analyse)
  - TIWAG-Zertifizierung seit 2011 (IT- + Office-Umgebung)
  - Konzernweite Zertifizierung 10/2017 (Erstzertifizierung TINETZ + Rezertifizierung TIWAG)
  - Projektstart Q4/2016

Umsetzungsprojekt ISO 27001 + 27019

- Projektkernteam: 8 MA + 1 ext. Berater
- Aufwand intern: ca. 1600 h
  - Aufwand extern: ca. 400 h

Zertifizierungsprozess CIS	
1	CIS Initial Registration & Planning; Kundenregistrierung
2	CIS-System & Risk Review/ STAGE 1
3	CIS-Reporting / STAGE 1
4	CIS-Certification Audit/ STAGE 2
5	CIS-Reporting / STAGE 2
ZERTIFIKAT	

Aufgrund bestehender Zertifizierung von TIWAG
- konnten wesentliche Teile des TIWAG-ISMS übernommen werden (Richtlinien, Risikomanagement)
- war kein STAGE 1 Audit erforderlich

Zertifizierungsaudit / Ergebnis

- Termin: 16.-20. Okt. 2017
- 2 Auditoren (CIS) + interne Interviewpartner
- Urteil der Auditoren

  „Das gesamte ISMS wird effizient, schlüssig, normkonform und den Bedürfnissen der TIWAG und TINETZ bestens angepasst umgesetzt“
- TIWAG-Konzern ist erstes EVU in Österreich, das vollständig (inkl. Netz und Erzeugung) nach ISO 27001 zertifiziert ist

Inhalt / Agenda

I. Einleitung / Vorstellung

II. Umsetzungsprojekt ISO 27001 + 27019 TINETZ

III. Herausforderungen: IT- vs. OT-Sicherheit

IV. Erkenntnisse / Fazit / Lessons Learnt

V. Zusammenfassung / Ausblick

Kritische Infrastruktur – Operational Technology

- **Definition OT**
  - Hard- und Software zum Überwachen und Steuern von Prozessen in technischen Anlagen (z.B. ICS, SCADA)
- **Definition Kritische Infrastruktur**
  - Infrastrukturen, die eine wesentliche Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen haben und deren (Zer-)Störung schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung haben würde

Herausforderungen: IT- vs. OT-Sicherheit

- **OT Security = RSA** (not CIA);
  reliability, safety and availability
- **Systemausfall kann gravierende Folgen haben (Blackout)**
- **Trennung zwischen OT- und IT-Welt schwindet zusehends**
  - Kein Air-Gap mehr, OT-Netz ∞ IT-Netz ∞ Internet
  - Business-Enablement, Digitalisierung, Fernwartung
- **Viele Legacy Systeme**
  - Lange Gerätelebensdauer (10-20 Jahre)
  - Veraltete Systeme (end-of-support, end-of-life)
  - Proprietäre Systeme
  - Insecure by design

Herausforderungen: IT- vs. OT-Sicherheit

- **Viele Schwachstellen in OT-Komponenten**
- **Unverschlüsselte Kommunikation**
- **Klassische Sicherheitsmechanismen nur bedingt anwendbar**
  - **Software/Security Updates:**
    - Viel größere Zykluszeit, teilweise keine Patches verfügbar
    - Häufiges Testen von Updates auf (Betriebs-)Sicherheit ist aufwändig/teuer
  - **Gefahr von Ausfall kritischer Systeme durch:**
    - AV Scan (jedes Signatur-Update ist potenziell gefährlich: „false positives“)
    - Penetrationstests, Schwachstellen-Scan, Port Scan etc.
  - **Daher *defense in depth* wichtig:**
    - Physische Sicherheit/Objektsschutz (Zutritt, Video etc.), Perimeterschutz, Application Whitelisting + Firewalls, Anomalieerkennung (IDS)

Inhalt / Agenda

I. Einleitung / Vorstellung

II. Umsetzungsprojekt ISO 27001 + 27019 TINETZ

III. Herausforderungen: IT- vs. OT-Sicherheit

IV. Erkenntnisse / Fazit / Lessons Learnt

V. Zusammenfassung / Ausblick

Erkenntnisse / Fazit / Lessons Learnt 1/4

- **Ein ISMS kann nur funktionieren, wenn**
  - die Mitarbeiter von der Sinnhaftigkeit überzeugt sind
  - und die Richtlinien in der täglichen Praxis umsetzen (Security Awareness)
  - Daher ist die Unterstützung seitens der Unternehmens-leitung enorm wichtig
- **Implementierungsaufwand**
  - wäre ohne vorhandenes Risikomanagement + Synergien mit TIWAG-ISMS deutlich höher gewesen
  - kaum Mehraufwand bezüglich ISO TR 27019

Erkenntnisse / Fazit / Lessons Learnt 2/4

- **Die Norm lässt viel Interpretationsspielraum zu**
  - z.B. wird ein „*angemessenes*“ Risikomanagement gefordert, aber der Begriff „angemessen“ nicht genauer definiert; daher:
  - MA (intern oder extern) mit ISO 27001 Expertise nötig
- **Viel organisatorische, wenig technische Sicherheit**
  - Schreiben von Richtlinien und Begleitdokumenten
  - Initiieren von Prozessen (Risikomanagement, KVP)

Erkenntnisse / Fazit / Lessons Learnt 3/4

- **Es geht bei den Audits um:**
  - den Nachweis einer angemessenen ISMS-Umsetzung
  - Unterstützung und NICHT Darstellung von Schwächen um jeden Preis
  - Hinweise, die helfen Verbesserungen vorzunehmen, optimalere Lösungen darzustellen
- **Es ist empfehlenswert**
  - alle benötigten Unterlagen wie Dokumentationen, Nachweise und Beispiele aus den Abteilungen im Vorhinein zu sammeln (keine Zeit während Audit)

Erkenntnisse / Fazit / Lessons Learnt 4/4

- ***„Nach dem Audit ist vor dem Audit“***
  - Jährliche Überwachungsaudits durch CIS
  - Rezertifizierungsaudits im 3-Jahreszyklus
- ***„Keep it simple“***
  - Man sollte nicht versuchen, alles bis ins kleinste Detail zu regeln; die Richtlinien müssen auch auf ihre Einhaltung überprüft und bei Bedarf verbessert werden
- ***„Technology is hard, people are harder“***

Inhalt / Agenda

I. Einleitung / Vorstellung

II. Umsetzungsprojekt ISO 27001 + 27019 TINETZ

III. Herausforderungen: IT- vs. OT-Sicherheit

IV. Erkenntnisse / Fazit / Lessons Learnt

V. Zusammenfassung / Ausblick

Zusammenfassung / Ausblick

- **OT-Sicherheit != IT-Sicherheit**
- **Adäquates Sicherheitsmanagement**
  bei Energieversorgungsunternehmen auf Basis ISO 270xy
  - Solide Basis für Umsetzung DSGVO und NIS-Richtlinie
- **ABER: viele Legacy Systeme in kritischen Bereichen**
- **Blackout-Risiko**
  - Nicht nur durch Cyberangriffe / Hacker
  - Auch durch erneuerbare Energien (z.B. Sonnenfinsternis)
  - Überlastung der Netze durch E-Mobilität

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Friedrich Neurauter
TINETZ

14. Information-Security-Symposium, Wien 2018