OT Security meets Compliance: was wollen die Regulierer?

Heiko Adamczyk
Fortinet

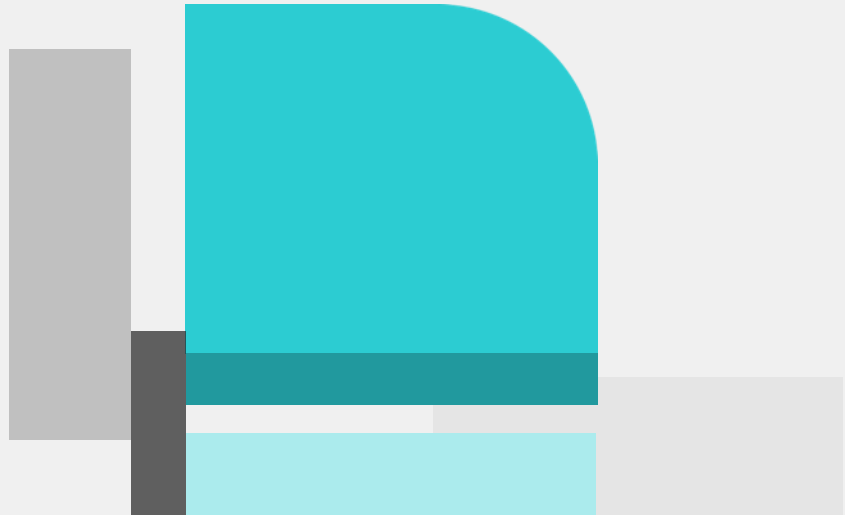
Über mich

Heiko ADAMCZYK

Business Development Manager OT / IIoT

- Electrical Engineer with Focus on Industrial Communication
- Standardization committees (since 2005):
  - VDI/VDE-GMA: Founder & Chairman FA 5.22 “Industrial Security”
  - DKE: (Founding) Member of UK 931.1
  - IEC: Member of TC65 WG10
- OT Security Life Cycle Experiences:
  - Research: 13 years national & international founded projects
  - Manufacturer: 4 years responsible for product development
  - Asset Owner: 4 years strategic projects
  - Technical Certifier: 2 years certification according IEC 62443

Wer regelt Cyber-Risiken (Fokus EMEA)?



Regulierung und Standardisierung

European

- NIS Directive (EC 2016/1148)
- Cybersecurity Act (EC 2019/881)
- *Cyber Resilience Act*

→ ENISA

National

- IT-Sicherheitsgesetz (🇩🇪: IT-SiG 2.0)
- Kritische Infrastruktur (🇩🇪: BSI-KritisV; 🇦🇹: APCIP)

→ BSI

…dienen zur Erfüllung (Konformitäts-vermutung)

Standardisierung

- ISO/IEC 27001 (Info Sec.)
- IEC 62443 (OT Security)
- ISO/IEC 27019 (Energy)

→ ISO, IEC

…werden (normalerweise) beauftragt

enisa THE EU CYBERSECURITY AGENCY

European Union Agency for Cybersecurity

ISO International Organization for Standardization (ISO)

IEC International Electrotechnical Commission (IEC)

NIS - Network and Information Security
BSI - Bundesamt für Sicherheit in der Informationstechnik
APCIP - Österreichisches Programm zum Schutz kritischer Infrastrukturen

NIS2: Richtlinie für Netz- und Informationssicherheit

Wesentliche Änderungen des neuen (fertigen) Gesetzentwurfes

- Erhöhung der Sektoren: +3 bei den Essential Sektoren & +5 bei den Important Entities
- Abschaffung der Schwellwerte: **keine** separaten **Schwellenwerte** für Betreiber **mehr**, dafür im Scope Medium und Large Enterprises (Definition gemäß 2003/361/EC)
- Höhere Anforderungen: unter anderem durch Betrachtung der **Lieferkette**
- Höhere Sanktionen: **Strafen** und Enforcement Actions werden deutlich **ausgeweitet**
- Starke Kooperation**:** Die Aufsicht und Zusammenarbeit in der EU zwischen Behörden und Betreibern werden vertieft (Cyber Crises Liaison Organisation Network [**CyCLONe**] für ein EU-weites Incident- & Kriesenmanagement; **CSIRT** Zusammenschluss für Info Sharing)

Schwerpunkt sind organisatorische Herausforderungen

Aber auch einzelne technische Herausforderungen (Monitoring!)

IT-Sicherheitsgesetz 2.0 (IT-SIG 2.0)

Nationale Umsetzung der NIS2

§8a (1a) BSIG

Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die **eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten.**

Sie sollten dazu in der Lage sein, **fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen**.

§2 (9b) BSIG

Systeme zur Angriffserkennung im Sinne dieses Gesetzes **sind** durch **technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme**. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.

Source: https://www.gesetze-im-internet.de/

IT-Sicherheitsgesetz 2.0 (IT-SIG 2.0)

§8a (1) BSIG

[KRITIS-Betreiber sind verpflichtet, ...] angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der **Stand der Technik** eingehalten werden.

§9b BSIG

Voraussetzung für ein mögliches Prüfverfahren ist, dass für einen der in § 10 Abs. 1 S.1 BSI-Gesetz genannten KRITIS-Sektoren kritische Komponenten im Sinne des § 2 Abs. 13 BSI-Gesetz festgelegt wurden

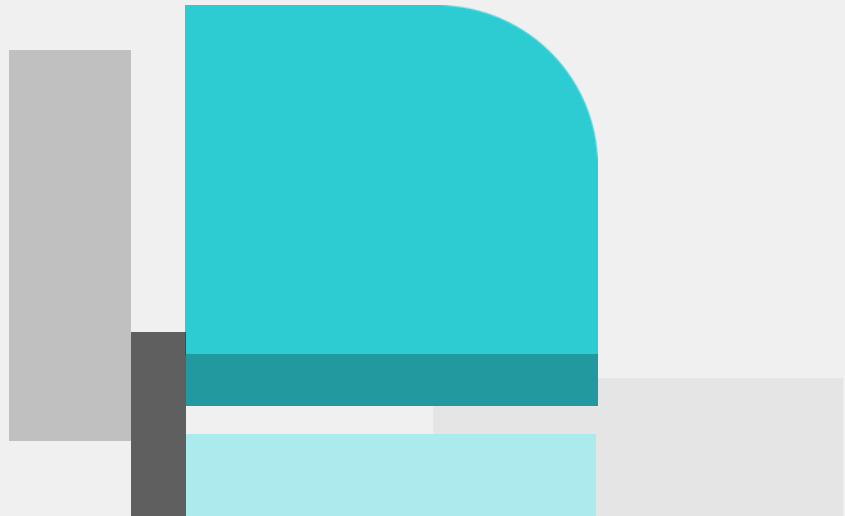
Werden für einen Sektor keine kritischen Komponenten ausdrücklich auf Grund eines Gesetzes bestimmt, bzw. keine kritischen Funktionen festgelegt, aus denen kritische Komponenten abgeleitet werden können (jeweils unter ausdrücklichem Verweis auf § 2 Abs. 13 BSI-Gesetz), **gibt es in diesem Sektor keine kritischen Komponenten** im Sinne der Regelung.

Mit der Veröffentlichung der Liste der kritischen Funktionen im Rahmen des Sicherheitskataloges nach § 109 Abs. 6 Nr. TKG am 25. August 2021 liegen die Voraussetzungen für die **Ableitung kritischer Komponenten in der Branche Telekommunikation** vor (Stichwort: 5G Komponenten)

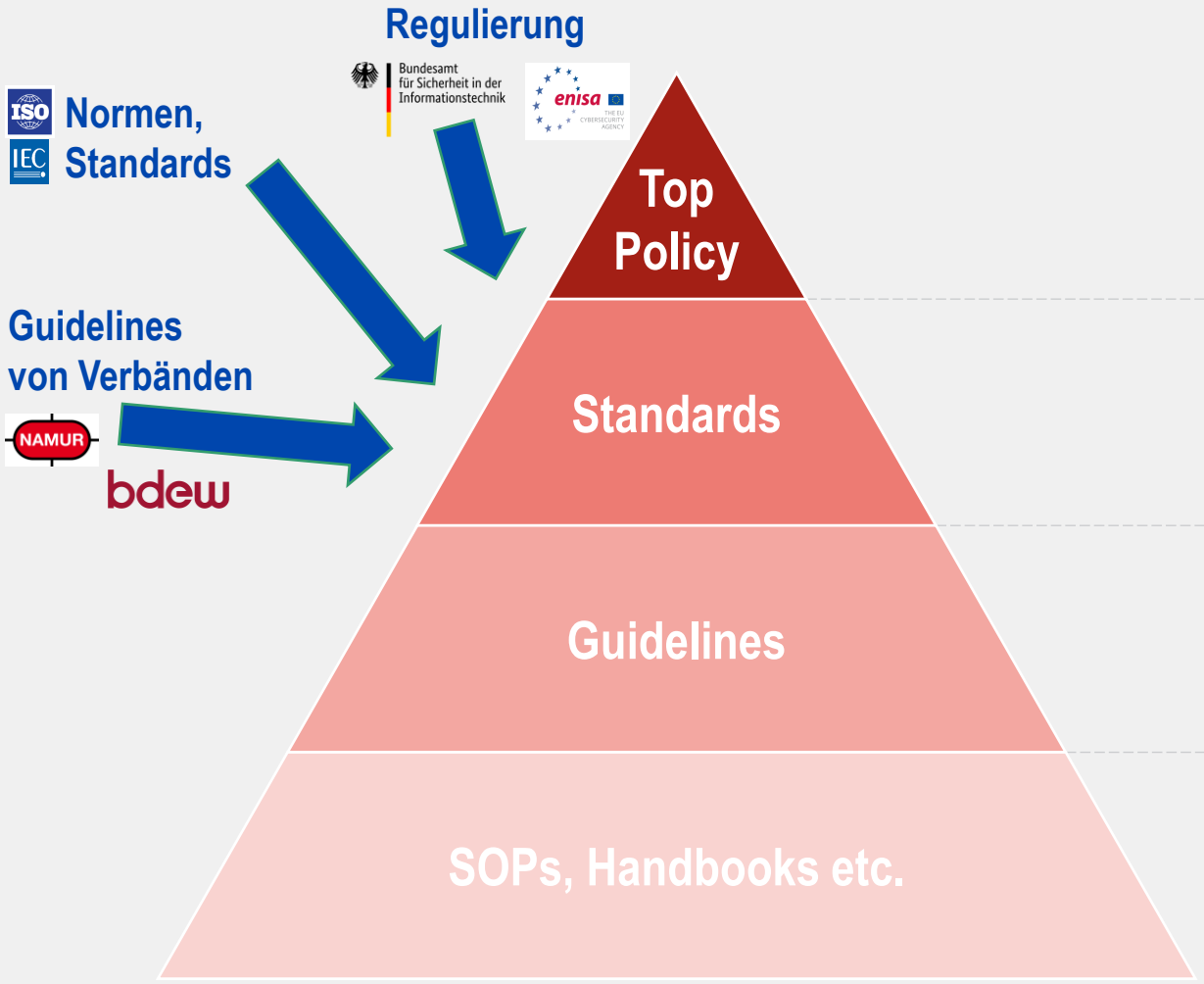
Source: https://www.gesetze-im-internet.de/

Wie erreiche ich Compliance?

Standards & Guidelines



Industrial Cyber Security als Teil der GRC Aktivitäten innerhalb eines “individuellen” Unternehmens



Policy: the policy contains the very important Management commitment, defines companies overall Security goals and principals

Standards: containing relevant requirements coming from **ISO 27001 & IEC 62443 & Domain-specific Standards**

→ Welche stellen den Regulierer zufrieden? Stand der Technik?

Detailed Guidelines: addressing the requirements and provide solutions to the standard requirements

Standard operational procedures describing a dedicated security solution

BSI: IT-Grundschutz

Seit über 25 Jahren ist der **IT-Grundschutz** dabei **Methode, Handlungsanweisung und Empfehlung**.

Er ist anwendbar für alle Institutionen, die in Zeiten der Digitalisierung ihre IT-Systeme und Datennetze und damit ihre Geschäfts- oder Verwaltungsprozesse nach dem **Stand der Technik** absichern wollen.

Forderung durch §8a (1) BSIG

BSI: Domain-spezifische Sicherheitsstandards

z.B. für Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung


bdew
Energie. Wasser. Leben.

BDEW Bundesverband
der Energie- und
Wasserwirtschaft e. V.
Reinhardtstraße 32
10117 Berlin

www.bdew.de

Branchenspezifischer Sicherheitsstandard
für

Anlagen oder Systeme zur
Steuerung / Bündelung
elektrischer Leistung
(B3S Aggregatoren)

Nach § 8a Abs. 2 BSI-Gesetz

Version: 1.1
Stand: 15.02.2021

Der Bundesverband der Energie- und Wasserwirtschaft (BDEW), Berlin, und seine Landesorganisationen vertreten über 1.900 Unternehmen. Das Spektrum der Mitglieder reicht von lokalen und kommunalen über regionale bis hin zu überregionalen Unternehmen. Sie repräsentieren rund 90 Prozent des Strom- und gut 60 Prozent des Nah- und Fernwärmeabsatzes, 90 Prozent des Erdgasabsatzes, über 90 Prozent der Energienetze sowie 80 Prozent der Trinkwasser-Förderung und rund ein Drittel der Abwasser-Entsorgung in Deutschland.

Welche **konkreten Maßnahmen innerhalb eines Sektors bzw.** einer **spezifischen Branche** geeignet sein können, **um** die im **BSI-Gesetz** abstrakt formulierten Anforderungen **umzusetzen**, wird dabei weder in der entsprechenden Rechtsnorm noch der korrespondierenden Rechtsverordnung („BSI-KritisV“) geregelt.

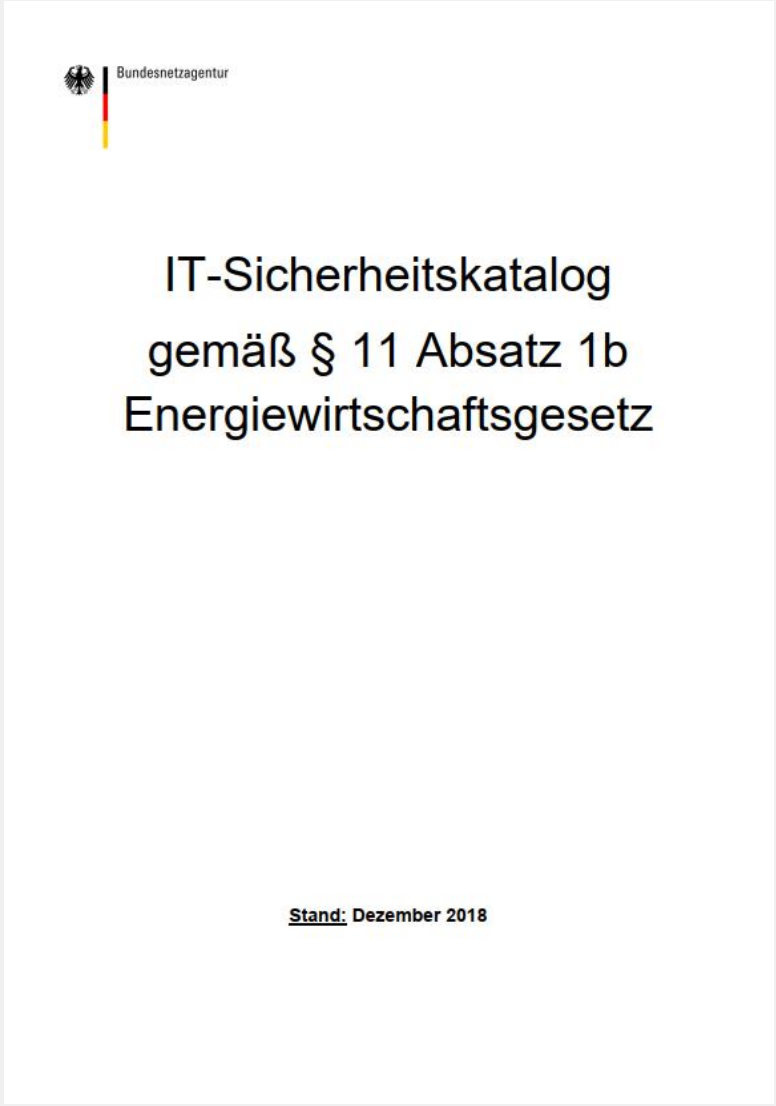
Die Branchen selbst können durch das Erarbeiten sog. branchenspezifischer Sicherheitsstandards (**B3S**) die für ihren Bereich sinnvollen und notwendigen Maßnahmen zusammenfassen und dem BSI zur Prüfung der Eignung bei der Erfüllung der im IT-Sicherheitsgesetz formulierten Ziele vorlegen.

Weitere Bespiele (Auszug):

- Ernährungsindustrie
- Pharma
- Verkehrssteuerungs- & Leitsysteme im kommunalen Straßenverkehr

BNetzA: Domain-spezifische Sicherheitsstandards

z.B. IT-Sicherheitskatalog der BNetzA für Netzbetreiber



Betreiber von Energieanlagen, die nach der BSI-KritisV als **Kritische Infrastruktur** identifiziert wurden, sind nach § 11 Abs. 1b Energiewirtschaftsgesetz (EnWG) verpflichtet, den 2018 von der Bundesnetzagentur (BNetzA) veröffentlichten IT-Sicherheits-katalog für Energieanlagen umzusetzen.

Nachgewiesen wird dies **durch ein Zertifizierungsverfahren (ISO/IEC 27001)**, das Betreiber von Energieanlagen **bis zum 31. März 2021*** abschließen und bei der BNetzA anzeigen müssen.

* durch die Corona Situation wurde die Frist angepasst, bis zum genannten Zeitraum ist ein „Erreichen der Zertifizierungsreife“ ausreichend

IEC 62443: Lebenszyklus Modell

International Standard: IEC 62443

Product Supplier

Service Provider
(System Integrator & Maintenance Provider)

Asset Owner

Produkt Lebenszyklus

Vertrauenswürdigkeit durch:

- der Entwicklungsprozess bewährten Verfahren folgt ***und*** — 4-1
- das Produkt die beanspruchten Funktionalitäten in einer definierten Umgebung erfüllt (Verwendungszweck) — 4-2

IACS Lebenszyklus

Vertrauenswürdigkeit durch:

- der Dienstleister bewährte Verfahren befolgt ***und*** — 2-4
- Der Systemintegrator kann die erforderlichen Funktionalitäten der Automatisierungslösung erfüllen — 3-3

Schutz einer integrierten Automatisierungslösung im Betrieb durch:

- Betriebs- & Wartungsrichtlinien sowie Verfahren inklusive der Personenqualifikation — 2-1 Ed.2
- funktionale Fähigkeiten des IACS in finaler Umgebung (Verwendung = Verwendungszweck) — 3-3

IEC 62443: Holistisch mit Organisation & Technik

z.B. für Betreiber im Sektor Energie

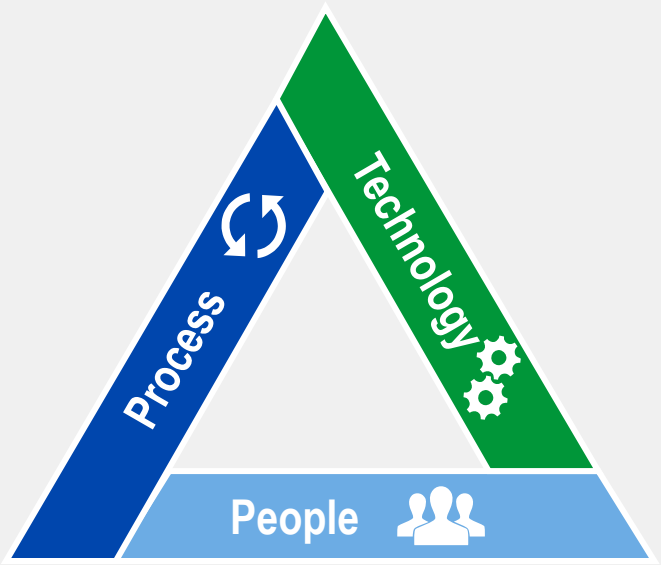
Organisatorische Anforderungen

- Organizational security measures
  - Org 1.1: ISMS (ISO/IEC 27001+27019, NIST CSF)
- Configuration management
- Network and communications security
- Component security
- Protection of data
- User access control
- Event and incident management
- System integrity and availability

IEC 62443-2-1 Ed.2

↓

Security Programm Elements



Technische Anforderungen

- Identification and Authentication Control (IAC)
- Use Control (UC)
- System Integrity (SI)
- Data Confidentiality (DC)
- Restrict Data Flow (RDF)
- Timely Response to Event (TRE)
- Resource Availability (RA)

IEC 62443-3-3 / -4-2

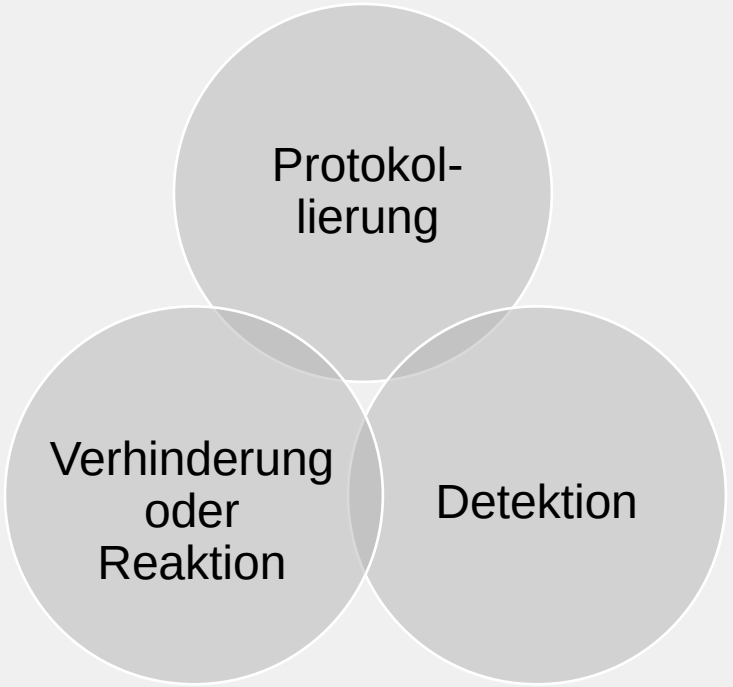
↓

Foundational Requirements

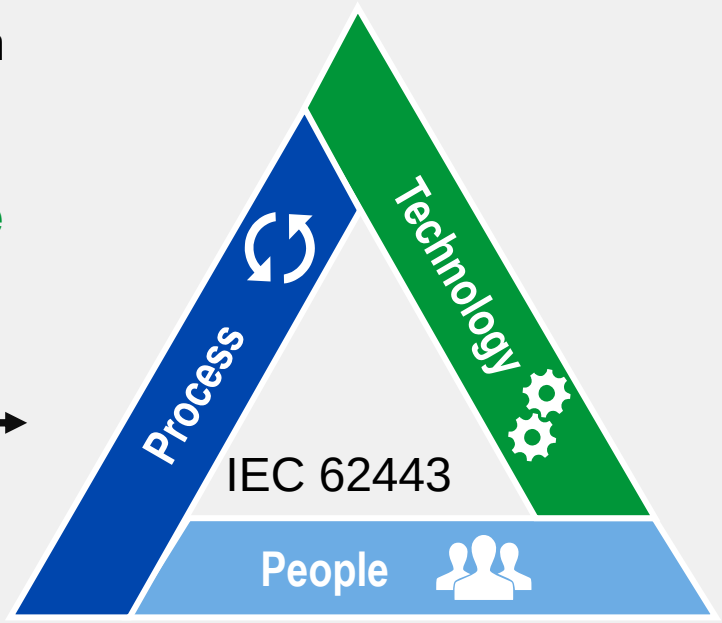
Umsetzungsaspekte

Compliance Use Case „Angriffserkennung IT-SIG“

Anforderung aus §8a (1) BSIG mit IEC 62443 begegnen



Recap: **Systeme zur Angriffserkennung** im Sinne dieses Gesetzes **sind** durch **technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse** zur Erkennung von Angriffen auf informationstechnische Systeme.



Compliance Use Case „Angriffserkennung IT-SIG“

Anforderungen aus IEC 62443 & entlang des Live Cycle

Organizational Requirements

Product Supplier

Secure Product Development Lifecycle
- Security Verification & Validation Testing (SVV)
- **Management of Security-Related Issues (DM)**
- Security Update Management (SUM)
- …

IEC 62443-4-1 (ISO 9001 & ISO/IEC 27001)

Service Provider

Security Program Requirements
- Remote access (SP.07)
- **Event management (SP.08)**
- Account management (SP.09)
- …

IEC 62443-2-4

Asset Owner Security Program Elements

Security Program Elements
- User access control (SPE 6)
- **Event and incident management (SPE 7)**
- System integrity and availability (SPE 8)

IEC 62443-2-1 Ed.2

Technical Requirements

- Identification and Authentication Control
- **Use Control (Audit)**
- System Integrity
- Data Confidentiality
- Restrict Data Flow
- **Timely Response to Event**
- Resource Availability

IEC 62443-3-3

Compliance Use Case „Angriffserkennung IT-SIG“

Beispiel Anforderungen aus IEC 62443-2-1 Ed.2 (CDV): Event and incident management (SPE 7)

Event detection

- Security management activities that include reporting, logging, analysis and response

Event reporting

- IACS events shall be reported in a **timely manner**

Event reporting interfaces

- IACS events are reportable through interfaces **commonly accepted by the industrial and security communities**

Logging

- IACS events are written to … protected event/audit logs and retained for an **adequate time period**

Log entries

- IACS security-related audit and event log entries contain information adequate to support non-repudiation and time-correlated analysis of events

Log access

- IACS event logs are accessible through interfaces **commonly accepted by the industrial and security communities**

Event analysis

- security-related events shall be analyzed to identify and characterize attacks, security compromises and security incidents

Incident handling and response

- process shall be employed and kept current for evaluating and responding to IACS security incidents

Vulnerability handling

- existing and **newly identified IACS vulnerabilities** shall be addressed and resolved

Compliance Use Case „Angriffserkennung IT-SIG“

Beispiel Anforderungen aus IEC 62443-3-3: Use control (UC)

FR 2 – Use control (UC)	SL1	SL2	SL3	SL4
Enforce the assigned privileges of an authenticated user to perform the requested action on the ICAS, monitor the use of these privileges				
SR 2.9 – Audit storage capacity	**X**	**X**	**X**	**X**
▪ Sufficient audit record storage capacity shall be available **according to commonly recognized recommendations** ▪ Auditing mechanism to reduce the likelihood of capacity being exceeded shall be implemented				
RE (1) Warn when audit record storage capacity threshold reached			**X**	**X**
▪ When the audit record storage volume reaches a configurable percentage, a warning shall occur				
SR 2.10 – Response to audit processing failures	**X**	**X**	**X**	**X**
▪ Personnel must be alerted, in case that an audit processing failure occurs to prevent loss of services and functions ▪ Appropriate actions in response to an audit processing failure shall be possible				

Compliance Use Case „Angriffserkennung IT-SIG“

Beispiel Anforderungen aus IT-Grundschutz: IND.1: Betriebs- und Steuerungstechnik

76	**IND.1 Prozessleit- und Automatisierungstechnik**		**IND.1 Prozessleit- und Automatisierungstechnik**	
77	**IND.1.A1**	Basis	Einbindung in die Sicherheitsorganisation	MUSS
78	**IND.1.A2**		ENTFALLEN	
79	**IND.1.A3**	Basis	Schutz vor Schadprogrammen	MUSS
80	**IND.1.A4**	Standard	Dokumentation der OT-Infrastruktur	SOLLTE
81	**IND.1.A5**	Standard	Entwicklung eines geeigneten Zonenkonzepts	SOLLTE
82	**IND.1.A6**	Standard	Änderungsmanagement im OT-Betrieb	SOLLTE
83	**IND.1.A7**	Standard	Etablieren einer Berechtigungsverwaltung	SOLLTE
84	**IND.1.A8**	Standard	Sichere Administration	SOLLTE
85	**IND.1.A9**	Standard	Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten	SOLLTE
86	**IND.1.A10**	Standard	Monitoring, Protokollierung und Detektion	SOLLTE
87	**IND.1.A11**	Standard	Sichere Beschaffung und Systementwicklung	SOLLTE

IND.1.A10 Monitoring, Protokollierung und Detektion
[Bereichssicherheitsbeauftragter] (S)

Es SOLLTEN betriebs- und sicherheitsrelevante Ereignisse zeitnah identifiziert werden. Hierzu SOLLTE ein geeignetes Log- und Event-Management entwickelt und umgesetzt werden. Das Log- und Event-Management SOLLTE angemessene Maßnahmen umfassen, um sicherheitsrelevante Ereignisse zu erkennen und zu erheben. Es SOLLTE zudem einen Reaktionsplan (Security Incident Response) enthalten.

Der Reaktionsplan SOLLTE Verfahren zur Behandlung von Sicherheitsvorfällen festlegen. Darin abgedeckt sein SOLLTEN die Klassifizierung von Ereignissen, Meldewege und Festlegung der einzubeziehenden Organisationseinheiten, Reaktionspläne zur Schadensbegrenzung, Analyse und Wiederherstellung von Systemen und Diensten sowie die Dokumentation und Nachbereitung von Vorfällen. Der Reaktionsplan SOLLTE regelmäßig getestet und auf Aktualität geprüft werden.

Reifegradmodell für KRITIS: mindestens STUFE 4:

Alle MUSS- Anforderungen wurden für alle Bereiche umgesetzt. **Alle SOLLTE-Anforderungen wurden umgesetzt**, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen.

Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

Alignment with Standards & Guidelines

Meet compliance requirements with Fortinet Security Fabric

Appliance | Virtual Machine | Cloud | Security-as-a-Service | Software

Asset Management
SIEM | NAC | NGFW | API

Access Control to Networks & Assets
NGFW | NAC | FAC | Client | Tokens | Proxy

Segmentation, Protection & Response
NGFW | Switch | WIFI | EDR | Tokens | Proxy

Events, Alerts and Incident Detection
SOAR | SIEM | Analyzer

Risk Management
Manager | SIEM | Analyzer | Tester

Single Pane Management

Threat Intelligence

Interoperability

Fazit

1. DACH: IT-Grundschutz, ISO 27001, IEC 62443 sind derzeit die Buidling Blocks für Compliance im Bereich OT Security
   Aber: der Regulierer fordert weitere Domainen-spezifische Standards (siehe B3S)

2. EU: bisher starke Fokussierung auf Betreiber (NIS2), wobei die Performance der Zulieferer „maßgebend“ ist
   (Cyber Resilience Act: Fokus Zulieferer, Liste harmonisierter Normen wünschenswert, Cybersecurity Act: Zertifizierung)

3. Die IEC 62443 hat Schwächen! (CSMS der 2-1), insgesamt aber eine gute Balance der o.g. Punkte
   (Stichworte: Profilbildung, Evaluationskriterien, … , Anerkennung, Trägheit)

4. Technologie Anbieter müssen “Unschärfen” der Anforderungen umsetzen … schafft Raum für proprietäre Lösungen
   (Wunsch nach „echten“ Technologie Standards, z.B. NIST SP 800-57 Key Management)

Ihr Kontakt

Heiko ADAMCZYK

Business Development Manager OT / IIoT

E: hadamczyk@fortinet.com
M: +49 151 51931854

Fortinet GmbH
Feldbergstraße 35
60323 Frankfurt a.M.
Germany

UNSERE VISION

Eine digitale Welt ermöglichen, der man immer vertrauen kann