Compliance für den Mittelstand

Fissenewert

3. Auflage 2026
ISBN 978-3-406-83242-0
C.H.BECK

(d) Pflichtmeldungen im Überblick

Regelwerk	Meldepflichtige Vorfälle	Frist/Zeitpunkt	Empfänger/Ziel	Bemerkungen	Regelwerk
NIS-2-Richtlinie	„erhebliche Sicherheitsvorfälle“	unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntnis	nationale zuständige Behörde (zB BSI in Deutschland)	Erstmeldung + Aktualisierungen + Abschlussmeldung möglich	RL (EU) 2022/2555
DS-GVO (Art. 33)	Verletzungen des Schutzes personenbezogener Daten	unverzüglich, möglichst binnen 72 Stunden	zuständige Datenschutzaufsichtsbehörde	Bei verspäteter Meldung muss Verzögerung begründet werden	DS-GVO (Art. 33)
KRITIS/BSIG / BSI-KritisV	IT-Störungen, Cyberangriffe in kritischen Infrastrukturen	Unverzüglich	BSI/zuständige Meldebehörde	Mit Geltung von RL (EU) 2022/2555 werden KRITIS-spezifische Pflichten erweitert oder überlagert	KRITIS/BSIG / BSI-KritisV
CRA (Cyber Resilience Act)	Aktiv ausgenutzte Sicherheitslücken in Produkten mit digitalen Elementen	gemäß Artikel 14 – Meldung an nationale Behörden + ENISA	nationale Behörde, ENISA	Hersteller müssen explizit melden, wenn Lücken aktiv ausgenutzt werden.	VO (EU) 2024/2847

412

Praxisbeispiel:

Ein Unternehmen implementiert eine interne „72-Stunden-Checkliste“ für DS-GVO-Meldungen. 413

Bei einem Datenleck wird innerhalb von sechs Stunden eine erste Risikobewertung erstellt, nach 24 Stunden die Erstmeldung an die Aufsichtsbehörde übermittelt und innerhalb von 72 Stunden ein Abschlussbericht nachgereicht.

(5) Lessons Learned und Reifegrad-Management

(a) Einleitung

Nach dem Vorfall ist vor dem Vorfall. Jeder kleinere oder größere Störfall liefert wertvolle Erkenntnisse darüber, wie Angriffe schneller erkannt, effizienter bekämpft oder im besten Fall ganz verhindert werden können. Der Lessons-Learned-Prozess schließt den Kreis der operativen Cybersicherheit und sorgt dafür, dass das ISMS kontinuierlich leistungsstärker wird. 414

(b) Verstehen

415 Vor der Umsetzung sollte klar sein:

- **Feedback-Loop:** Erkenntnisse aus Vorfällen müssen zurück in die Risikoanalyse (Kapitel 4) und in die Auslegung und Justierung von TOMs fließen.
- **Erkennungs-Reifegrad messen:** Kennzahlen wie Mean Time to Detect (MTTD) und Mean Time to Respond (MTTR) zeigen, ob die Erkennungs- und Reaktionsfähigkeit besser wird.
- **Lernen ist auch eine Unternehmenskultur-Frage:** Nur wenn Vorfälle ohne Angst vor Schuldzuweisung gemeldet werden können, entsteht eine Lernkultur, die zu echten Verbesserungen führt.

(c) Umsetzung – typische Maßnahmen

416
- **Lessons-Learned-Meetings:** Nach jedem größeren Incident ein strukturiertes Nachbesprechungs-Meeting („Post-Mortem") durchführen. Ziel ist nicht die Schuldfrage, sondern das Sammeln von Erkenntnissen, die in Maßnahmen überführt werden.
- **Maßnahmen-Backlog:** Eine zentrale Liste führen, in der alle Verbesserungsmaßnahmen gesammelt, priorisiert und nachverfolgt werden – von technischen Fixes, über Prozessanpassungen bis zu Schulungen.
- **Kennzahlen verfolgen:** Entwicklung von MTTD und MTTR beobachten. Sinken die Werte, deutet das auf eine bessere Detektion und schnellere Reaktion hin.
- **Management-Review:** Ergebnisse in regelmäßige Management-Reviews einbringen, damit Budgets und Ressourcen für notwendige Verbesserungen bereitgestellt werden.

Praxisbeispiel:

417 Nach einem erfolgreichen Phishing-Angriff führt ein Unternehmen ein Lessons-Learned-Meeting durch. Ergebnis: Multi-Faktor-Authentifizierung wird auf alle Konten ausgeweitet, Phishing-Trainings werden intensiviert und eine zusätzliche E-Mail-Filterregel implementiert. Drei Monate später sinkt die Klickrate auf Phishing-Mails um 60 % – ein messbarer Fortschritt in der Security-Awareness der Belegschaft.

(6) Die Cyber-Killchain und ihre Implikationen für TOMs und Reaktionszeiten
(a) Einleitung

418 Jeder Cyberangriff folgt einem wiederkehrenden Ablauf – von der Aufklärung bis zur eigentlichen Ausführung.

419 Die sog. Cyber-Killchain beschreibt diese Phasen und macht sichtbar, an welchen Punkten technische und organisatorische Maßnahmen (TOMs) ansetzen müssen, um einen Angriff so früh wie möglich zu stoppen.

420

Abb. 11: Die Killchain – typische Phasen eines Cyberangriffs

421

1. **Aufklärungs- und Ausspähphase (Reconnaissance):** Angreifer sammeln Informationen über das Ziel – oft mit OSINT-Methoden (Open Source Intelligence), um ein detailliertes Angriffslagebild zu erstellen.
2. **Angriff (Intrusion/Initial Access):** Phishing, Social Engineering oder das Ausnutzen von Schwachstellen ermöglichen den ersten Zugang.
3. **Erschließungs-Phase (Exploitation):** Der Zielrechner wird kompromittiert; der Angreifer oder die Schadsoftware übernimmt Kontrolle.
4. **Ausbreitungs-Phase (Lateral Movement).** Der Angreifer oder die Schadsoftware bewegt sich innerhalb des Netzwerks, analysiert Systeme und versucht, sich weiter auszubreiten.
5. **Erhöhung der Zugriffsrechte (Priviledge Escalation):** Ziel ist es, Administratorrechte oder besonders schützenswerte Zugänge zu erlangen.
6. **Verschleierung (Anti-Forensik)** – Mit speziellen Techniken wird die spätere forensische Untersuchung erschwert. Spuren werden verwischt, zB durch Löschen von Logfiles oder Manipulation von Systemspuren.
7. **Schadfunktion ausführen (Execution)/Persistenz:** Schadfunktionen wie Verschlüsselung, Datenabfluss oder Zerstörung werden ausgeführt – zusätzlich – **Persistenz** – es werden Hintertüren eingerichtet, um später erneut zugreifen zu können.
8. **Rückzug (Exfiltration)** Der Angreifer bzw. die Schadsoftware verlässt das Netzwerk oder geht in den „Stealth-Modus".

422 Zwischen Phase 2 (Initial Access) und Phase 6 (Anti-Forensik) befindet sich der Angreifer aktiv im Netzwerk des Opfers.

423 In dieser Zeit besteht die größte Chance, den Angriff zu erkennen und zu stoppen, bevor Schaden entsteht.

424 Je nach Netzwerkgröße, Segmentierung und Abwehrfähigkeit kann dieser Zeitraum von wenigen Minuten bis zu mehreren Tagen reichen.

425 Nachfolgende Tabelle stellt eine Art strategische Landkarte für die Verteidigung und das Zurückdrängen (Incident Response) eines Angriffs durch die in Abschnitt 5 zusammengestellten und beschriebenen TOMs dar.

426

Phase	Geeignete TOMs zur Abwehr	Reaktionszeit
Aufklärung (Reconnaissance)	Attack-Surface-Monitoring, Schwachstellenmanagement, Awareness-Trainings zu Social Engineering, Schutz sensibler Infos (LinkedIn, Website)	präventiv/kontinuierlich
Angriff (Initial Access)	MFA, E-Mail-Filter, Patch-Management, sichere Remote-Zugänge	Minuten bis Stunden
Erschließungs-Phase (Exploitation)	EDR/XDR, Application Control, Härtungsrichtlinien, Sandboxing	Minuten
Ausbreitungs-Phase (Lateral Movement)	Netzwerksegmentierung, SIEM/Logging, UEBA-Regeln	Minuten
Erhöhung der Zugriffsrechte	Privileged Access Management, Rechte-Review, Session-Recording	Minuten
Verschleierung (Anti Forensik)	Manipulationssichere zentrale Log-Speicherung, SIEM-Korrelation, schneller SOC-Eingriff	Minuten
Schadfunktion ausführen (Execution)	Notfall-Runbooks, automatisiertes Containment, Krisenstab-Aktivierung	Minuten (MTTR)
Rückzug (Exfiltration)	DLP-Systeme, Netzwerk-Monitoring, Sperrung von Datenkanälen	sofort nach Erkennung

gg) Spezialbereiche, OT-, IoT- und IIoT-Security sowie ein Exkurs zur EU-Maschinen-VO

(1) Einleitung

427 Nachdem das Werk nun einen umfassenden Werkzeugkasten technischer und organisatorischer Maßnahmen (TOMs) vorgestellt und gezeigt hat, wie diese Maßnahmen im operativen Alltag – von der Detektion bis zum Wiederanlauf – wirken, richtet es den Blick auf spezielle Anwendungsfelder und branchenspezifische Besonderheiten.

428 Im Mittelpunkt steht die Frage, wie sich die generischen Sicherheitsprinzipien aus den vorherigen Kapiteln in der Praxis gerade auch im produzierenden Gewerbe anwenden lassen – insbes.:

- in industriellen Netzen (OT), IoT- und IIoT-Umgebungen,
- in physisch-kritischen Anlagen,
- unter Einbeziehung aktueller regulatorischer Entwicklungen.

429 Dies schlägt damit die Brücke zwischen Technologie und Anwendung. Es zeigt,

- wie sich die TOMs auf IT-/OT-Architekturen, industrielle Netzwerke und IoT-Geräte übertragen lassen,
- warum physische Sicherheit und Cybersecurity miteinander verzahnt werden müssen, um echte Resilienz zu erreichen,
- wie Safety- und Security-Anforderungen in Produktions- und Steuerungssystemen integriert werden können,
- welche neuen regulatorischen Vorgaben die EU-Maschinenverordnung mit sich bringt – und warum Cybersecurity dadurch erstmals CE-relevant wird.

Abschließend rundet ein Praxisbeispiel aus dem Energie- und PV-Sektor das Kapitel ab und zeigt, wie die Bausteine in einer realen Umgebung ineinandergreifen. 430

(2) OT-Security, produzierende Unternehmen und industrielle Netzwerke

(a) Einleitung

Operational Technology (OT) bildet das Rückgrat von Produktion, Energieversorgung und kritischer Infrastruktur. Anders als in klassischen IT-Umgebungen stehen hier Produktionsanlagen, Steuerungssysteme und physische Prozesse im Mittelpunkt der Schutzmaßnahmen. Jeder Sicherheitsvorfall kann direkte Auswirkungen haben – von Produktionsstillständen über Umweltschäden bis hin zu Lieferkettenunterbrechungen – und so erhebliche finanzielle Schäden und Reputationsverluste verursachen. 431

OT-Security bedeutet daher vor allem den **Schutz der Verfügbarkeit, der Produktivitätskontinuität und der Prozessintegrität.** 432

Dieser Abschnitt beleuchtet die besonderen Security-Anforderungen an industrielle Netzwerke, die über klassische IT-Sicherheitsmaßnahmen hinausgehen. 433

(b) Verstehen

Vor der Umsetzung sollten Sie sich insbes. mit folgenden Überlegungen vertraut machen: 434

- **Andere Schutzziele:** In der IT ist Vertraulichkeit meist oberstes Ziel, in der OT hingegen ist das Verfügbarkeit und die Sicherheit[136] von Menschen und Anlagen.
- **Produktionsketten und Abhängigkeiten:** Im Bereich der Produktion und damit in der OT-Security bauen oft eine Vielzahl von Fertigungsschritten und deren Produktions-Anlagen sequentiell aufeinander auf. Fällt ein zentrales Steuerungssystem aus, kann dies die gesamte Produktion zum Stillstand bringen.
- **Lieferketten-Relevanz:** Störungen in der Produktion können kaskadierende Effekte in komplexen Supply Chains auslösen. Ein abgestimmtes Frühwarn- und Benachrichtigungssystem für Partner ist daher essenziell.
- **Lange Lebenszyklen:** OT-Systeme sind oft über Jahrzehnte bereits in Betrieb. Nach dem Prinzip „Never change a running horse" werden derartige Anlagen auch heute noch genutzt und stellen möglicherweise kritische Engpässe im Fertigungs-Gesamtprozess dar. Teilweise sind bei diesen Anlagen uralte, nicht mehr von den Herstellern gepflegte Betriebssysteme, Speicher, I/O-Geräte[137] und Maschinen-Programme im Einsatz.

[136] Gemeint ist hier tatsächlich „Sicherheit für Leib und Leben". Eine produzierende Anlage, die eklatante Fehlfunktionen durchführt, kann (Beispiel Industrieroboter) schnell auch schwere Verletzungen beim Bedienpersonal bewirken.

[137] Tatsächlich sind bis heute CNC-Werkzeugmaschinen, die noch über Lochstreifen „programmiert" oder über Lochkarten in ihren Arbeitssequenzen angeleitet werden, im produzierenden, metallverarbeitenden Gewerbe im Einsatz.

- **Nicht netzwerkgeeignet:** Viele historisch gewachsene Produktionsumgebungen nutzen Steuerungssystem, die niemals für eine Anbindung an IP-Netze ausgelegt waren. Ein unsensibles Anbinden derartiger Anlagen über Gateways schafft uU fatale Angriffsflächen und möglicherweise ungeschützt über das Web frei steuerbare Fernzugänge.
- **Lokale und zeitlich eng begrenzte Wartungszugriffe,** Patches oder Upgrades können häufig nur direkt an den Anlagen und nur in differenziert geplanten Wartungsfenstern durchgeführt werden.
- **Protokolle und Standards:** Viele OT-Protokolle (zB Modbus, Profinet) wurden ohne Security-Mechanismen entwickelt und benötigen heute zusätzliche Schutzschichten.
- **Fernwartung und Remote Access:** Um Wartungsunternehmen und Servicetechniker nicht für jeden Eingriff in Produktionsanlagen ins Unternehmen holen zu müssen sind Remote Access Zugänge nahezu unverzichtbar. Schlecht konfiguriert stellen diese Zugänge aber eine Hauptangriffsfläche für hochspezialisierte Cyberangriffe (zB APT-Exploiting-Routinen) dar.
- **Regulatorische Einbettung:** Die Norm IEC 62443 bietet ein umfassendes Rahmenwerk (Zonen- und Kondukte-Modelle, Risikomanagement, Security Levels).

(c) Umsetzung – typische Maßnahmen

435

- **Zonen- und Segmentierungs-Architektur:**
  - Produktionsnetz vom Büro-IT-Netz trennen.
  - Sicherheitszonen definieren (zB Büro-IT, OT-DMZ als Pufferzone, SCADA- oder Steuerungsebene).
  - Kondukte sind definierte, kontrollierte Kommunikationspfade zwischen diesen Zonen – sie werden über Firewalls oder Industrial Security Appliances abgesichert.
- **Patch- und Wartungsstrategie:**
  - Patchfenster planen und in Testumgebungen vorab prüfen.
  - Virtuelles Patching: Wenn kein Hersteller-Patch verfügbar ist, können Intrusion-Prevention-Systeme (IPS) oder spezielle Firewall-Regeln die Schwachstelle temporär schließen.
- **Miteinander verzahnte Produktionsschritte und Lieferketten-Abhängigkeiten kennen und beachten.**
  - Die Lieferketten, die darin verorteten Partner und die Produkt-Abhängigkeiten genau zu kennen schafft längere Reaktionszeiten bei Ausfällen.
  - Gegebenenfalls Redundanzen und alternative Produktionsverfahren vorsehen.
  - Ein Lieferketten-Störungs-Frühwarnsystem konzipieren und etablieren.
- **Fernwartung absichern:**
  - Zentrale Zugangspunkte nutzen (Jump-Hosts oder Bastion-Hosts = kontrollierte Einstiegssysteme).
  - Zeitlich befristete Freigaben („Just-in-Time-Access"), MFA und vollständige Protokollierung erzwingen.
- **Monitoring:** Alle Remote-Sitzungen mitschneiden oder zumindest loggen.
- **Sensible Einbindung alter Anlagen in moderne Netze**
  - IIoT-Systeme und Gateways hin zu IP-Netzwerken sehr sensibel vorab evaluieren (Risikoanalyse);
  - Kontinuierliche Sicherheitsprüfungen (zB Penetrationstests) einplanen.
  - Know-how zu veralteten Betriebssystemen und Programmiersprachen sichern.
- **Monitoring auf Anlagenebene:**
  - Deep Packet Inspection für OT-Protokolle nutzen.
  - Anomalieerkennung für unzulässige Befehle
  - Whitelisting für zulässige Kommunikation zwischen Automatisierungs- und Steuerungssystemen beachten.

- **IEC 62443-Bezug:**
  - Security Levels (SL1–SL4) definieren: SL1 = Grundschutz, SL4 = höchster Schutz vor gezielten Angriffen.
  - Rollen, Policies und Audit-Intervalle dokumentieren und regelmäßig überprüfen.

Praxisbeispiel:
Ein Energieversorger implementiert ein Zonen- und Kondukte-Modell nach IEC 62443: Das Büro-IT-Netz, die OT-DMZ[138] und das SCADA-Netz[139] werden durch Industrial Firewalls voneinander getrennt. Fernwartung erfolgt über einen gesicherten Remote-Zugang mit MFA und Session-Recording. Bei einer späteren Malware-Infektion in der Büro-IT bleibt die Prozesssteuerung unbeeinträchtigt – die Stromversorgung läuft stabil weiter. 436

(3) IIoT/IoT-Security

(a) Einleitung

Das Internet of Things (IoT) und seine industrielle Variante, das Industrial Internet of Things (IIoT), verbinden Maschinen, Sensoren, smarte Unternehmensbereiche, Gateways und Cloud-Dienste mit dem WWW und zu einem IP-basierten, hochvernetzten Ökosystem. Diese Vernetzung eröffnet enorme Effizienz- und Komfortgewinne – erhöht aber auch die Angriffsfläche dramatisch. 437

Angreifer nutzen oft schlecht gesicherte IIoT-Gateways und smarte Unternehmens-Devices als Einstiegspunkt in Netze oder für den Aufbau von Botnetzen (zB Mirai). Dieser Abschnitt zeigt, wie Unternehmen ihre IIoT-/IoT-Umgebungen von Anfang an sicher gestalten. 438

(b) Verstehen

Vor der Umsetzung sollte klar sein: 439

- Exponentielle Angriffsfläche: Hunderte oder tausende vernetzte Geräte, oft unkonfiguriert oder mit Standard-Passwörtern, können die Sicherheitsarchitektur sprengen.
- **Lebenszyklus-Management ist Pflicht:** IIoT-Geräte dürfen nicht „installiert und vergessen" werden – ohne Updates entstehen Langzeitrisiken.
- **Ungeplante Vernetzung:** Wartungsfirmen ersetzen manchmal nicht vernetzte Steuerungen durch IIoT-Versionen und schaffen so unbeabsichtigt Internet-Angriffsflächen.
- **Default Credentials sind tödlich:** Werksvoreinstellungen mit Einfachst-Passwörtern oder Hardcoded Keys sind nach wie vor eines der häufigsten Einfallstore.
- Physische Schnittstellen: Ungesicherte USB-Ports oder offene Debug-Schnittstellen können zu Kompromittierungen führen.
- Funknetze mitdenken: Gerade smarte IoT- und IIoT-Devices funken häufig in unterschiedlichsten Frequenzbändern weit über das Unternehmensgelände hinaus. Billigst verbaubare SoCs mit Funk-Komponenten für WiFi, Bluetooth, ZigBee, LoRa-WAN usw. werden in IoT und IIoT Devices implementiert und nahezu ungeschützt (generische Einfachpassörter, im Internet jederzeit auffindbar) auch in bisher gut abgeschirmte Produktionsbereiche (oft aus Unwissenheit) eingebaut.

[138] Die OT-DMZ (Operational Technology – Demilitarized Zone) ist eine Sicherheitszone zwischen dem Büro-IT-Netzwerk und dem Produktionsnetz. Sie dient als Puffer, in dem Daten- und Kommunikationsflüsse kontrolliert und gefiltert werden, bevor sie in die sensiblen OT- oder SCADA-Bereiche gelangen. Typische Komponenten in der OT-DMZ sind Protokollkonverter, historische Server oder Terminal-Server. Ziel ist es, eine klare Trennung zwischen IT- und OT-Systemen zu gewährleisten und Angriffe aus dem Büro- oder Internetbereich abzufangen, bevor sie die Prozesssteuerung erreichen.

[139] SCADA (Supervisory Control and Data Acquisition) bezeichnet Systeme zur Überwachung und Steuerung von Industrieanlagen. Sie erfassen Prozessdaten in Echtzeit, visualisieren sie für Bediener und ermöglichen Eingriffe in die Anlagensteuerung.

- Edge und 5G: Mit der Verlagerung von Intelligenz in kleine, dezentrale Produktionsserver (Edge Computing) und mit direkter Cloud-Anbindung über 5G von Maschinen, steigt die Komplexität der Sicherheitsarchitektur und eröffnen sich signifikant mehr Angriffsflächen.

(c) Umsetzung – typische Maßnahmen

440
- Inventarisierung und Sichtbarkeit:
  - Alle IoT-/IIoT-Geräte erfassen (Typ, Firmware-Version, Standort, Verantwortlicher).
  - Gegebenenfalls Scanner nutzen/etablieren zur Erkennung nicht geplanter Funknetze und deren Verursacher (nicht beachtete „Funknetz-Qualitäten" von IoT-/ IToT-Devices und -Gateways).
  - Passive Discovery-Tools einsetzen, um auch „vergessene" oder Schatten-Devices aufzuspüren.
- Bewusste Konfiguration und Sicherer Rollout:
  - Werkspasswörter ändern, nur starke, individuelle Credentials verwenden.
  - Standard-Ports, unnötige Protokolle und Dienste deaktivieren.
  - Nicht genutzte Funknetzwerke abschalten
  - USB-Ports mechanisch blockieren
  - Secure Boot aktivieren um Manipulation von Firmware verhindern.
- Update- und Patch-Management:
  - Firmware-Update-Prozess etablieren, regelmäßige Aktualisierungen einplanen.
  - Überwachung von Hersteller-Security-Advisories und CVEs.
  - Automatisierte, signierte Updates bevorzugen – inklusive Fallback-Möglichkeit bei fehlerhaften Updates.
- Netzwerkarchitektur konsequent planen:
  - Produktions- bzw. auf Produktionssystemen nachträglich aufgebrachten IIoT-Devices von Büro- und Verwaltungsnetzen trennen (eigene VLANs oder Mikrosegmentierung).
  - Kommunikation auf erlaubte Ziele beschränken (Allow-Lists).
  - TLS/DTLS-Verschlüsselung[140] für Geräte-zu-Cloud-Kommunikation.
- Edge- und 5G-Sicherheit:
  - Zero-Trust-Architektur[141] auf Edge-Devices[142] anwenden.
  - Network Slicing[143] in 5G-Umgebungen mit klaren Sicherheitszonen einführen.
  - Remote Attestation[144] und Gerätezertifikate einsetzen.

[140] TLS (Transport Layer Security) und DTLS (Datagram Transport Layer Security) sind Verschlüsselungsprotokolle, die die Kommunikation zwischen Geräten und Servern absichern. Sie sorgen dafür, dass Daten während der Übertragung weder mitgelesen noch manipuliert werden können. TLS wird für verbindungsorientierte Protokolle (zB HTTPS), DTLS für verbindungslose Protokolle (zB UDP) eingesetzt.

[141] Zero Trust ist ein Sicherheitsansatz, bei dem kein Gerät, Nutzer oder Netzwerk standardmäßig als vertrauenswürdig gilt – selbst dann nicht, wenn es sich innerhalb des Unternehmensnetzwerks befindet. Jeder Zugriff muss authentifiziert, autorisiert und protokolliert werden („never trust, always verify").

[142] Edge-Devices sind dezentrale Rechenknoten, die Datenverarbeitung nahe an der Datenquelle durchführen – zB direkt in der Produktionshalle oder an der Maschine. Dadurch werden Latenzen reduziert und Daten müssen nicht immer zuerst in die Cloud oder auf zentrale Produktionsserver übertragen werden.

[143] „Network Slicing" bezeichnet das Erstellen mehrerer virtueller, logisch getrennter Netzwerke auf derselben physischen 5G-Infrastruktur. Jedes Slice kann eigene Sicherheits- und Qualitätsparameter haben, zB für besonders kritische Produktionssysteme.

[144] Remote Attestation ist ein Sicherheitsmechanismus, bei dem ein Gerät beim Verbindungsaufbau kryptografisch nachweist, dass es sich in einem vertrauenswürdigen Zustand befindet – zB dass seine Firmware unverändert ist. Erst nach erfolgreicher Prüfung wird die Verbindung zugelassen.