Präsentation Cyber BFE

Cyber Krieg -ukrainisches Reaktion-

Phase 1: Russland greift Ukraine an.
Phase 2: Minister Fedorov setzt ein **Ukrainian IT Army** ein.

IT Army of Ukraine hacks website of Wagner PMC: " Personal data of mercenaries at our disposal"

MONDAY, 19 SEPTEMBER 2022, 22:00

76331

YEVHEN KIZILOV – MONDAY, 19 SEPTEMBER 2022, 22:00

The IT Army of Ukraine received all the personal data of the mercenaries of Wagner Private Military Company (PMC) by hacking their website.

Source: Mykhailo Fedorov, Minister of Digital Transformation, on Telegram

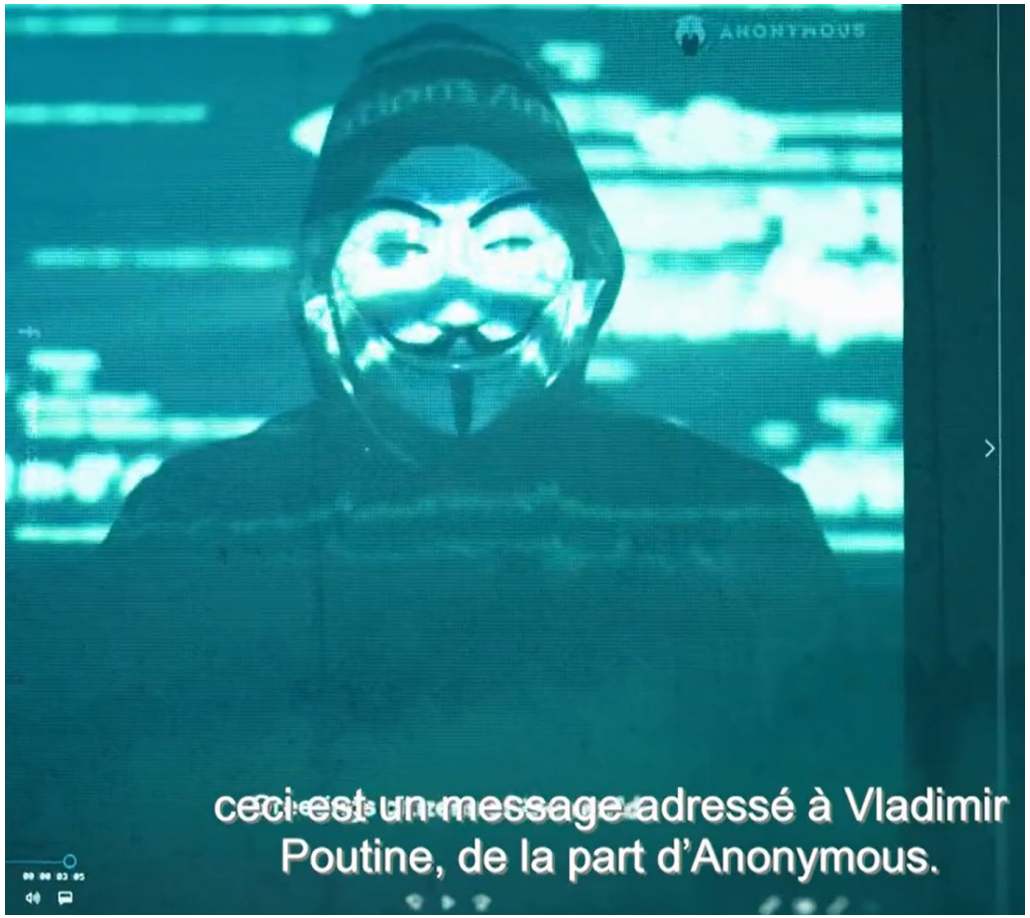
Quote: "The website of the Wagner group, which recruits Russian prisoners for the war in Ukraine, has been hacked by the IT Army!

We have all the personal data of mercenaries! Every executioner, murderer and rapist will be severely punished. Revenge is inevitable!"

Cyber Krieg -Weltreaktion-

Phase 3: die **Cyberwelt** trennt sich in 2 Gruppe (für oder gegen Russland).

-Anonymous droht Putin. Das erste Mal, dass diese Hackergruppe für einen Land Partei ergreift.



Cyber Krieg –Wirkungen-

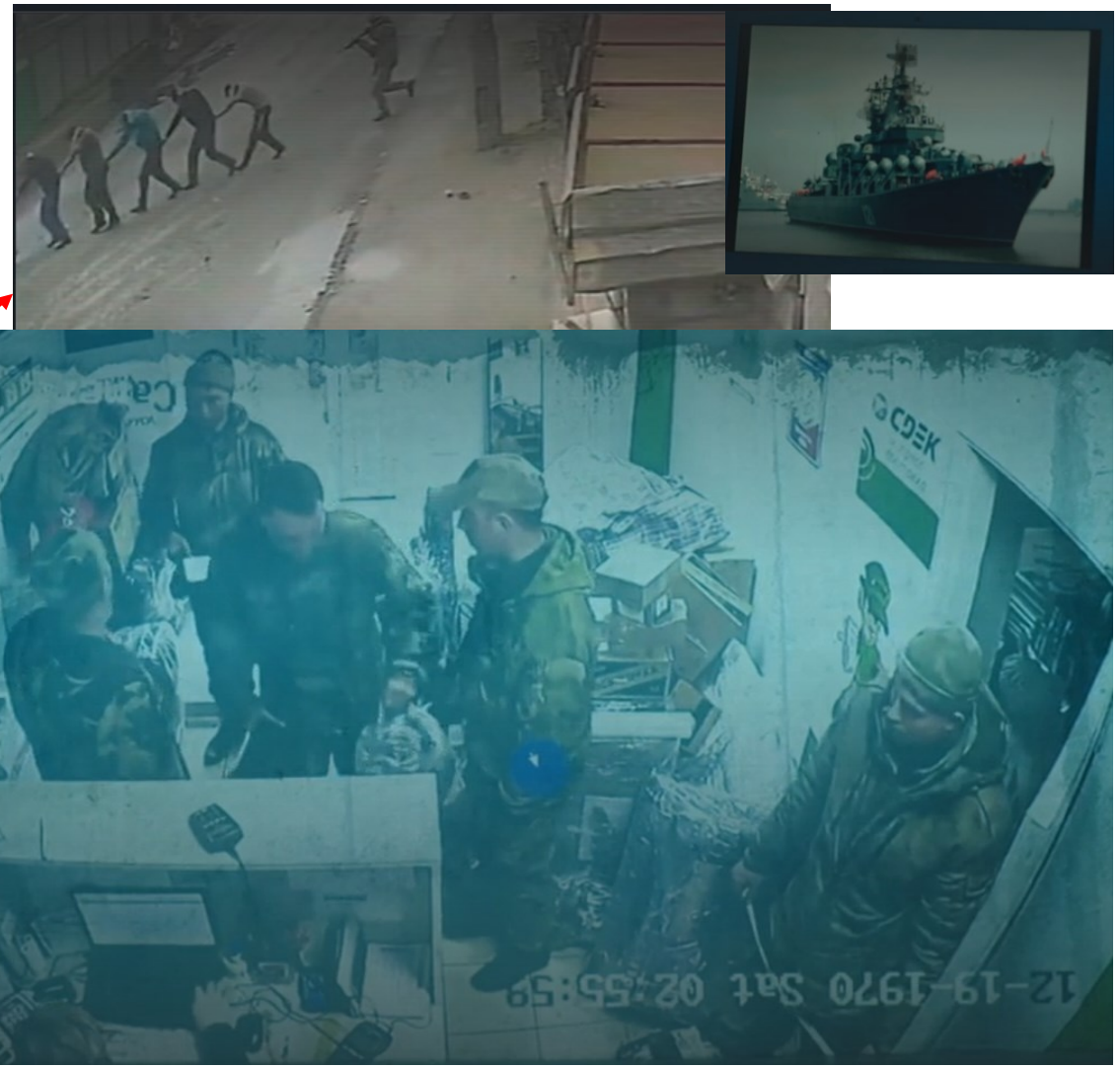
Phase 4: Russland darf sich auch verteidigen

- Wenige Ressourcen, um andere Länder (und ihre kritischen Infrastruturen) anzugreifen.
- Das bedeutet überhaupt nicht, dass unsere KI geschützt sind!

Es bleibt noch viele Angriffe
Ransomware-Angriffe am meistens
Wo es Geld zu holen gibt, gibt es oder wird es Angriffe geben.

Bekannte Ergebnisse der Cyber Aktivitäten:

- Videoüberwachung (Info für Gericht).
- Liste von FSB Agenten. Viele im Westens.
  - Werden verklagt werden, weil identifiziert.
- Pläne des Moskva-Schiff.
- Diebe identifizieren (Russen die schicken gestohlene Material nach Russland ab Belarus).
- Geolokalisation der Soldaten.



Grundlegende Prinzipien : CIA - AAA

CIA

Confidentiality / Vertraulichkeit

Integrity /Integrität

Availability / Verfügbarkeit

Die Informationen sind vertraulich und müssen verfügbar sein. Dritte dürfen keinen Zugang zu ihnen haben oder sie verändern können.

AAA

Authentification / Authentifizierung

Authorization / Autorisierung

Accounting / Nachvollziehbarkeit

Wir prüfen, wer auf was zugreift, welche Rechte er hat und welche Aktionen er an den Systemen durchführen kann.

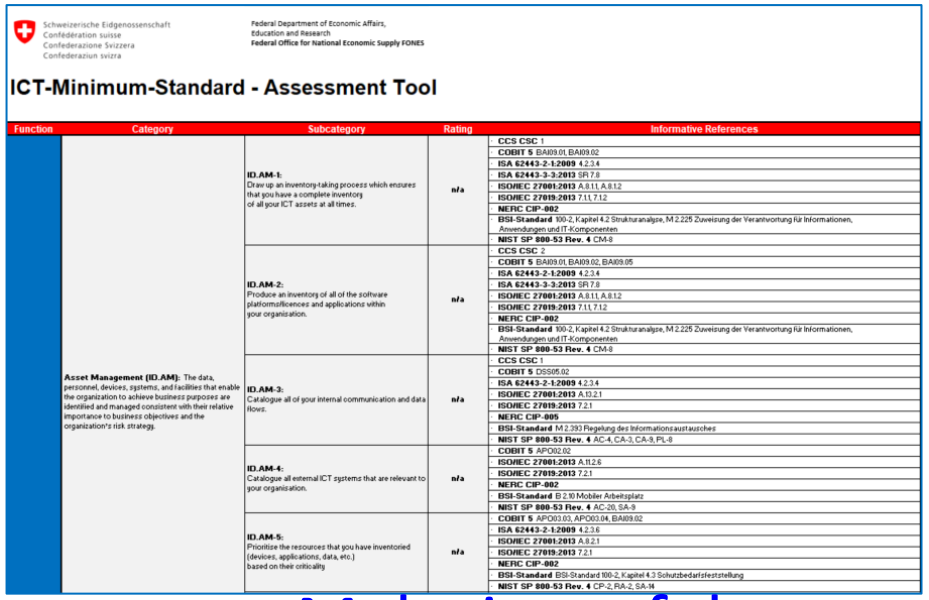
Make it simple

Welche Standards sollen als Referenz herangezogen werden?

Norme	Description
ISO 38500	IT-Governance durch das Unternehmen
ISO 31000	Risikomanagement
ISO 27001	Umsetzung des Sicherheitsmanagementsystems
ISO 27002	Umgang mit Sicherheitsrisiken
ISO 27019	Für die ICS-Systemen
ITIL	Für IT Dienste und IT-Support
CMMi	Für die Entwicklung 5 Reifegrade
TOGAF	IT-Unternehmensarchitektur
COBIT 5	Die 11 Vektoren zur Verbesserung der IT-Governance
RiskIT	Governance, Risikobewertung und -reaktion
ValIT	Projektportfoliomanagement
NERC	North American Electric Reliability Corporation
CPNI/NCSC	Centre for the Protection of National Infrastructure
MEHARI	Risikoanalyse und -behandlung
BSI….	Deutsche Norm.

Make it complex

Was ist für die Branche sinnvoll?
Arbeitsgruppe zur Festlegung von IKT-Mindeststandards (BWL, VSE, ...)



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

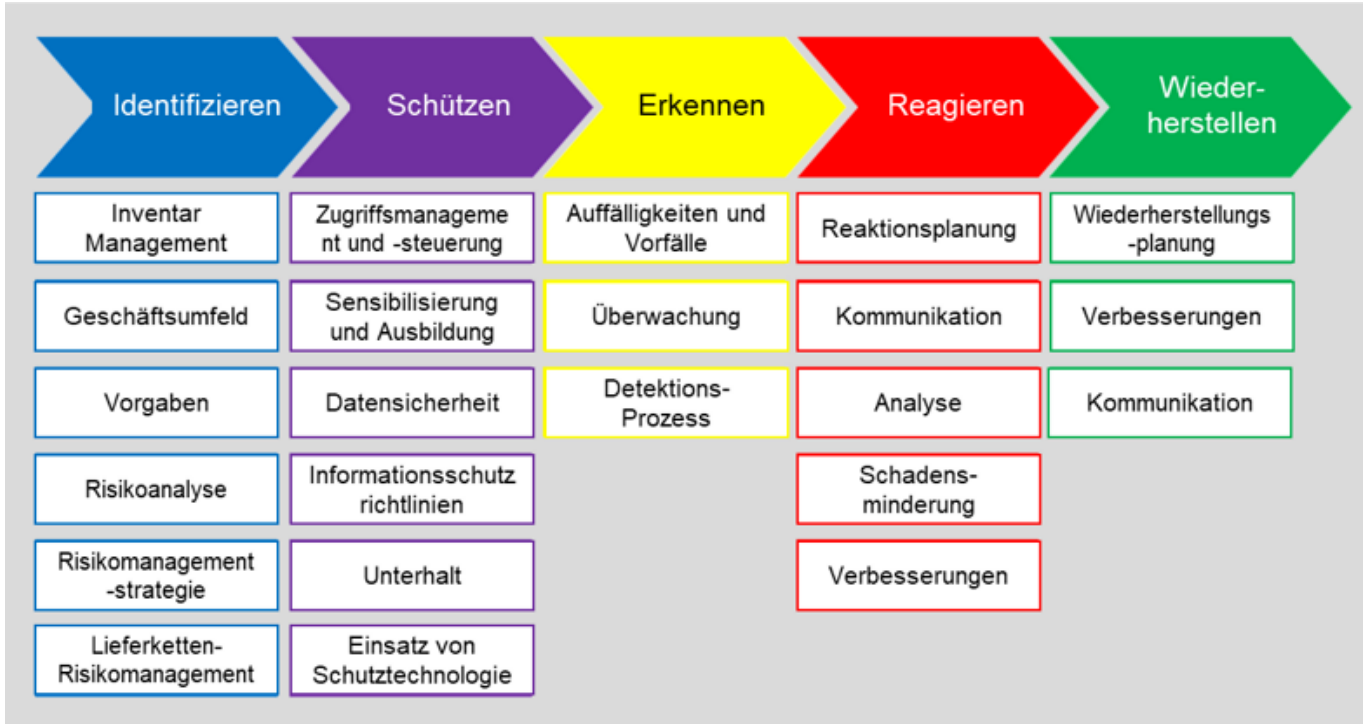
Federal Department of Economic Affairs, Education and Research
Federal Office for National Economic Supply FONES

ICT-Minimum-Standard - Assessment Tool

Function	Category	Subcategory	Rating	Informative References
	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Draw up an inventory-taking process which ensures that you have a complete inventory of all your ICT assets at all times.	n/a	CCS CSC 1 COBIT 5 BAI09.01, BAI09.02 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 ISO/IEC 27019:2013 7.1.1, 7.1.2 NERC CIP-002 BSI-Standard 100-2, Kapitel 4.2 Strukturanalyse, M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Produce an inventory of all of the software platforms/licences and applications within your organisation.	n/a	CCS CSC 2 COBIT 5 BAI09.01, BAI09.02, BAI09.05 ISA 62443-2-1:2009 4.2.3.4 ISA 62443-3-3:2013 SR 7.8 ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 ISO/IEC 27019:2013 7.1.1, 7.1.2 NERC CIP-002 BSI-Standard 100-2, Kapitel 4.2 Strukturanalyse, M 2.225 Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Catalogue all of your internal communication and data flows.	n/a	CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO/IEC 27001:2013 A.13.2.1 ISO/IEC 27019:2013 7.2.1 NERC CIP-005 BSI-Standard M 2.393 Regelung des Informationsaustausches NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Catalogue all external ICT systems that are relevant to your organisation.	n/a	COBIT 5 APO02.02 ISO/IEC 27001:2013 A.11.2.6 ISO/IEC 27019:2013 7.2.1 NERC CIP-002 BSI-Standard B 2.10 Mobiler Arbeitsplatz NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Prioritise the resources that you have inventoried (devices, applications, data, etc.) based on their criticality	n/a	COBIT 5 APO03.03, APO03.04, BAI09.02 ISA 62443-2-1:2009 4.2.3.6 ISO/IEC 27001:2013 A.8.2.1 ISO/IEC 27019:2013 7.2.1 NERC CIP-002 BSI-Standard BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung NIST SP 800-53 Rev. 4 CP-2, PA-2, SA-14

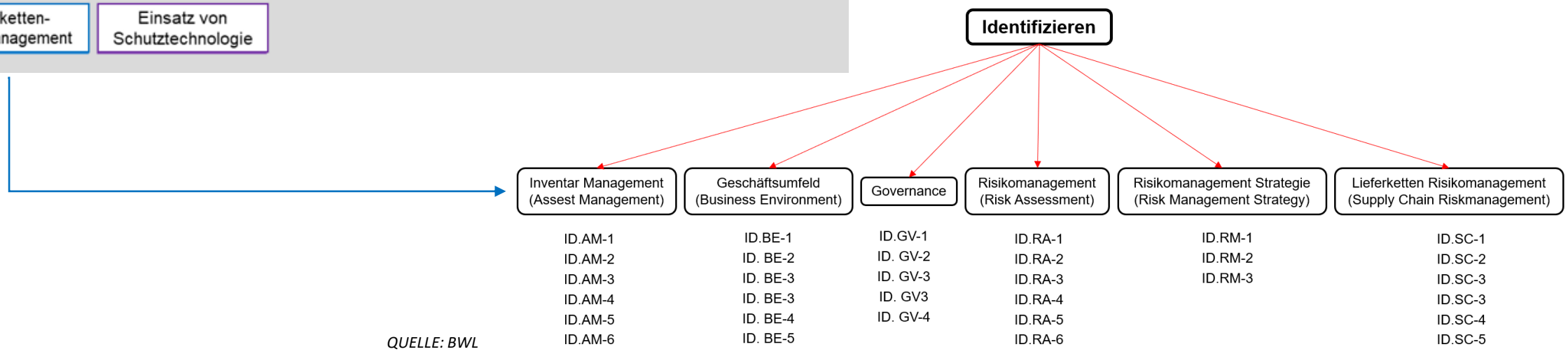
Make it useful

Die NIST-Standards als Grundlage für IKT-Minimalstandards



5 Funktionen /23 Kategorien

- Identifizieren
- Schützen
- Detektieren
- Reagieren
- Wiederherstellen



QUELLE: BWL

Auto-Evaluation nach IKT Minimalstandards

Gesamtbewertung der Cybersicherheit		Bemerkung
0	Nicht umgesetzt	Keine Sicherheitsmassnahmen.
1	Partiell umgesetzt, nicht vollständig definiert und abgenommen	Anfang des Weges.
2	Partiell umgesetzt, vollständig definiert und abgenommen	Unterstützung durch das Management, laufende Massnahmen
3	Umgesetzt, vollständig oder grösstenteils umgesetzt, statisch	Massnahmen eingeleitet.
4	Dynamisch, umgesetzt, kontinuierlich überprüft, verbessert	Massnahmen umgesetzt mit Nachverfolgung.
n/a	Nicht applizierbar / Begründung notwendig	-

Zur Erinnerung:
Das "vorgeschlagene" Ziel des IKT-Mindeststandards liegt bei 2.6 (Mittelwert).

2.6 ist als Beispiel angegeben, entspricht aber einem wünschenswerten Niveau.

Startpunkt

EnG Art. 7 [1] Eine sichere Energieversorgung umfasst die jederzeitige Verfügbarkeit von ausreichend Energie, ein breit gefächertes Angebot sowie technisch sichere und leistungsfähige Versorgungs- und Speichersysteme. Zu einer sicheren Energieversorgung gehört auch der Schutz der kritischen Infrastrukturen einschliesslich der zugehörigen Informations- und Kommunikationstechnik

↓

Die Branche und das BWL haben IKT-Mindeststandards festgelegt ("Minimalstandard zur Verbesserung der IKT-Resilienz" + Excel-Bewertungstool + "OT-Grundschutz").

↓

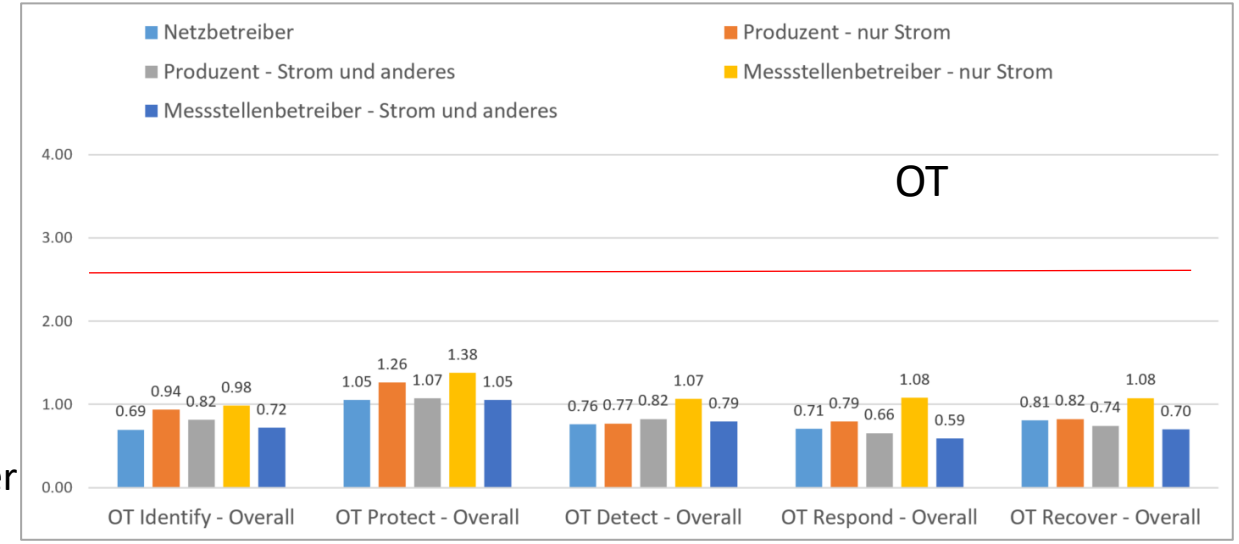
Wie ist der Stand der Cybersicherheit in den Schweizer Elektrizitätsunternehmen?

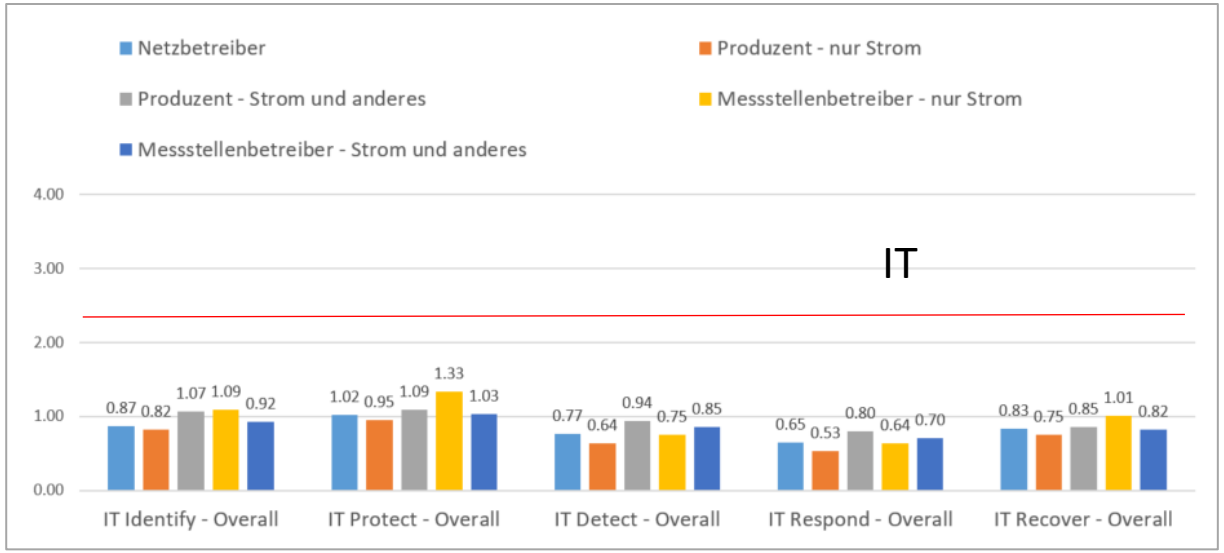
↓

E-Survey und Studie von BFE/Deloitte.

E-Survey 2020

- Die IKT-Minimalstandards wurden als Referenz für die Umfrage herangezogen.
- Teilnahme:
  - 113 VNB (ca.18%).
  - 54 Produzenten (ca. 50% Produktion in der Schweiz, ausser KKW).
  - 79 Messstellenbetreiber (ca. 40% des Messpunkte in der Schweiz).
- Ergebnisse: Das Niveau der Cybersicherheit liegt weit unter dem gewünschten Niveau (2.6, als Beispiel in den IKT-Mindeststandards genannt).
- Die IKT-Mindeststandards sind eine Empfehlung der Branche, keine Verpflichtung.





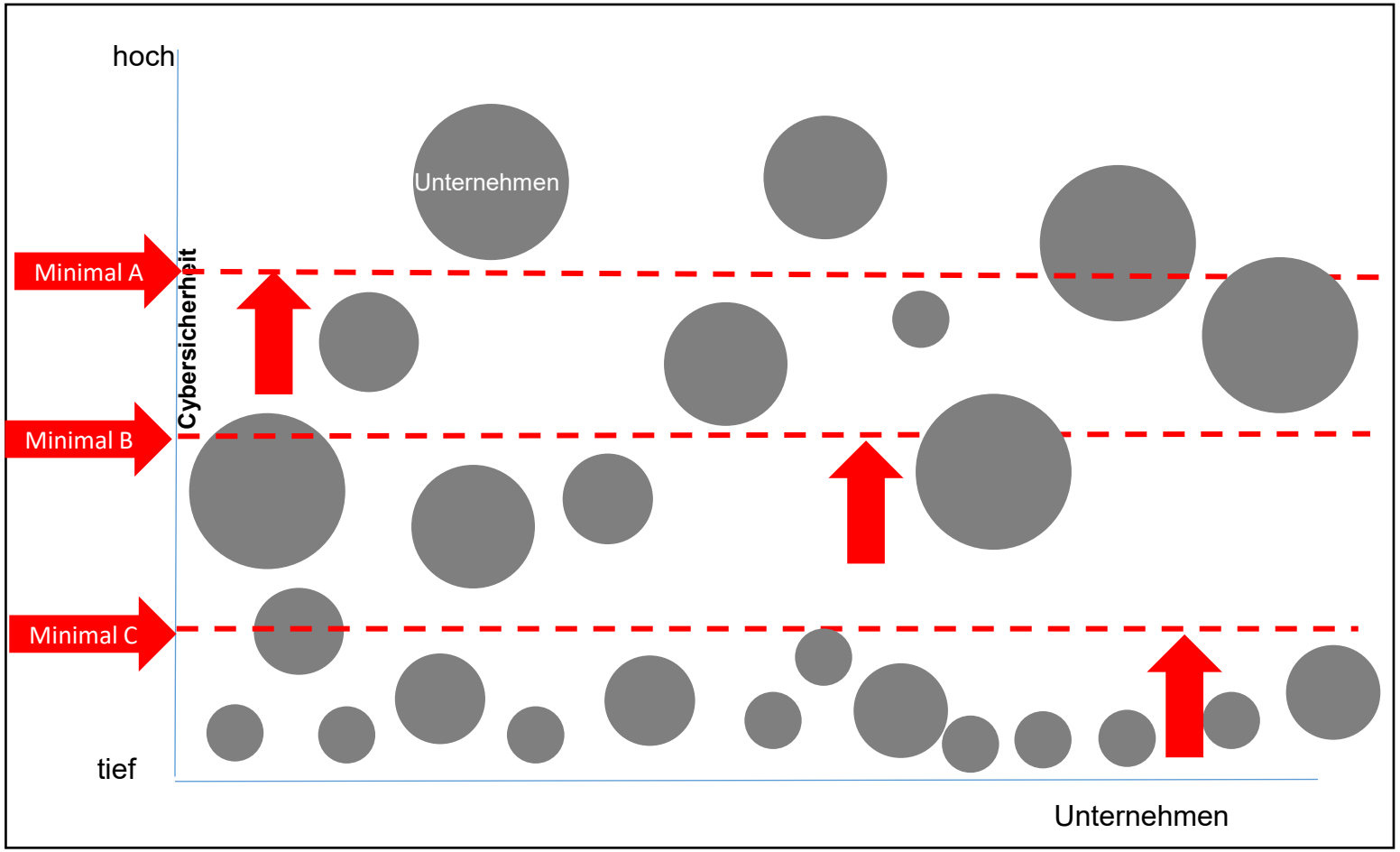
IT-Ergebnisse nach Anzahl der Messpunkte

Scaling gemäss Minimale Standards	Per Anzahl Verbrauchermesspunkte			Nur Netzbetreiber
	A	B	C	D
	>100'000	25-100'000	5-25'000	1-5'000
ID.AM 1-6: Inventar Management	0.73	1.76	1.12	0.78
ID.BE 1-5: Geschäftsumfeld	1.24	2.04	0.99	0.64
ID.GV 1-4: Governance	1.65	2.00	0.99	0.75
ID.RA 1-6: Risikomanagement	1.23	1.63	0.72	0.48
ID.RM 1-3: Risikomanagement Strategie	1.40	1.44	0.91	0.47
ID.SC 1-4: Lieferketten Risikomanagement	0.24	1.36	0.46	0.27
PR.AC 1-6: Zugriffsmanagement und -steue	1.20	2.02	1.66	0.97
PR.AT 1-5: Awareness and Training	1.12	1.36	1.29	0.65
PR.DS 1-8: Datensicherheit	0.78	1.56	1.05	0.82
PR.IP 1-12: Schutz von Daten	0.95	1.54	0.96	0.75
PR.MA 1-2: Maintenance	0.40	1.67	1.00	0.58
PR.PT 1-5: Protective Technology	0.64	1.36	1.00	0.72
DE.AE 1-5: Vorfälle	0.64	1.27	0.42	0.37
DE.CM 1-8: Überwachung	1.05	1.50	1.05	0.64
DE.DP 1-5: Detection Processes	0.44	1.18	0.65	0.50
RS.AN 1-4: Analyse	0.50	1.39	0.45	0.32
RS.MI 1-3: Mitigation	0.47	1.74	0.77	0.41
RS.IM- 1-2: Verbesserungen	0.70	1.44	0.48	0.44
RS.RP-1 : Response Planning	0.68	1.29	0.60	0.33
RS.CO 1-5: Kommunikation	1.00	1.11	0.66	0.22
RC.RP 1: Wiederherstellungsplanung	1.20	1.56	0.97	0.67
RC.CO 3: Kommunikation	1.00	1.50	0.70	0.39

OT-Ergebnisse nach Anzahl der Messpunkte

	Per Anzahl Verbrauchermesspunkte			Nur Netzbetreiber
Scaling gemäss Minimale Standards	A	B	C	D
	>100'000	25-100'000	5-25'000	1-5'000
ID.AM 1, 3-6: Inventar Management	0.80	1.29	0.89	0.56
ID.BE 4: Geschäftsumfeld	1.20	1.00	0.79	0.39
ID.RA 1, 3-6: Risikomanagement	1.08	0.84	0.52	0.51
PR.AC 1-3, 5-6: Zugriffsmanagement und -steuerung	1.40	1.96	1.31	0.97
PR.AT 3: Awareness and Training	0.60	1.11	0.97	0.50
PR.IP 4: Schutz von Daten	1.80	2.22	1.18	1.05
PR.MA 1-2: Maintenance	0.40	1.78	0.83	0.53
PR.PT 3, 5: Protective Technology	0.90	1.22	0.62	0.72
DE.AE 1: Vorfälle	1.00	1.22	0.66	0.71
DE.CM 2-4, 7: Überwachung	0.95	1.03	0.77	0.91
DE.DP 4: Detection Processes	1.00	1.25	0.45	0.35
RS.CO 2: Kommunikation	0.60	0.89	0.34	0.47
RS.AN 2: Analyse	0.60	1.22	0.52	0.63
RS.MI 1-2: Mitigation	0.60	1.11	0.66	0.67
RC.RP 1: Wiederherstellungsplanung	0.80	0.89	0.72	0.79
RC.IM 1: Verbesserungen	0.80	1.00	0.55	0.56

Folge des Berichtes: Umsetzungskonzept



Projekt:
Das BFE will Unternehmen dazu verpflichten, die IKT-Mindeststandards umzusetzen.

- Klare Erwartungen an die Unternehmen (was getan werden muss und wie es getan werden muss).
- Ein gemeinsamer Referenzrahmen.
- Bleibt ein Mindeststandard.

Firmenprofile A, B, C
Kriterien für die Zuteilung laufend:

Digitalisierung 2.0
Data Science im Energiesektor & im BFE

USE CASE I
(Cyber-) Kritikalität VNB

- Welche VNB sind besonders kritisch für die Versorgung.

Data Science Ansatz: «Clustering»
Daten: Bevölkerung. Kritische Infrastrukturen.Stromproduktion. Vulnerable Bevölkerungsgruppen. Ökonomische Bedeutung.

USE CASE II
Profiteure Gebäudeprogramm

- Welche Subvenitonen für Gebäude & Effizienz werden genutzt.
- Wer profitiert von den Massnahmen?

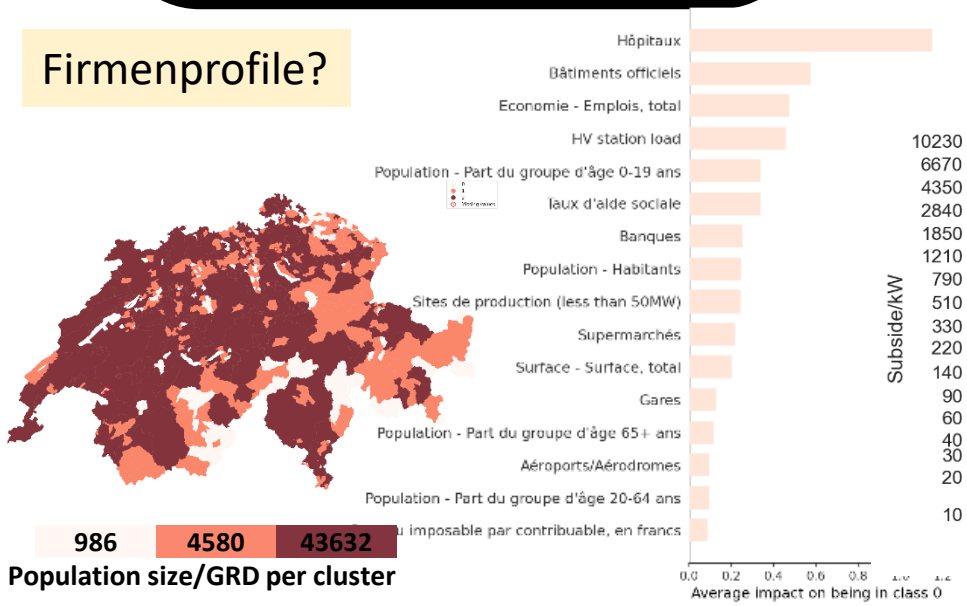
Data Science Ansatz: « Analytics »
Daten: Gebäudeprogramm.

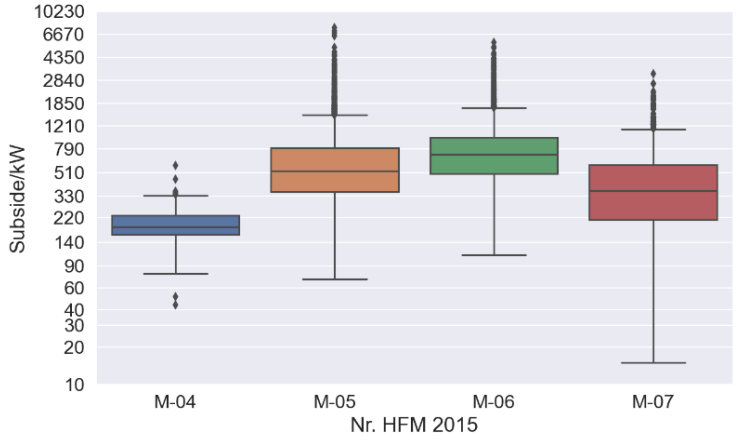
USE CASE III
Indikator Energieabhängigkeit

- Energieversorgungsportfolio und sein Risiko?
- Wie hat sich die Energie-abhängigkeit entwickelt?

Data Science Ansatz: «Research, Modellierung & Analytics »
Daten: Marktdaten offen & beschafft

Firmenprofile?





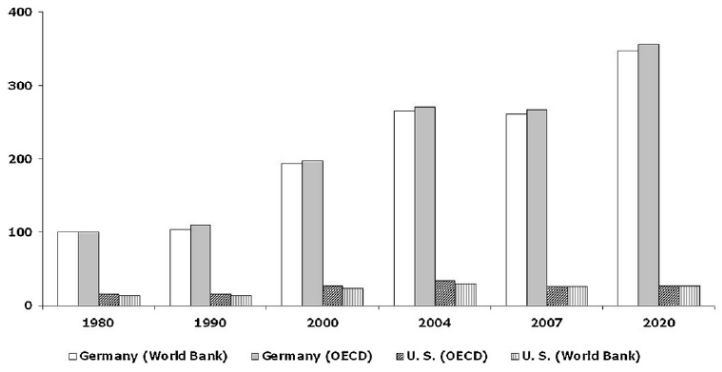


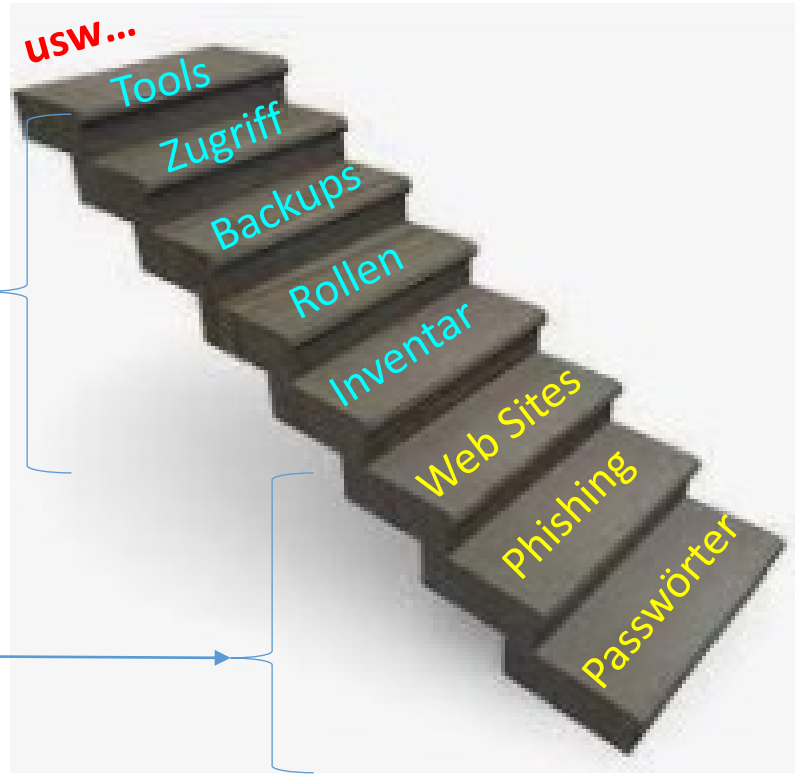
Fig. 4. Total energy supply risks in Germany and the U.S. (1980–2007). *Note*: All values refer to the situation in Germany in 1980 (1980:100).

Erwartungen von BFE

Die Kette ist so stark wie ihre Weak Link.
Ihre Cybersicherheit: was ist der Weak Link?

Meistens ist der Mensch der erster "Weak Link" der Cybersicherheit

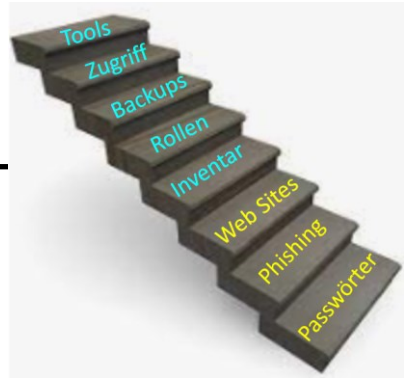
Schon jetzt die Treppe auf… Stufe um Stufe



Sensibilisierung der Firmen Minimalstandards

Sensibilisierung der Mitarbeiter

Treppe: Stufe für Stufe



Welche Aktionen werden an den Systemen durchgeführt? Wer macht was und wer greift auf was zu?=> logs

Systeme, Anwendungen, Sofware, Hardware sowie Daten müssen geschützt werden.

Wer braucht Zugriff auf welches System? Definieren Sie Zugriffe nach dem Need-to-know-Prinzip und nach dem Prinzip des minimalen Zugriffs.

Daten, Software und Anwendungen müssen ausserhalb des Netzwerks gesichert (backup) werden. Backup-Hardware erforderlich.

Technische Massnahmen

Das Unternehmen muss seine Anforderungen an seine Dienstleister klären.

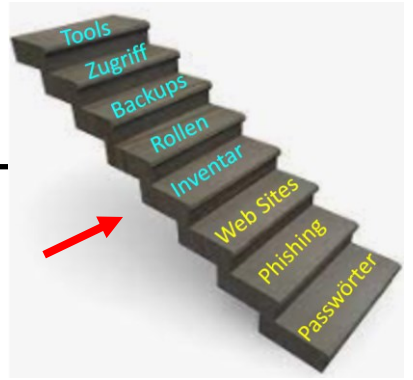
Was muss unbedingt funktionieren, um die Stromversorgung zu gewährleisten? Welche Prozesse, Personen und Systeme sind daran beteiligt?

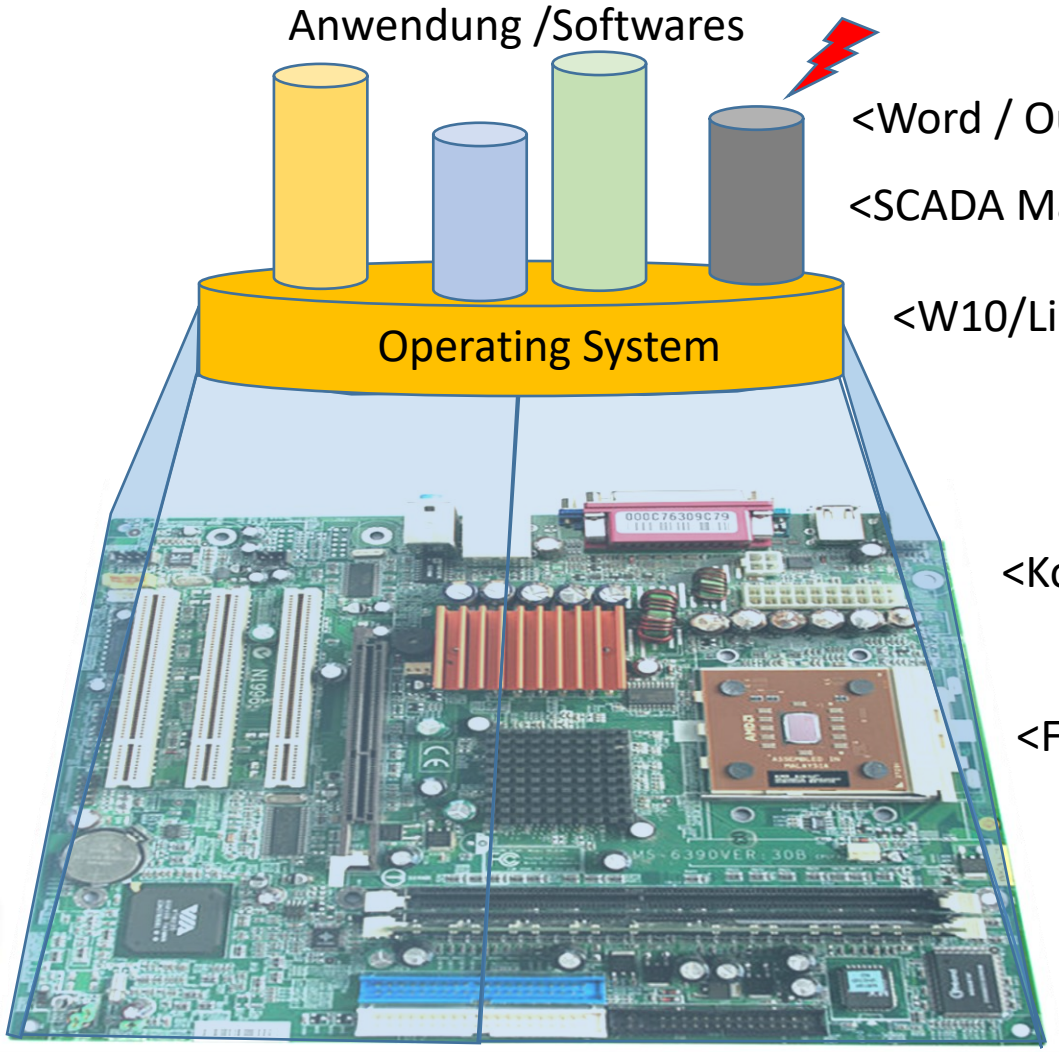
Wer macht was, wer ist für die Cybersicherheit verantwortlich? Werden die Zugriffe rollenbasiert definiert?

Kennt das Unternehmen seine Assets (Harware, Software, Firmware, Daten)?

Organisatorische Massnahmen

Inventar: Hardware, Software, Firmware





<Word / Outlook…

<SCADA Management, Metering…

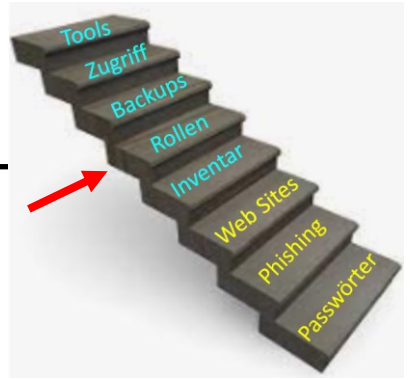
<W10/Linux…

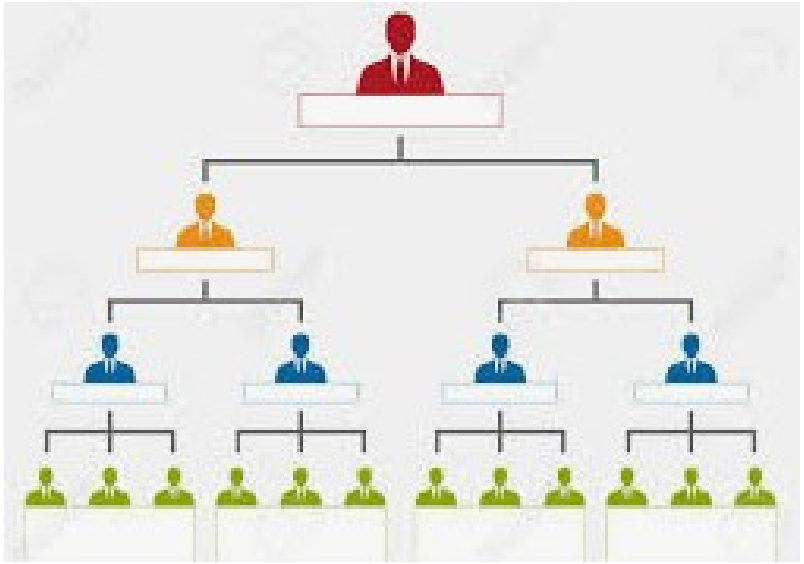
<Komponenten

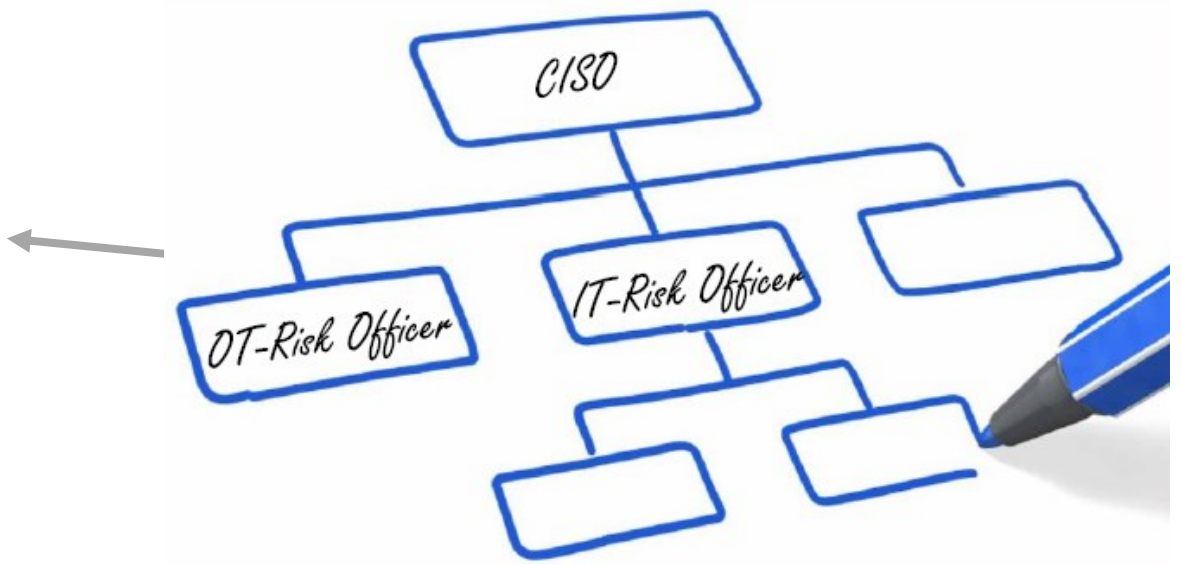
<Firmwares

/!\ Patches

Rollen

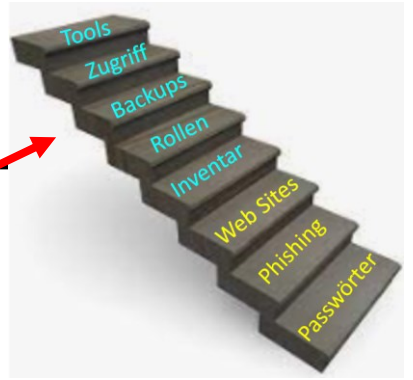






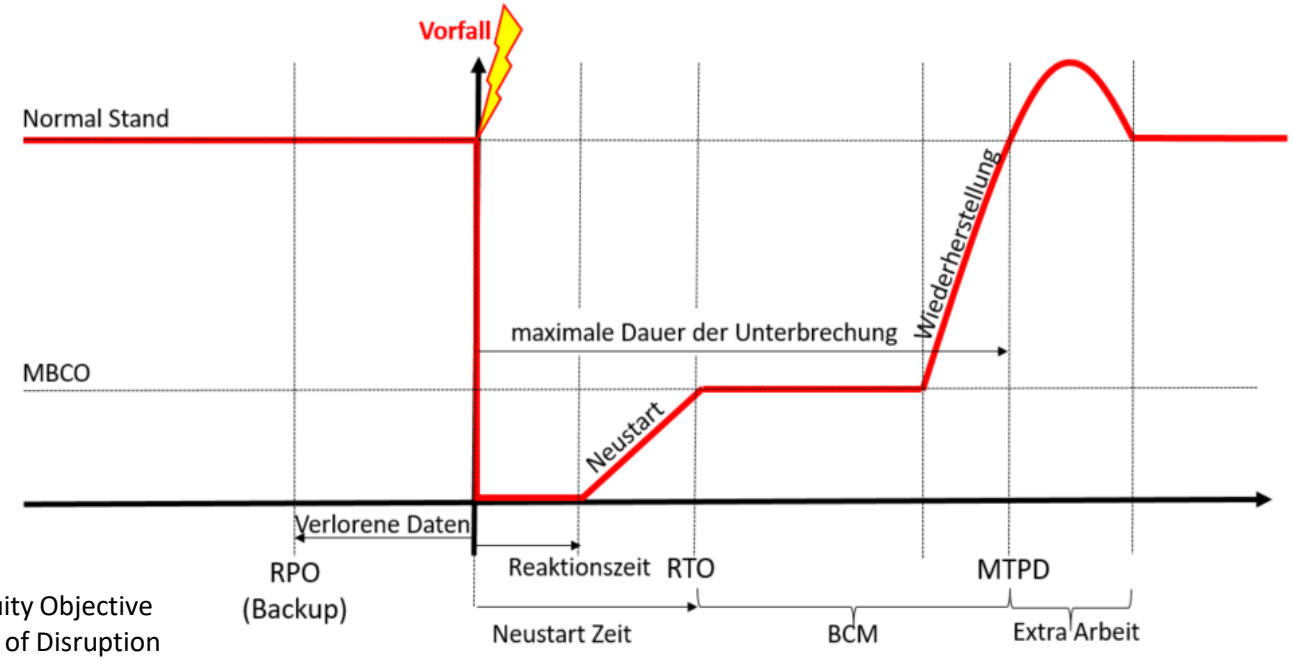
- Haben Sie bereits einen Platz für Cybersicherheit im Organigramm?
- Gilt das Vier-Augen-Prinzip?
- Wer ist für die Cybersicherheit verantwortlich?
- Externer Dienstleister oder interner Mitarbeiter?
- An wen muss er berichten?
- Sind Cyber-Risiken in die Unternehmensrisiken integriert?

Backup & Restore



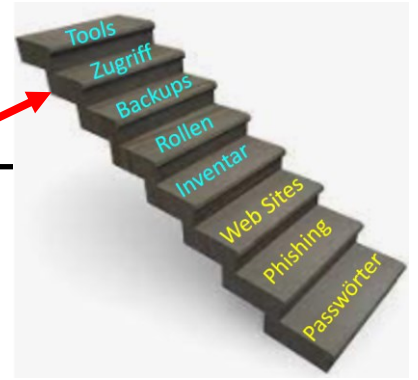
Offline Backups

- Wie oft müssen Backups durchgeführt werden?
- Welche Daten können wir verlieren?
- Testen Sie den Restore!



RPO: Recovery Point Objective
RTO: Recovery Time Objective
MBCO: Minimum Business Continuity Objective
MTPD: Maximum Tolerable Period of Disruption

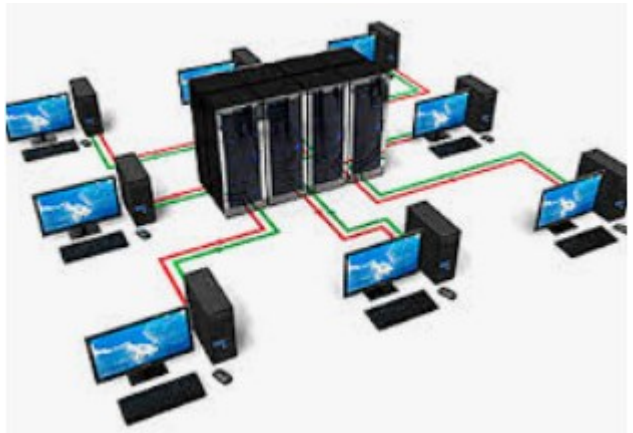
Zugriff



Identity and Access Management

Least Priviledge

- Minimale Berechtigung
- Die Mitarbeiter haben nur die Berechtigungen die sie für ihre Tätigkeiten brauchen, keine mehr.



Quelle: Metric Mind Institute

Need-to-know principle

- Minimale Zugriff
- Die Mitarbeiter zugreifen an Daten erst wenn sie es für ihre Tätigkeiten brauchen.

Quelle: 3columns.io

Werkzeuge (Tools)

Um sich zu schützen: => einen Angriff verhindern/bremsen.

- Firewalls
- IAM / MFA
- Klare und eingehaltene Verfahren
- Sensibilisierung der Mitarbeiter/innen

Um einen Angriff zu identifizieren:

- Monitoring-Tools / Syslogs
- Intrusion Detection Tool (IDS) => Netzwerk- und Flussansicht.
- End Point Detection & Response (EDR) => Geräteansicht

Um sich nach einem Angriff wieder aufzustehen:

- Regelmässige und geschützte Backups ausserhalb des Netzwerks.
- Hardware-Reserven
- Support-Verträge
- Verfahren und Training

Supply Chain Management

Security by design

Die Systeme berücksichtigen die Cybersicherheit bereits bei ihrer Konzeption.

Security by default

Sicherheit wird standardmässig angeboten.
Es handelt sich dabei nicht um eine zusätzliche Option.

Genaue Verträge

Der Auftraggeber (Betreiber) muss die Pflichten und Erwartungen klarstellen.
Dazu gehören die Kontrolle der Komponenten, der Support und die Versorgung.

Recht auf Prüfung

Der Kunde (Betreiber) kann ein Prüfungsergebnis vom Lieferanten verlangen oder selbst ein Unternehmen damit beauftragen.

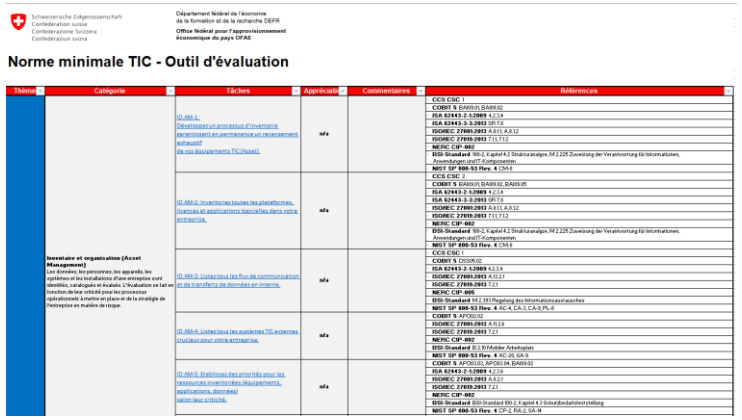
Informationspflicht

Der Lieferant muss alle Informationen über bekannte Schwachstellen in seinen Systemen oder Komponenten offenlegen und Aktionspläne vorschlagen.

Um weiter zu gehen

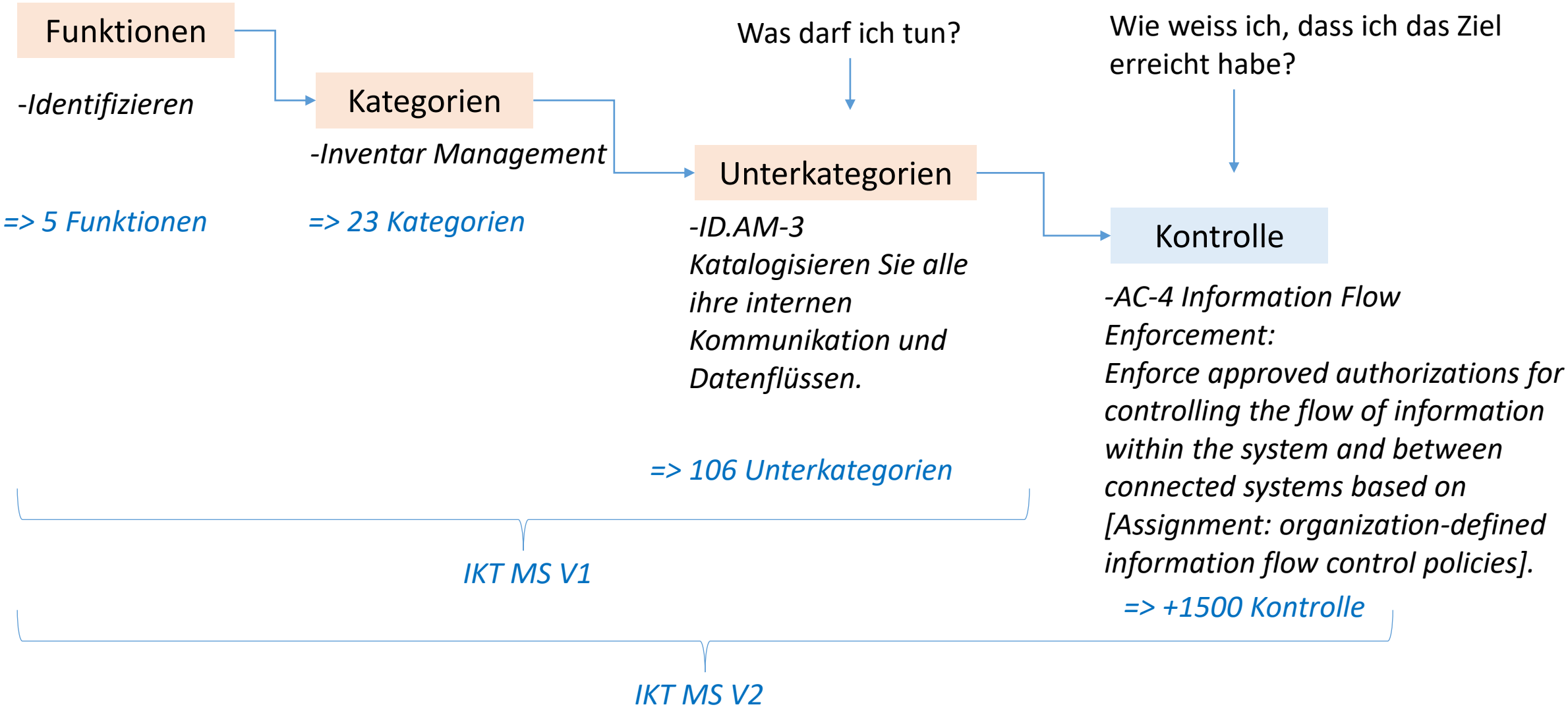
- IKT-Mindeststandards (Version 2 ist in Vorbereitung/Projekt, sie werden genauer sein).
- Bewertungstool (Excel) => wird in Version 2 durch die Einbeziehung der NIST-Kontrolle verbessert.
  - AG des BWL => Globale IKT-Mindeststandards (VSE und BFE in der AG).
  - AG VSE => Anhang, Anforderungen an Elektrizitätsunternehmen, Präzisierungen (BFE und ELCOM teilen in der AG mit).

Handbuch Grundschutz für «Operational Technology» in der Stromversorgung



Norme minimale TIC - Outil d'évaluation

IKT Minimalstandards V1 und V2 (Projekt)



Jaber…

Jaber kostet es viel, oder?

Quelle: fr.freepik.com

Jein!

Sich verteidigen

Risiken akzeptieren

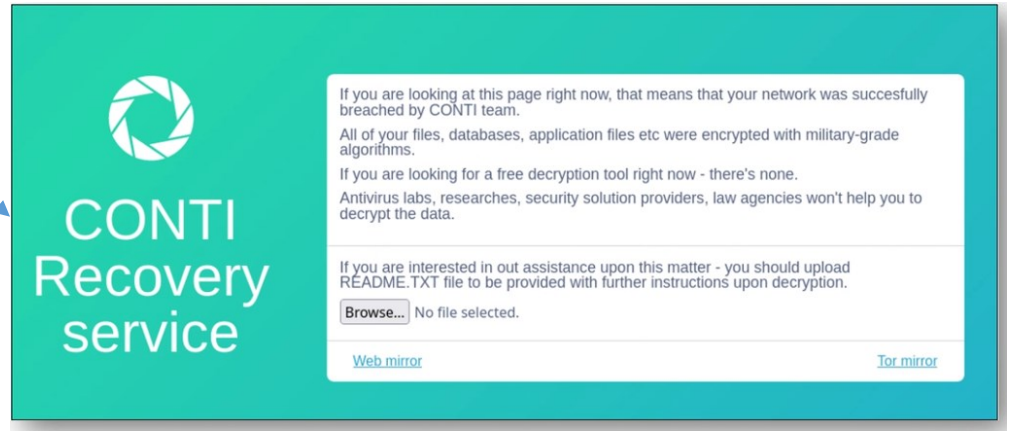
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössische Elektrizitätskommission ElCom
Fachsekretariat

Mitteilung

Anrechenbarkeit Kosten Cybersicherheit

Bern, 28.09.2022



Risiken akzeptieren?

Umfrage Sophos in 2021

37% der Firmen haben ein Ransomware erhalten (USA: 64%)

54% hatten ihre Daten verschlüsselt

32% davon haben Lösegeld bezahlen (53% der US Firmen)

140'000 €: Durchschnittliche Höhe des von den mittelgrossen Unternehmen gezahlten Lösegelds.

1,53 Mio€: Durchschnittlichen Kosten für die Behebung eines Ransomware-Angriffs unter Berücksichtigung der Ausfallzeiten, der Ressourcen (erforderliche Personal, Kosten für Geräte und Netzwerke, entgangene Gewinne, gezahltes Lösegeld usw).

80% der Firmen die bezahlen haben wurden kurz nachher wieder angegriffen /!\ (Quelle unidentifiziert)

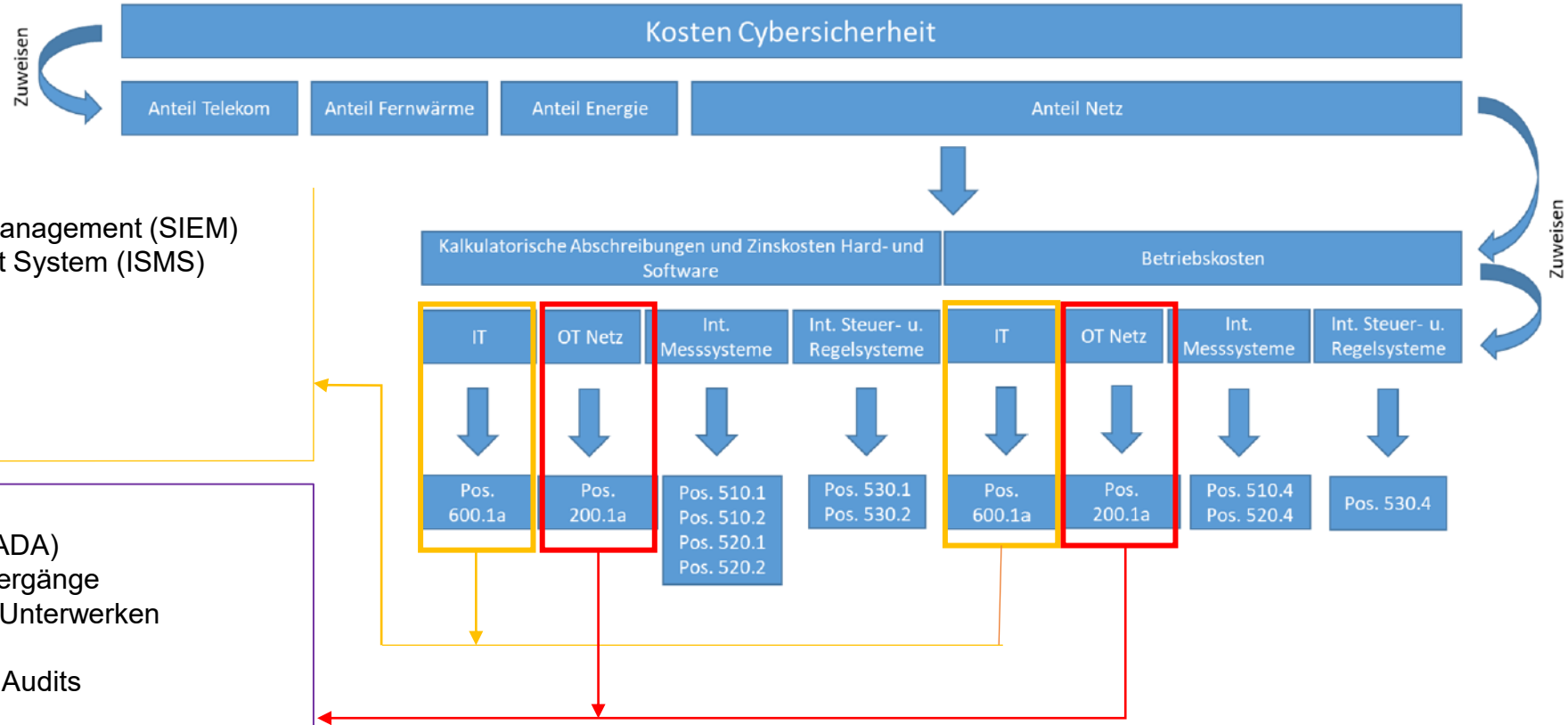
65% der Daten wurden zurückgehalten. 1/3 definitiv verloren.
8% davon stellten ihre Daten vollständig wieder her.

57% konnten mittels Backups ihre Daten selbst rekuperieren

ELCOM: Anrechenbarkeit Kosten Cybersicherheit

Beispiel:
- Anteilige Kosten Security Operation Center (SOC)
- (Anteilige) Raumkosten für z. B. SOC
- Kosten für Awarenesskampagnen
- Schulungen der Mitarbeitenden IT
- Anteilige Kosten Intrusion Detection System (IDS)
- Anteilige Kosten Security Information and Event Management (SIEM)
- Anteilige Kosten Information Security Management System (ISMS)
- Security as a Service (SECaaS)
- Kosten Netzsegmentierung
- Anteilige Kosten Schutz Zonenübergänge IT – OT
- Audits / - Zertifizierung
- Erstellung Inventar IT /- Log-Analyse IT

Beispiel:
- Hard- und Software für DMZ für Netzleitstelle (SCADA)
- Anteil OT Hard- und Software für Schutz Zonenübergänge
- Wartung Sicherheitssysteme in Netzleitstelle oder Unterwerken
- Kosten Schutz Energiedaten Management (EDM)
- Berater / externe Mandate /- Kosten Pen-Tests /- Audits
- Patches / Updates
- Anteilige Kosten SOC
- Schulungen der Mitarbeitenden OT
- Anteilige Kosten Intrusion Detection System (IDS) OT
- Anteilige Kosten Security Information and Event Management (SIEM) OT
- Anteilige Kosten Information Security Management System (ISMS) OT
- Security as a Service (SECaaS) OT
- Teilnahme an BugBounty Programm OT



- ELCOM-Logik: Vertretbare Kosten, keine luxuriösen, aber effizienten Lösungen.
- Man muss die Kosten begründen können

Ende

Vielen Dank für Ihre Aufmerksamkeit!

Stephane.henry@bfe.admin.ch