
E-CONTROL
PROFITIEREN. WO IMMER SIE ENERGIE BRAUCHEN.

Netz- und Informationssicherheitsanforderungen an Betreiber Kritischer Infrastruktur – IKT-Risikoanalyse Elektrizität / Gas

RTR-Workshop

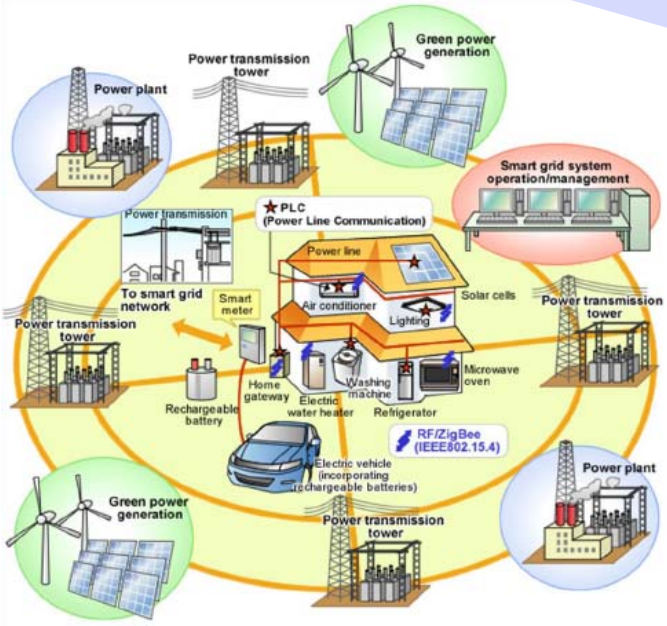
Mag. Philipp Irschik, MIM

Energie-Control Austria (E-Control)

28. Juni 2016

Die Transformation der Energiewirtschaft führt zu neuen Bedrohungsszenarien

- Das zukünftige Energiesystem wird..
  - **vielfältiger** (konventionelle und erneuerbare Erzeugungstechnologien)
  - **modularer und kleinteiliger** (Anzahl und Vielfalt von Marktakteuren steigt)
  - **dezentraler** (Einspeisung vermehrt auf Verteilnetzebene; „Prosumer“)
  - **multidirektionaler** (verstärkter multidirektionaler Strom- und Wertefluss)
  - **fluktuierender** (Integration von volatiler Erzeugung aus Erneuerbaren)
  - **flexibler** (Flexibilisierung der Nachfrage anstatt „Angebot folgt Nachfrage“)



- Zunahme an Marktakteuren, Vernetzung und **Komplexität** → Reaktion: **Automatisierung** von Prozessen und Auslagerung an Systemdienstleister
- **Einsatz von „intelligenten“ IKT-Lösungen** zur Steuerung und Regelung **nimmt zu**.
- Exogene sowie systemimmanenten Faktoren führen zu **neuen Bedrohungssituationen**

Mit der Zunahme an Komplexität steigt der Einsatz von “intelligenten” IKT-Lösungen

E-CONTROL

Makro-Trends
Technologischer Fortschritt

- Industrie 4.0
- Digitalisierung / “Smartifizierung”
- “24/7” Konnektivität
- Internet of Things (IoT)
- “Big Data”, “Smart Analytics”
- Prozess- und Rechenleistung
- Automatisierung, “Machine 2 Machine”
- etc.

Zunehmende
Systemkomplexität

- Demand Response
- Wettbewerbs- / Konsolidierungsdruck
- Zunahme der Marktakteure / “Prosumer” / Vernetzung
- Echtzeitbetrieb
- Multi-direktionale Systeme
- Systemstabilisierung / Volatilität
- Dezentralisierung / Erneuerbare Energieträger
- Standardisierung / Regulierung / Politische Veränderungen

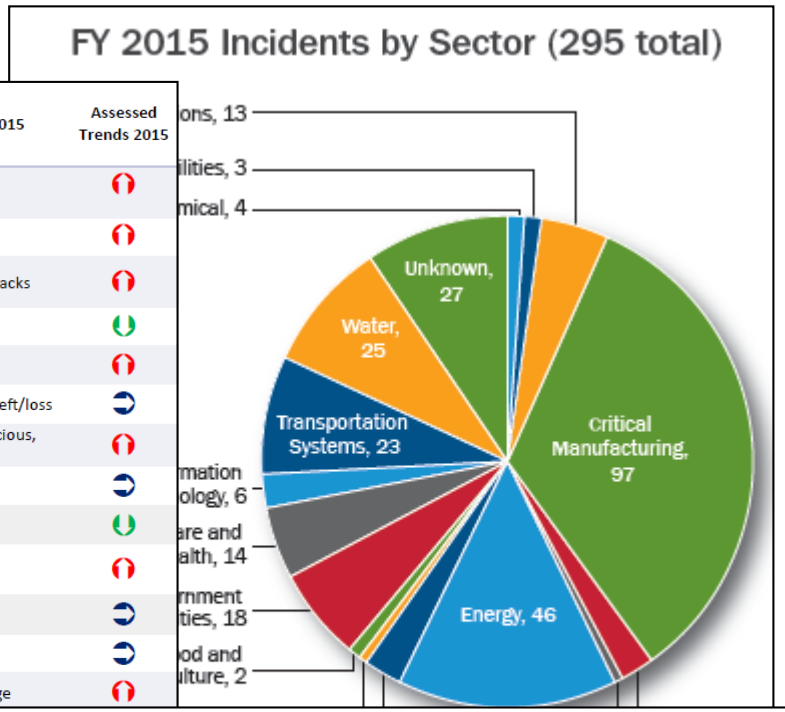
Neue Interdependenzen entstehen durch das Verschmelzen von Informations- und Betriebstechnologie.

Aktuelle Ereignisse zeigen die existierende Gefahr von intentionalen Cyberangriffen

E-CONTROL

- Unternehmen aus dem Energiesektor gehören (angeblich) zu den **weltweit bevorzugtesten Zielen von Cyberattacken**.
- Die **Frequenz, Schwere und Raffiness** von Cyberangriffen nimmt zu. Währenddessen steigen die **Kosten für IT-und Cybersecurity** konstant (Schätzung: $575 Mrd.).
- Die Anzahl von Cyberangriffen mit dem vorsätzlichen Ziel **physische Infrastruktur zu zerstören** und die **Versorgungs-sicherheit zu beeinträchtigen** steigt.

Top Threats 2015	Assessed Trends 2015
1. Malware	
2. Web based attacks	
3. Web application attacks	
4. Botnets	
5. Denial of service	
6. Physical damage/theft/loss	
7. Insider threat (malicious, accidental)	
8. Phishing	
9. Spam	
10. Exploit kits	
11. Data breaches	
12. Identity theft	
13. Information leakage	



Year	Country	Target	Business Sector	Incident Description
2016	Bangladesh	National Central Bank	Financial Services	cyber-heist - financial fraud
2016	Belgium	AFCN	Energy & Utilities	website defacement
2016	Germany	Hospital Provider	Health Care	network disruption
2016	Austria	FACC	Aeronautics	fake president fraud – financial fraud
2015	Ukraine	National Power Sector	Energy & Utilities	physical destruction of equipment
2015	UK	TalkTalk	Telecommunication	credentials and credit card details theft
2015	Germany	German Parliament	Public Administration	retrieval of information, espionage
2015	France	TV5 Monde	Media	network disruption, website defacement
2015	USA	Anthem Inc.	Health Care	medical-related data theft
2014	Japan	Sony	Media	extraction of intellectual property
2015	USA	AshleyMadison.com	Online Services	credentials and user access details theft
2014	Germany	Steel Mill [no name]	Heavy Industry	physical destruction of equipment

Quelle: European Union Agency for Network Security, 2015; ICS-CERT Jahresbericht 2015

Die Bedeutung von Cybersicherheit im Energiesektor beruht auf einer Reihe von Faktoren

E-CONTROL

- **Motivation hinter Angriffen** unterscheidet sich in der Regel von jenen in anderen Sektoren (Beeinträchtigung der Versorgungssicherheit)
- **Kritikalität des Energiesektors für die Gesellschaft** (Kaskadenwirkung)
- **Die signifikanten (volks-)wirtschaftlichen Kosten eines Stromausfalls**
- Breite Verwendung von teils **veralteten, proprietären, selbstgebauten Altsystemen**
- **Wenige "digital natives"**; **geringes Bewusstsein** für Cybersicherheit auf Ebene der Entscheidungsträger / des Managements
- **Lange Investitionszyklen und Schwierigkeit bei der technologischen Anpassung**
- Hohe **Abhängigkeit** von externen **Dritt- und Systemanbietern**
- **Paradigmenwechsel (Betriebs- und Ausfallssicherheit zu Angriffssicherheit)**

Das Diskussionsumfeld in Österreich

- **Betreiber kritischer Infrastruktur vermehrt Ziel von gezielten Cyberangriffen**
- **Start der flächendeckenden Einführung von Smart Meter** (2015) als eines der wichtigsten Projekte der österreichischen Energie- und Wirtschaftspolitik
- **Emotional geführte öffentliche Debatte** zu den Risiken von Smart Meter und dem Bedrohungspotential durch Cyberattacken (Datenschutz, Datensicherheit)
- **Zusammenwirken verschiedener nationaler und internationaler Prozesse:**
  - „Roll-Out“ von Smart Meter
  - Gesamtstaatlicher Lagebildprozess
  - Nationale Cyberstrategie (ÖSCS)
  - Beschlussfassung der NIS-RL & GDPR der EK
  - Umsetzungsinitiativen auf nationaler Ebene (z.B. Cybersicherheitsgesetz)
- **Nutzung von Synergien** zur realistischen Analyse und Bewertung von potentiellen Bedrohungen durch den zunehmenden Einsatz von IKT Systemen im Energiebereich

Relevante Diskussionspunkte für die Strategie aus Sicht der E-Wirtschaft

- Schaffung von Strukturen und Prozessen für den **Informationsaustausch zwischen Betreibern kritischer Infrastruktur, Behörden und Gesellschaft**
- Diskussionen über einen **adäquaten ordnungspolitischen Rahmen**
  - Meldeverpflichtungen
  - regulatorische Maßnahmen
  - freiwillige Selbstverpflichtungen
  - Definition von allgemeinen Mindestsicherheitsstandards
- **Sensibilisierung und Ausbildung von Sicherheitsbewusstsein**
- **Internationale Zusammenarbeit und branchenübergreifender Wissensaustausch**
- **Schutz kritischer Infrastruktur**
  - Definition von Mindesstandards für Cybersicherheit
  - Ausbau und Stärkung der Krisenkommunikation inkl. Meldepflicht bei Cyberattacken
  - Laufende Aktualisierung einer umfassenden Sicherheitsarchitektur bei systemrelevanten EVUs

Überblick über ausgewählte europäische und österreichische Rechtsakte und Initiativen

E-CONTROL

EPCIP
European Programme for Critical Infrastructure Protection
2006

APCIP
Austrian Programme for Critical Infrastructure Protection
(BM.I, 2008)
Identifizierung von ~400 Betreiber Kritischer Infrastruktur

Cyber-Security-Risikoanalyse Österreich
(KSÖ/BM.I)
2011

IKT-Sicherheitsstrategie
(BKA, 2012)

Austrian Trust Circle (ATC)
Public-Private Cooperation
2012

General Data Protection Regulation (GDPR)
EC (05/2016)

RL zur Netz- und Informationssicherheit (NIS)
EC (08/2016)

Cyber-Sicherheits Platform (CSP, CSS)
(BKA, 2015)

IKT-Riskikoanalyse Gas 1
(ECA/BKA/BM.I/BMLVS/BMWFW/FVGW)
2015 - 2016

IKT-Risikoanalyse Strom 1+2
(ECA/BKA/BM.I/BMLVS/BMWFW/OE)
2014 / 2015 - 2016

ÖSCS
Österreichische Cyber-Security Strategie
(BKA/BM.I/BMLVS)
2013

Ziele und Inhalte des durchgeführten Cyber-Security Projektes der E-Wirtschaft

- **Projekt:**
  - Multidisziplinäres **Public-Private Partnership** (Regulator, Branche, Ministerien)
  - Prinzip der Freiwilligkeit
  - Projekt basierend auf international anerkannten Risikomanagement Standards (ISO 31.000, ONR 49.002-1-3, ÖNORM S2410)

- **Projektziele:**
  - **Versachlichung** der öffentlichen Diskussion
  - **Sensibilisierung** und Ausbildung von Sicherheitsbewusstsein
  - Schaffung von inhaltlichem Mehrwert durch internationale „Best Practices“ und **branchenübergreifenden Informationsaustausch** zwischen Beteiligten
  - Förderung von **Interoperabilität** zwischen Komponenten und Netzen durch gemeinsame Zusammenarbeit und technischen Diskurs
  - Erstellung einer **umfassenden Risikoanalyse** mit End-2-End Betrachtung und Priorisierung der identifizierten Risiken für die flächendeckende Stromversorgung
  - Entwicklung und Formulierung von **Mindestsicherheitsstandards** und **detailliertem Umsetzungsplan**
  - **Freiwillige Selbstverpflichtung** der Branche mit periodischen Audits

Für die Projektdurchführung wurde ein Public-Private Partnership initiiert

Elektrizitätswirtschaft	Regulierungsbehörde	Öffentliche Hand
▪ Oesterreichs Energie ▪ Elektrizitätserzeuger ▪ Verteilernetzbetreiber (VNB) ▪ Übertragungsnetzbetreiber (ÜNB)	▪ Energie-Control Austria (Projektleitung)	▪ Bundeskanzleramt (BKA) ▪ BM für Inneres (BM.I) ▪ BM für Landesverteidigung und Sport (BMLVS) ▪ BM für Wissenschaft, Forschung und Wirtschaft (BMWFW)

Projekt-Struktur

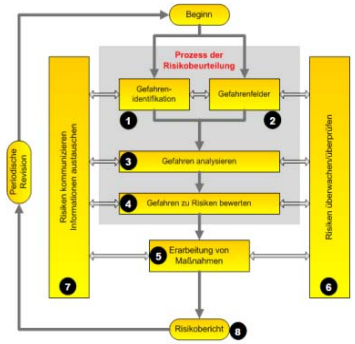
Lenkungsausschuss: Entscheidungsträger aus Elektrizitätswirtschaft und öffentlicher Verwaltung; steuert und evaluiert Aktivitäten und Projektfortschritt

Technische Fachexperten: IT-Experten und Risikomanager aus dem IKT-/Cybersecurity Umfeld. Identifiziert und evaluiert Risiken und Schwachstellen; erarbeitet inhaltliche Maßnahmen und Handlungsempfehlungen.

Die Vorgehensweise unterteilte sich in sechs Phasen mit ansteigender Komplexität

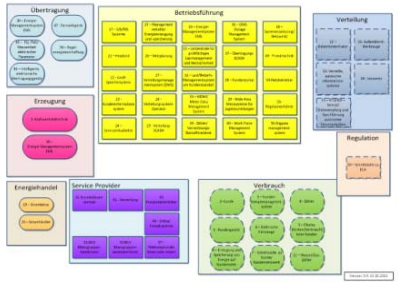
E-CONTROL

Literaturanalyse



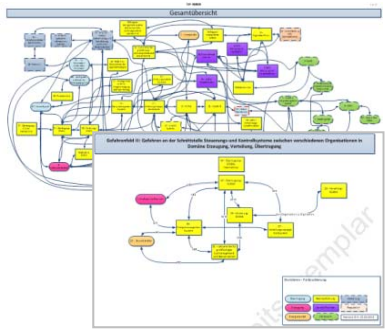
1

Domänenmodell



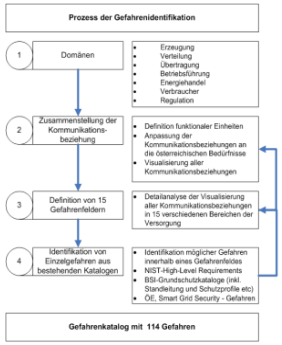
2

Risiko-Identifizierung



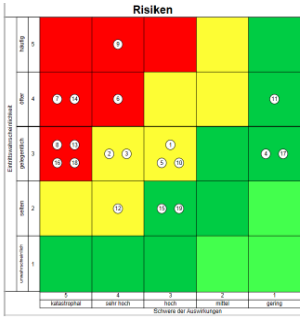
3

Risiko-Bewertung



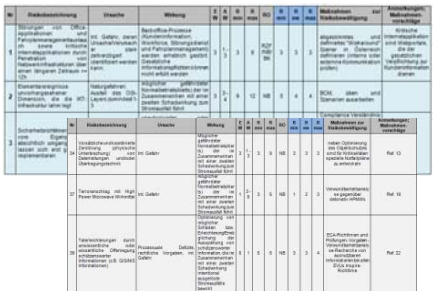
4

5x5 Risiko Matrix



5

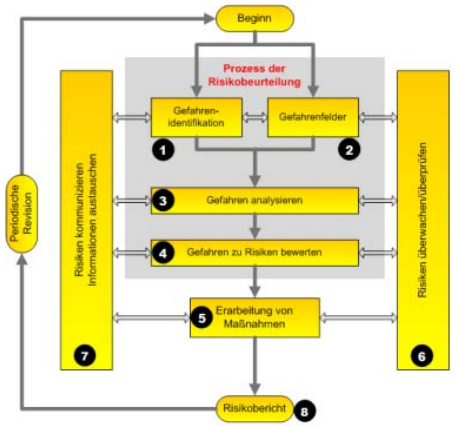
Maßnahmenplan



6

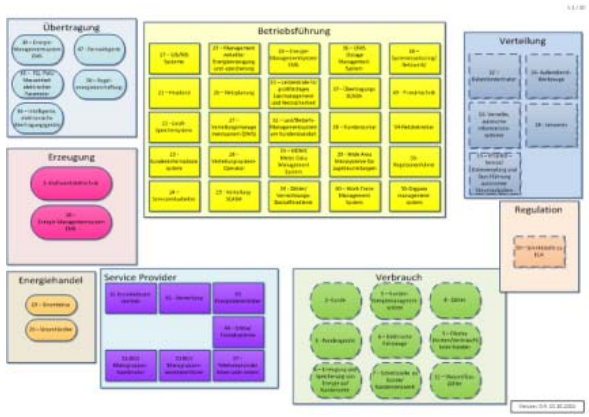
Die Ausgangsbasis war eine detaillierte Analyse des aktuellen Wissensstandes

1 Literaturanalyse



- Literaturzusammenstellung
- Analyse und Auswertung bereits gewonnener Erfahrungen / Anwendungsfällen (öst. und int.)
  - Schweizer IKT-Risikoanalyse
  - NIST Cyber-Security Framework
  - BIS-Schutzprofil
  - NESCOR Guide to Penetration Testing for Electrical Utilities

2 Domänenmodell AT

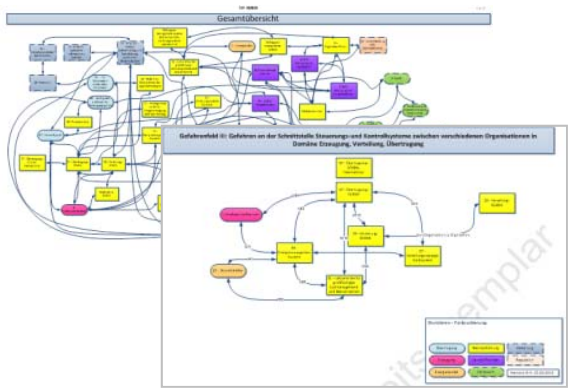


- Erstellung eines Domänenmodells mit 8 Gruppen:
  - Erzeugung
  - Strombörse
  - Betriebsführung
  - Übertragung
  - Verteilung
  - Endverbraucher
  - Service Provider
  - Regulator
- Identifizierung von 58 „funktionalen Einheiten"
- High-level Visulisierung ohne Darstellung von Kommunikationsbeziehungen / Schnittstellen

Existierende Kommunikationsbeziehungen wurden in 15 Gefahrenfelder gruppiert

Risiko-Identifizierung

3



- Erarbeitung der technisch- organisatorischen Kommunikationsbeziehungen
- “Werkzeug “um IKT-Interdependenzen darzustellen
- Gruppierung in 15 Bereich (“Gefahrenfelder”)
- Basis: gemeinsame sicherheitsrelevante Charakteristika

Technisch-organisatorische Kommunikationsbeziehungen - 15 Gefahrenfelder

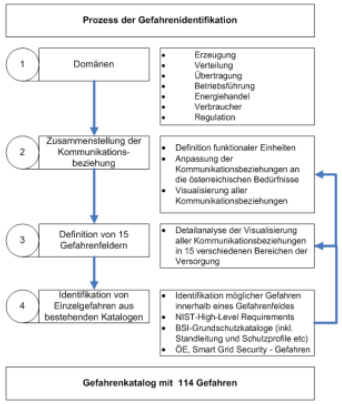
- M2M-Kommunikation
- SCADA und Kontrollsysteme innerhalb d. Organisation
- SCADA und Kontrollsysteme zwischen Organisationen
- Back-Office Systeme
- Intraorganisatorische Kommunikation
- Steuerungssysteme / Verwaltungssysteme
- Sensoren und Sensorennetzwerke
- Schnittstellen im Smart Meter Netzwerk
- HAN/BAN/NAN
- Externe Systeme mit „direkter“ Beziehung zum Endverbraucher
- Service- und Wartungsschnittstellen
- Schnittstellen am Smart-Meter
- Decision-Support Systeme
- Entwicklung / Wartung an der Sekundärtechnik
- Netzwerküberwachung und Securitymonitoring-Systeme

Eine erste Analyse führte zur Identifikation von 114 Einzelrisiken

E-CONTROL

Risiko-Bewertung

4



- Erstidentifikation von 114 Einzelrisiken unter Berücksichtigung von:
  - Technische Gefahren
  - Naturgefahren
  - Intentionale Gefahren
- Entwicklung eines ganzheitlichen Risikobewertungsprozesses mit einheitlichen Bewertungskriterien

Risiko (R) = Eintrittswahrscheinlichkeit (E) [Machbarkeit (M)] x Auswirkung (A)

Risikobewertung der Einzelgefahren

- Auswirkung (A) gemessen als Kombination von

1) Anzahl der von Stromunterbrechung betroffenen Anschlüsse im Versorgungsgebiet in % (Skala: 1% bis >50%) und
2) Dauer der Unterbrechung in Minuten (Skala: 30 Minuten bis > 12 Stunden) oder
3) von Stromunterbrechung betroffene Höchstlast in % (Skala: 1% bis > 10%)

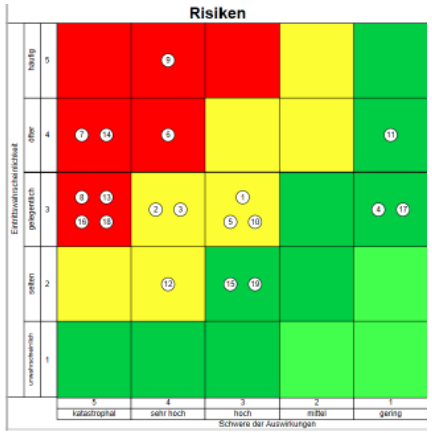
- Risikobewertung basierend auf:

1) Machbarkeit (M) – finanzieller, zeitlicher, personeller und organisatorisch-technischer Aufwand
2) Eintrittswahrscheinlichkeit (E) – 5-stufige Skala von unwahrscheinlich (1x in 50 Jahren) bis häufig (mind. 1x/Jahr)

Von 114 identifizierten Risiken wurden 73 als potentiell kritisch eingestuft

E-CONTROL

5x5 Risiko Matrix



5

- Identifikation von 73 Einzelrisiken mit Potential einer flächendeckenden Störung der Stromversorgung
- Risikoassessment für 3 Szenarien - worst, best, und most-likely case
- Darstellung als 5x5 Risikomatrix mit den Axen Eintrittswahrscheinlichkeit (unwahrscheinlich – häufig) und Schwere der Auswirkung (gering – katastrophal)
- Zusammenfassung zu 19 Aggregationsrisiken

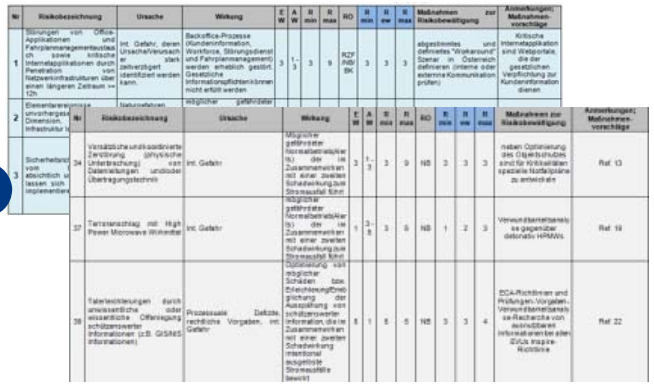
Ergebnisdarstellung

- Hohe Risikostufe / Kritikalität (Priorität 1) = 8 aggregierte Risiken (rot)
- Mittlere Risikostufe / Kritikalität (Priorität 2) = 7 aggregierte Risiken (gelb)
- Niedrige Risikostufe / Kritikalität (Priorität 3) = 5 aggregierte Risiken (grün)

- Zusammengefasst in 6 Risikocluster (Priorität 1 und 2):
- (Krisen)Kommunikation- und Eskalation
- Design und Architektur
- „Human Factor“
- Hard- und Software
- Organisatorische Sicherheit
- Zugriffskontrolle und Kryptographie

Ein detaillierter Maßnahmenplan dient in weiterer Folge dazu Risiken zu mitigieren

Maßnahmenplan



- Erstellung eines detaillierten Maßnahmenplans zur Risikominimierung mit **konkreten Handlungs-empfehlungen**, **größenspezifischen Mindesstandards** und **Umsetzungshorizont**
- Benennung von Prozesseignern und Prozessverantwortlichen
- Erstabschätzung der für die Umsetzung benötigten finanziellen und personellen Ressourcen
- Priorisierung der Umsetzungsmaßnahmen unter Berücksichtigung der Risikostufe
- Maßnahmenempfehlungen waren z.B.:
  - Durchführung von Zertifizierungen (z.B. ISO)
  - Bennenung eines CISO mit entsprechenden Kompetenzen
  - Institutionalisierung eines Kommunikations- und Alarmierungsprozesses für IKT-Vorfälle (“E-CERT”)
  - Beteiligung bei nationalen und internationalen Sicherheitsplanspielen (z.B. ENISA CyberEurope)

Key Learnings und aktuelle Schritte

- **Public-Private Partnerships** eignen sich um den Informationsaustausch und die Zusammenarbeit zwischen öffentlichen und privaten Stakeholdern zu erhöhen
- **Freiwillige Selbstverpflichtungen** von Unternehmen zu Mindestsicherheits-standards sind eine **Alternative zu gesetzlichen Vorgaben**
- **Umsetzung der Maßnahmenempfehlung** aus der durchgeführten Risikoanalyse
  - Teilnahme an Sicherheitsübungen („Cyber-Europe 2014)
  - **Institutionalisierter Kommunikations- u. Alarmierungsprozesse** („E-CERT“)
  - etc.
- Durchführung einer IKT-Risikoanalyse für die heimische **Gaswirtschaft**
- **Periodischer Review** und Aktualisierung der IKT-Risikoanalyse Strom
- Aktive Involvierung und Unterstützung bei der **Umsetzung der europäischen NIS-RL auf nationaler Ebene** (nationales Cyber-Sicherheits-Gesetz)

Eckpunkte der europäischen NIS-RL

- **„Betreiber“ =**
  - **öffentliche** oder **private** Einrichtung,
  - aus dem Bereich **Energie**, Transport, Bank- und Finanzmarktinfrastrukturen, Gesundheit sowie Wasserversorgung – voraussichtlich auch Internetplattformen,
  - sofern der angebotene Dienst **wesentlich** ist, d.h. wesentlich für die Aufrechterhaltung **kritischer sozialer und wirtschaftlicher Aktivitäten UND** stark abhängig von **Netz- und Informationssystemen** sowie der Entfall / Störung des Dienstes einen **signifikanten Einfluss auf die Wirtschaft oder Gesellschaft** eines MS hat.

- **Ziel =** Erreichen einer hohen Netzwerk- und Informationssicherheit durch:
  - verbesserte Zusammenarbeit zwischen den MS
  - intensivere strategische Koordination (EK, ENISA, MS)
  - durch verbesserte nationale Kooperationsgruppe (NIS-Behörde, SPOCS)
  - operationale Kooperation (CERTs)
  - **verpflichtete Einführung eines angemessenen IT-Risikomanagements** und **Meldung signifikanter Störfälle**

Vielen Dank für Ihre Aufmerksamkeit.

Mag. Philipp Irschik, MIM

+431 24724

philipp.irschik@e-control.at

www.e-control.at


E-CONTROL
PROFITIEREN. WO IMMER SIE ENERGIE BRAUCHEN.