Verband der
Chemischen Industrie e.V.
Wir gestalten Zukunft.

VCI-STATUSPAPIER ZUR

Cybersicherheit in der Chemie -Risikobasiertes Vorgehen

Responsible Care – ein Beitrag zur Nachhaltigkeitsinitiative Chemie3

CHEMIE3 DIE NACHHALTIGKEITSINITIATIVE DER DEUTSCHEN CHEMIE

Getragen von:
Wirtschaftsverband VCI,
Gewerkschaft IG BCE und
Arbeitgeberverband BAVC

Mitwirkende

Jörg Becker	TÜV SÜD
Benedikt Bittcher	Wacker
Jens Cordt	BSI
Stephan Gebhard	LANUV NRW (Gast)
Hartmut Manske	Merck
Markus Runde	BASF
Jan Russmann	DOW
Christoph Thust	Evonik
Tobias Unglaube	Bayer

Inhaltsverzeichnis

Vorwort

Das Statuspapier beschreibt in allgemeiner Form ein in der Chemie angewendetes Verfahren zum Etablieren einer Cybersicherheit mit dem Ziel Leib, Leben und Umwelt zu schützen. Um hierzu eine rechtsgebiets- und interessenübergreifende Abstimmung zu erreichen, erfolgte die Erarbeitung unter Beteiligung von Betreibern, Behörden und Prüforganisationen.
Das im Statuspapier beschriebene risikobasierte Vorgehen greift die Vorgehensweisen aus der ISO 27001, IEC 62443-2-1 bzw. des BSI IT-Grundschutzes auf. Eine vertiefende Betrachtung und Beschreibung der Vorgehensweise enthält das noch in Bearbeitung befindliche BSI IT-Grundschutzprofil „Chemie“.
Zur Unterstützung bei der Umsetzung des Themas in der Praxis dienen u. a. die einschlägigen NAMUR-Publikationen wie NA 163 und NA 169.

Charakteristika von Chemieanlagen und Ausgangssituation

Chemieanlagen sind individuell und komplex. Des Weiteren sind sie i. d. R. genehmigungsbedürftig. Im Rahmen des Genehmigungsverfahrens werden verschiedene Rechtsgebiete geprüft (GefStoffV, 12. BImSchV, etc.). Die Cybersicherheit mit ihren Schutzzielen ist hierbei grundsätzlich relevant, sowohl wirtschaftlich als auch zum Schutz von Menschen und Umwelt. Rechtliche Verpflichtungen zur Umsetzung der erforderlichen Cybersicherheit resultieren derzeit im Wesentlichen aus dem Störfallrecht sowie aus dem Arbeitsschutzrecht, hier insbesondere der Betriebssicherheitsverordnung.
Konkretisierungen zur Cybersicherheit finden sich im untergesetzlichen Regelwerk (z. B. IEC 62443, dem ICS-Kompendium des BSI oder dem Leitfaden KAS 51) sind aber aufgrund des mangelnden Abgleichs mit den oben genannten Rechtsvorschriften nicht unmittelbar anwendbar. Insbesondere das Zusammenspiel von Methoden der klassischen Safety (SIL etc.) mit Methoden der Cybersicherheit ist zu konkretisieren, um Rechtssicherheit sowohl für die betroffenen Betreiber als auch für die zuständigen Behörden und die Prüforganisationen zu erreichen.
Dieses Dokument bezieht sich auf die in den o. g. Rechtsgebieten beschriebenen Schutzziele. Wirtschaftlich relevante Aspekte erfordern bisher bereits vielfach Cybersicherheitsmaßnahmen, welche ebenso zu dem rechtlich geregelten Schutz von Menschen und Umwelt beitragen.
Der Umfang der erforderlichen Maßnahmen zur Erreichung der Schutzziele aus den verschiedenen Rechtsgebieten richtet sich nach der möglichen Gefährdung. Ein risikobasiertes Vorgehen unter Berücksichtigung der anlagenspezifischen Eigenschaften und Randbedingungen ist im Bereich der „Safety“ üblich und wegen der individuellen und komplexen Charakteristik von Chemieanlagen notwendig. Das klassische Vorgehen der „Safety“ wendet hierfür etablierte Methoden an. In einer übergeordneten Sicherheitsbetrachtung werden u. a. die erforderlichen prozessleittechnischen Schutzfunktionen ermittelt und die an sie zu stellenden Zuverlässigkeitsanforderungen definiert. Darauf aufbauend ist im Rahmen der Bewertung von Aspekten der Cybersicherheit zu klären, ob Cyberbedrohungen übergeordnete Sicherheitsbetrachtungen in Frage stellen

oder die Zuverlässigkeit der „Safety-Maßnahmen“ beeinträchtigen. Hierbei wird analog zur Safety häufig ein risikobasiertes Vorgehen gewählt.
Systeme einzusetzen, die sowohl betriebliche als auch Sicherheitsfunktionen (z. B. PLT-BS gemäß VDI/VDE 2180) abdecken, ist zumindest bei den Großunternehmen der Chemischen Industrie tendenziell rückläufig. Im Zuge neuer Anlagenprojekte werden höhere Sicherheitsfunktionen (SIL ≥ 1) vorzugsweise wieder vom betrieblichen PLS getrennt. Dieses Vorgehen vermeidet Diskussionen zu formalen Restriktionen bei der Nutzung von Sicherheitsfunktionen im betrieblichen PLS und erleichtert vor allem die Darstellung zusätzlicher Barrieren der Cybersicherheit.

Risikobasiertes Vorgehen

Das risikobasierte Vorgehen erfolgt in zwei Schritten.

1. Bei der Festlegung des Cyberschutzbedarfs wird das Risiko einer Gefährdung von Leib, Leben und Umwelt als zentrales Kriterium berücksichtigt.
2. Bei der Festlegung und Umsetzung der erforderlichen Cybersicherheitsmaßnahmen ist das Risiko einer erfolgreichen Kompromittierung von Systemen unter Berücksichtigung des ermittelten Cyberschutzbedarfs maßgeblich.

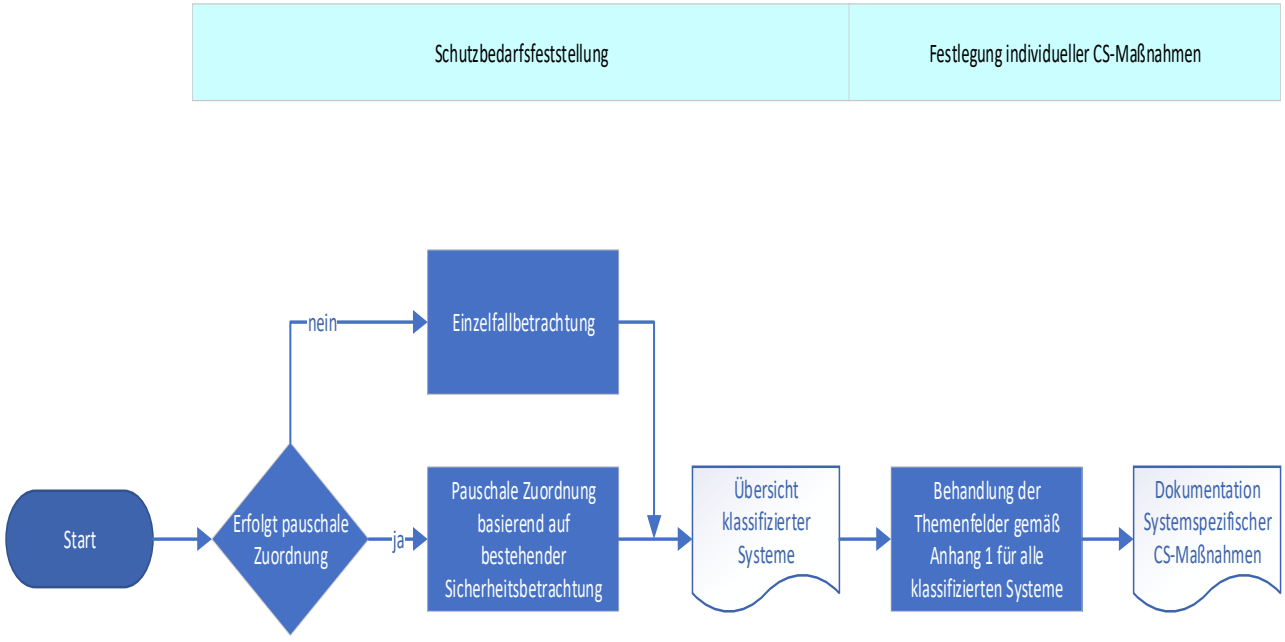

Abbildung 1 Risikobasiertes Vorgehen

Risikobasiertes Vorgehen zur Cyberschutzbedarfsfeststellung

Bestimmung des Cyberschutzbedarfes

Klassische Sicherheitsbetrachtungen (Safety) bewerten das Risiko im Sinne der Eintrittswahrscheinlichkeit von Ereignissen und deren Auswirkungen. Da die Eintrittswahrscheinlichkeit einer Cyberbedrohung von verschiedenen Faktoren abhängt, die nicht ausreichend quantifizierbar sind, ist lediglich eine qualitative Abschätzung möglich.
Der Cyberschutzbedarf ergibt sich damit im Wesentlichen aus den möglichen Auswirkungen der Kompromittierung verfahrenstechnischer Funktionen. Zu welchen Auswirkungen Fehlfunktionen führen können, wird in der Safety umfangreich beurteilt.
Es ist zu hinterfragen, ob die zugrundeliegenden Szenarien aus der Safety auch unter Berücksichtigung von Cyberbedrohungen weiterhin abdeckend sind.
Für die bereits in der Sicherheitsbetrachtung bewerteten Auswirkungen einzelner Fehlfunktionen ist es unerheblich, ob diese Fehlfunktionen durch eine Kompromittierung oder eine fehlerhafte Komponente verursacht werden. Der Cyberschutzbedarf steht deshalb im Zusammenhang mit den Ergebnissen der Sicherheitsbetrachtung. Die Höhe des Cyberschutzbedarfs orientiert sich damit am maximalen Safety-Schutzbedarf der Funktionen des jeweiligen Betrachtungsumfanges.
Im Folgenden wird durch eine Verknüpfung des Cyberschutzbedarfes mit dem Safety-Schutzbedarfes ein vereinfachtes Vorgehen bei der Festlegung der erforderlichen Cyberschutzmaßnahmen beschrieben.
Alternativ kann der Cyberschutzbedarf auch im Rahmen von Einzelfallbetrachtungen ermittelt werden. Alle datentechnischen Systeme, die für die Sicherstellung der Funktion erforderlich sind (Angriffsziel) sowie die datentechnischen Systeme, die mit diesen Systemen temporär oder dauerhaft verbunden sind (Angriffsweg), sind gemäß des festgelegten Cyberschutzbedarfs zu schützen.
Da ohne vertiefte detaillierte Untersuchung nicht ausgeschlossen werden kann, dass durch Cyberbedrohungen und deren Einfluss auf das Prozessleitsystem bzw. betriebliche Einrichtungen Anlagenzustände ausgelöst werden können, die durch die Ergebnisse der Sicherheitsbetrachtung nicht abgedeckt werden, sind auch für diese Systeme die jeweiligen Cyberschutzbedarfe festzulegen.
Weitergehende Informationen bzgl. der Kategorisierung des Cyberschutzbedarfs können dem BSI-Standard 200-2 IT-Grundschutz-Methodik entnommen werden. Die nachfolgende Terminologie der Klassifizierung der Schutzbedarfe orientiert sich an dem vorgenannten Dokument[1].
Die Ergebnisse der Cyberschutzbedarfsfeststellung für die betrachteten Systeme sind in einer Übersicht zu dokumentieren.

[1] https://www.docsetminder.de/it-grundschutz-bsi-200-2-und-200-3

Sehr hoher Schutzbedarf

Für Sicherheitsfunktionen ≥ SIL 1 ist ein sehr hoher Cyberschutzbedarf erforderlich.

Hoher Schutzbedarf

Ein hoher Cyberschutzbedarf für Sicherheitsfunktionen < SIL 1 (z. B. PLT-BS) ist für Einrichtungen erforderlich, die im betrieblichen PLS umgesetzt sind, da durch diese Einrichtungen eine geringere Risikoreduzierung als durch SIL-klassifizierte Einrichtungen gewährleistet wird.
Erfolgt für das Prozessleitsystem bzw. betriebliche Einrichtungen keine Einzelfallbetrachtung, so ist aus vorgenannten Gründen auch für diese Systeme von einem hohen Cyberschutzbedarf auszugehen.
In der Regel ist bereits aus Gründen der Wirtschaftlichkeit (Verfügbarkeit der Anlagen und Produktqualität) ein Cyberschutzbedarf erforderlich, der schon einen ausreichendend Abdeckungsgrad auch für die vorgenannten Sicherheitsfunktionen und Prozessleitsysteme bzw. betrieblichen Einrichtungen bietet.
Bei der Bewertung vorhandener Cyberschutzmaßnahmen sind alle beteiligten Komponenten zu berücksichtigen. Diese Bewertung muss alle benötigten Komponenten der Datentechnik und Infrastruktur berücksichtigen, z. B. auch Bedrohungen gemeinsam genutzter Komponenten, wie Bussysteme oder Netzwerkkomponenten einbeziehen.

Normaler Schutzbedarf

Dieses Dokument bezieht sich auf die sicherheitsrelevanten Aspekte. Deshalb ist der normale Cyberschutzbedarf in diesem Kontext nicht relevant.

Einzelfallbetrachtung

Alternativ zur Einstufung des zu erreichenden Niveaus sehr hoch/hoch sind Cyberschutzmaßnahmen szenarienbasiert und anlagenspezifisch zu bewerten.
Da Cyberangriffe vorsätzliche Handlungen darstellen, ist ihre Eintrittswahrscheinlichkeit nicht mit vergleichbaren statistischen Mitteln zu bestimmen, wie es im Fall der klassischen Safety erfolgt. Darüber hinaus korreliert der durch den Angreifer gewählte Zeitpunkt eines Angriffes nicht mit der in üblichen Risikobetrachtungen festgelegten Aufenthaltswahrscheinlichkeit von Personen im betroffenen Bereich. Insofern kann sich ein abgestufter Schutzbedarf lediglich an der Schwere der Auswirkungen orientieren. Die bisher bestehende Safety-Klassifizierung einer Sicherheitsfunktion kann somit nicht unmittelbar auf den erforderlichen Cyberschutzbedarf übertragen werden.
Der erforderliche hohe Aufwand individueller Analysen zur Ermittlung der geeigneten Cyberschutzmaßnahmen ist bei der Entscheidungsfindung für Einzelfallbetrachtungen zu berücksichtigen.

Festlegung anlagenspezifischer Cyberschutzmaßnahmen

Cybersicherheit erfordert eine Vielzahl unterschiedlicher Maßnahmen. Ziel ist es hierbei immer, ein ausreichendes Cybersicherheitsniveau für die betrachtete Sicherheitsfunktion zu gewährleisten. Dies kann durch eine geeignete Kombination von technischen und organisatorischen Maßnahmen erreicht werden.
Den spezifisch festzulegenden Cyberschutzmaßnahmen übergeordnet gibt es grundsätzliche Themenfelder, die in diesem Zusammenhang bearbeitet werden müssen. Der Themenkatalog im Anhang 1 beschreibt, zu welchen Themenfeldern geeignete Maßnahmen festzulegen und umzusetzen sind. Im Einzelnen sind dies:

- Informationssicherheits-Management
- Netzwerkarchitektur & Netzwerksicherheit
- Systemhärtung / Funktionsreduktion
- Schutz vor Malware
- Fernzugriff
- Sichere Installation und Modifikation
- Zutrittsbeschränkungen
- Überwachung des OT-Systems und seiner Datenkommunikation
- Training / Sensibilisierung

Des Weiteren enthält der Themenkatalog 50 praktische Fragen für eine strukturierte Vorgehensweise zur Festlegung der Cyberschutzmaßnahmen.
Die Festlegung der erforderlichen Cyberschutzmaßnahmen für Chemieanlagen ist in einer statischen, dauerhaften und abschließenden Checkliste wegen der Charakteristika dieser Anlagen nicht möglich. Im Detail sind es die vielfältigen Netzwerkstrukturen und Assets sowie der unterschiedliche Cyberschutzbedarf bei unterschiedlichen Cyberbedrohungen der verwendeten Systeme. All dies unterliegt darüber hinaus einer dynamischen zeitlichen Entwicklung. Letztlich sind auch bei den Maßnahmen vielfältige Kombinationen bzw. Konzepte zur Abdeckung des Cyberschutzbedarfs möglich.
Deshalb erfolgt die Festlegung der erforderlichen Cyberschutzmaßnahmen unter Berücksichtigung der Themenfelder und des Cyberschutzbedarfs auf Basis der für die verwendeten IT/OT-Systeme der jeweiligen Anlage relevanten Cyberbedrohungen[2]. Zur Ermittlung der Cyberbedrohungen kann der BSI-Grundschutz als Hilfestellung dienen. Ein spezifisches Grundschutzprofil für die Chemische Industrie ist derzeit in Vorbereitung. Bei der Festlegung und Umsetzung der erforderlichen Cyberschutzmaßnahmen gegen Cyberbedrohungen werden ggf. bereits vorhandene Cyberschutzmaßnahmen berücksichtigt.

[2] Cyberbedrohung bezeichnet gem. Verordnung (EU) 2019/881 einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte. In den Dokumenten des BSI wird in diesem Zusammenhang von Gefährdungen gesprochen.

Des Weiteren gibt es eine Vielzahl an Regelwerken/Erkenntnisquellen, welche zur Ableitung geeigneter Cyberschutzmaßnahmen herangezogen werden können wie z. B. ICS-Kompendium, IEC 62443, NIST SP 800-82.
Für das betriebliche PLS werden Cyberschutzmaßnahmen, welche einen hohen Schutzbedarf abdecken, üblicherweise als ausreichend angesehen. Dies liegt darin begründet, dass folgende Aspekte einen erfolgreichen Angriff zusätzlich erschweren:

- Es sind besondere verfahrenstechnische und anlagenbezogene Spezialkenntnisse erforderlich.
- Die Manipulationen müssen an mehreren – häufig an vielen - Stellen wirksam werden und Fehlzustände auslösen.
- Betriebliche regelungstechnische Einrichtungen der Anlage wirken Fehlzuständen kontinuierlich entgegen.
- Bedienpersonal kann ggf. korrigierend in das Prozessleitsystem und die Anlage vor Ort eingreifen und somit Fehlzuständen ebenfalls entgegenwirken.

Weitere Schritte zum Erreichen und dauerhaftem Aufrechterhalten der erforderlichen Cybersicherheit sind nicht Teil dieses Dokumentes. Hierzu wird auf die einschlägigen gesetzlichen Regelwerke einschließlich relevanter Normen und Standards verwiesen.

Ansprechpartner: Dipl.-Ing. Thilo Höchst
Abteilung Wissenschaft, Technik und Umwelt
Bereichsleiter Umweltschutz, Anlagensicherheit, Verkehr
T +49 (69) 2556-1507| **E** hoechst@vci.de

Verband der Chemischen Industrie e.V. – VCI
Mainzer Landstraße 55
60329 Frankfurt

www.vci.de | www.ihre-chemie.de | www.chemiehoch3.de

LinkedIn | Twitter | YouTube | Facebook

Datenschutzhinweis | Compliance-Leitfaden | Transparenz

- Registernummer des EU-Transparenzregisters: 15423437054-40
- Der VCI ist unter der Registernummer R000476 im Lobbyregister, für die Interessenvertretung gegenüber dem Deutschen Bundestag und gegenüber der Bundesregierung, registriert.

Der Verband der Chemischen Industrie (VCI) vertritt die Interessen von rund 1.900 Unternehmen aus der chemisch-pharmazeutischen Industrie und chemienaher Wirtschaftszweige gegenüber Politik, Behörden, anderen Bereichen der Wirtschaft, der Wissenschaft und den Medien. 2021 setzten die Mitgliedsunternehmen des VCI rund 220 Milliarden Euro um und beschäftigten mehr als 530.000 Mitarbeiterinnen und Mitarbeiter.

Anhang 1 – Themenkatalog

Der untenstehende Themenkatalog enthält praktische Fragen für eine strukturierte Vorgehensweise zur Festlegung der Cyberschutzmaßnahmen. Die Fragen ermöglichen den Einstieg in eine Erstbewertung der Cybersicherheit im Sinne dieses Dokumentes. Eine negative Antwort stellt dabei einen erklärungsbedürftigen Zustand dar. Eine positive Antwort sollte durch umgesetzte Prozesse und Cyberschutzmaßnahmen belegbar sein.

Themen der Cybersicherheit	Fragen	IEC62443-Bezug	BSI-Kompendium-Bezug	KAS-51-Bezug	Beispiel / Hilfestellung
1) Informationssicherheits-Management	Gibt es ein Security*-Managementsystem?	prEN IEC62443-2-1:2019: ORG 1.1: Information security management system	ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie durch die Leitung ISMS.1.A13 Dokumentation des Sicherheitsprozesses (S)	7.2.1 Einführung eines Sicherungsmanagements	z.B. basierend auf ISO27k, BSI Kompendium, IEC62443, NIST CSF
	Gibt es eine Security-Organisation?	prEN IEC62443-2-1:2019: ORG 1.3: Roles and responsibilities	ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit [Institutionsleitung] (B)	4 Festlegung von Verantwortlichkeiten	z.B. definierte und dokumentierte Security Rollen und Verantwortlichkeiten

*Security beinhaltet sowohl die Aspekte der Cybersicherheit als auch des physischen Schutzes

	Sind die laut Regelwerk erforderlichen Rollen besetzt und diese Mitarbeiter geschult?	prEN IEC62443-2-1:2019: ORG 1.3: Roles and responsibilities ORG 1.5: Security responsibilities training	ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit	4 Festlegung von Verantwortlichkeiten	z.B. Cybersicherheit - Fortbildungen, Awareness-Schulungen
	Gibt es ein Asset Management?	prEN IEC62443-2-1:2019: CM 1.1: Asset inventory baseline	OPS.1.1.2.A20 Verwaltung und Inbetriebnahme von Geräten IND.2.7.A1 Erfassung und Dokumentation [Planer, Wartungspersonal] (B)	6.3 IT-Risikobeurteilung	z.B. Handhabung mit Hilfe von Datenbanken, Excel-Listen
	Gibt es einen Cybersicherheit Risiko-Management-Prozess?	prEN IEC62443-2-1:2019: ORG 2.1: Security risk mitigation	BSI-Standard 200-1 und 2 ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen	6.3 IT-Risikobeurteilung	z.B. Beschreibungen für die Identifikation, Bewertung und den Umgang mit Risiken
	Gibt es einen Prozess zur Festlegung der erforderlichen Maßnahmen der Cybersicherheit?	prEN IEC62443-2-1:2019: ORG 2.1: Security risk mitigation	ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen (B) ISMS.1.A15 Wirtschaftlicher Einsatz von Ressourcen für	6 Sicherungsanalyse	z.B. Beschreibung, in welchem Kontext einzelne Maßnahmen umzusetzen sind

			Informationssicher-heit		
	Gibt es einen Änderungs-Management-Prozess? (Management Of Change, MOC)	prEN IEC62443-2-1:2019: CM 1.4 Change control	OPS.1.1.3 Patch- und Änderungsmanage-ment IND.1.A6 Änderungs-management im OT-Betrieb (S)	Anhang 1 Verände-rungsmanagement	z.B. Betrachtung von Cybersicherheit-Risi-ken bei Änderungen; Dokumentation neuer/geänderter As-sets; Prüfungen (FAT/SAT/IBN) umfas-sen auch Security-Prüfungen; Security ist Teil der Schulungen für neue Systeme; OT-Security Anforde-rungen sind Teil der Ausschreibung;
	Gibt es ein Management von Schwachstellen?	prEN IEC62443-2-1:2019: EVENT 1.9 Vulner-ability handling	APP.6.A4 Regelung für die Installation und Konfiguration von Software IND.1.A12 Etablieren eines Schwachstel-len-Managements OPS.1.1.3 Patch- und Änderungsmanage-ment	4 Reaktion auf neue Schwachstellen und IT-Bedrohungen	z.B. Anbindung an ein Schwachstellen-Informationssystem (CERT, Hersteller-Ad-visories), der an-schließenden Identi-fikation und Bewer-tung

	Gibt es eine einen Prozess für die Behandlung von Abweichungen vom Regelwerk (Ausnahmeprozess als Teil des Risikomanagements)?	prEN IEC62443-2-1:2019: ORG 2.1: Security risk mitigation IEC 62443-3-2 DRAR DRAR 10	ISMS.1.A12 Management-Berichte zur Informationssicherheit ORP.5.A5 Ausnahmegenehmigungen		z.B. Umgang mit dem Fall, dass eine Anforderung nicht umgesetzt werden kann
	Sind die definierten Anforderungen, Prozesse aus dem Cybersicherheit-Management und deren Umsetzung dokumentiert?	prEN IEC62443-2-1:2019: implizit mit Erreichung von ML2, siehe Definition der Maturity Level	ISMS.1.A13 Dokumentation des Sicherheitsprozesses IND.1.A20 Systemdokumentation [Mitarbeiter, OT-Betrieb]	Anhang 1 Dokumentation	z.B. versionierte Dokumente und eine dokumentierte Umsetzung in den Anlagen
	Gibt es einen Prozess für den Umgang mit Sicherheitsvorfällen?	prEN IEC62443-2-1:2019: EVENT 1.7 Event analysis EVENT 1.8 Incident handling and response	DER.2.1.A1 Definition eines Sicherheitsvorfalls DER.2.1.A2 Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen	Anhang 1 Notfallmanagement	z.B. einen Incident-Response-Plan, Playbooks
	Gibt es Prozesse zur regelmäßigen Überprüfung und Anpassung von Sicherheitsmaßnahmen?	prEN IEC62443-2-1:2019: ORG 2.4 SP Überprüfungen	ISMS.1.A11 Aufrechterhaltung der Informationssicherheit IND.1.A17 Regelmäßige Sicherheitsüberprüfung	4 Festlegung von Verantwortlichkeiten	z.B. Anleitung zur regelmäßigen Prüfung von Firewall-Regeln

	Werden Maßnahmen regelmäßig überprüft?	EN IEC62443-3-3:2019: SR 3.3 Verifikation der IT-Sicherheitsfunktionalität (zusätzlich: RE1/RE2)	ISMS.1.A11 Aufrechterhaltung der Informationssicherheit ORP.5.A8 Regelmäßige Überprüfungen des Compliance Managements	4 Festlegung von Verantwortlichkeiten	z.B. Durchführung der regelmäßigen Prüfung von Firewall-Regeln, regelmäßige Assessments
	Gibt es ein Berechtigungskonzept / Berechtigungs-Management?	prEN IEC62443-2-1:2019: USER 1.1: User identity assignment USER 1.2: User identity removal USER 1.3: User identity persistence USER 1.4: Access rights assignment	IND.1.A7 Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT ORP.4 Identitäts- und Berechtigungsmanagement	4 Zugangs- und Zutrittsmanagement und -überwachung	z.B. dokumentiere Zugriffs- und Zugangs-Berechtigungen und eine Beschreibung, wie mit Veränderungen umgegangen wird (Zuweisung, Überprüfung und Entfernung von Zugriffsrechten bei Joiners/Movers/Leavers)
	Gibt es ein Konzept zur Überprüfung von Identitäten?	prEN IEC62443-2-1:2019: USER 1.8: User authentication USER 1.9: Multi-factor authentication USER 1.10: Mutual authentication	IND.1.A7 Etablieren einer übergreifenden Berechtigungsverwaltung zwischen der OT und in der Office-IT ORP.4 Identitäts- und Berechtigungsmanagement	4 Zugangs- und Zutrittsmanagement und -überwachung	z.B. mittels Ein- oder Mehr-Faktor-Authentisierung, wie Passwort/PIN und/oder Chipkarte zur Überprüfung von Identitäten vor Zutritt (physisch) oder (System-)Zugang (logisch)

		USER 1.11: Password protection			
	Wird die Cybersicherheit beim Lieferanten in der Lieferantenbeziehung berücksichtigt?	prEN IEC62443-2-1:2019: ORG 1.4 Security Awareness Training ORG 1.2 Background checks ORG 1.3 Security roles and responsibilities ORG 1.4 Security responsibilities training ORG 3.1 Physical access control	IND.1.A11 Sichere Beschaffung und Systementwicklung ORP.5.A4 Konzeption und Organisation des Compliance Management APP.6.A3 Sichere Beschaffung von Software	4 Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen	z.B. mittels Regelungen für den Umgang und den Schutz von Daten; Meldepflicht von Security-Vorfällen beim Lieferanten
	Werden Security-Aspekte berücksichtigt, wenn Dienstleistungen von Fremdfirmen bezogen werden?	prEN IEC62443-2-1:2019: ORG 1.4: Security awareness training ORG 1.5: Security responsibilities training	IND.1.A11 Sichere Beschaffung und Systementwicklung ORP.5.A4 Konzeption und Organisation des Compliance Management APP.6.A3 Sichere	4 Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen	z.B. eine vertragliche Verpflichtung zur Einhaltung definierter Security-Regeln, wie dem verpflichtenden Virenscan der Laptops von Servicemitarbeitern vor Verbindungsaufnahme oder

		IEC62443-2-4:2019+A1 2019	Beschaffung von Software		verpflichtende Security-Awareness-Schulungen der Fremd-Mitarbeiter
	Werden Security-Aspekte von Produkten/Systemen in Serviceverträgen mit Herstellern berücksichtigt?	IEC62443-2-4:2019+A1 2019 IEC 62443-4-1 DM-4 - Addressing security-related issues DM-5 - Disclosing security-related issues	IND.1.A11 Sichere Beschaffung und Systementwicklung ORP.5.A4 Konzeption und Organisation des Compliance Management APP.6.A3 Sichere Beschaffung von Software	4 Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen	z.B. mittels Regelungen zu Vulnerability/Patch Management von betreuten Produkten
	Werden gesetzlichen Anforderungen zur Cybersicherheit berücksichtigt und sind ggf. Meldeprozesse etabliert?	prEN IEC62443-2-1:2019: EVENT 1.8: Incident handling and response	ORP.5.A1 Identifikation der Rahmenbedingungen ORP.5.A2 Beachtung der Rahmenbedingungen	4 Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen	z.B. bzgl. Datenschutz, BSIG ("ITSicherheitsgesetz") oder Arbeitsschutz.
2.) Netzwerkarchitektur & Netzwerksicherheit	Gibt es für PLT-Schutzeinrichtungen ein eindeutiges Zonenkonzept?	EN IEC62443-2-1:2019 NET 1.3: Network segmentation from safety systems	IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts [Planer] (S) IND.2.1.A6 Netzsegmentierung [OT-	Anhang 2 Asset Register und Netzwerkarchitektur	z.B. eine Unterteilung des Netzwerks in Zonen (Netzwerksegmentierung) gemäß NA 163.

		NET 1.4: Network autonomy	Betrieb (Operational Technology, OT), Planer] (B)		
	Ist keine direkte Kommunikation zwischen zwei Geräten auf nicht unmittelbar nebeneinander liegenden Netzwerk(-Purdue-)leveln möglich?	EN IEC62443-2-1:2019: NET 1.1: Segmentation from non-IACS networks NET 1.6: Internal network access control IEC 62443-3-2 ZCR 3	IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts [Planer] (S) IND.2.1.A6 Netzsegmentierung [OT-Betrieb (Operational Technology, OT), Planer] (B)	Anhang 2 Asset Register und Netzwerkarchitektur	z.B. darf ein Gerät, das auf Purdue-Level 2 angesiedelt ist, nur mit einem Gerät kommunizieren, das sich entweder auf demselben Level oder dem nächsthöheren oder -niedrigeren Level befindet?
	Für den Fall, dass das Automatisierungssystem Komponenten umfasst, die auf unterschiedlichen Purdue-Leveln angesiedelt sind (z. B. Server auf Purdue-Level 3 und Client auf Purdue-Level 2): ist für diese Übergänge jeweils eine Liste der	EN IEC62443-2-1:2019 NET 1.2: Documentation of network segment interconnections	IND.1.A21 Dokumentation der Kommunikationsbeziehungen [OT-Betrieb (Operational Technology, OT)] (S)	Anhang 2 Asset Register und Netzwerkarchitektur	z.B. Die Unterteilung des Netzwerks (Netzwerksegmentierung) in unterschiedliche Level erfolgt i.d.R. über Firewalls. Wenn das Automatisierungssystem Komponenten umfasst, die auf

	Netzwerkprotokolle und -ports dokumentiert und der Datenverkehr auf diese eingeschränkt?				unterschiedlichen Leveln angesiedelt sind (z. B. Server auf Purdue-Level 3 und Client auf Purdue-Level 2), sollte eine Liste der Netzwerkprotokolle und -ports bereitgestellt werden, damit die entsprechenden Firewall-Regeln einrichten werden können, die auf einem strikten Whitelisting-Ansatz basieren.
	Sind die Daten und Signalverbindungen von PLT-Schutzeinrichtungen angemessen gesichert?	prEN IEC62443-2-1:2019: DATA 1.3: Safety system configuration mode	IND.2.7.A9 Absicherung der Daten- und Signalverbindungen [Planer, Wartungspersonal, ICSInformationssicherheitsbeauftragter] (S)	7.2.2 Schutz vor cyberphysischen Angriffen	z. B. mittels Überwachung, physischem Schutz oder Darlegung anderer Maßnahmen, wie Erkennung von gezielten Manipulationen
	Werden Kommunikationsbeziehungen (beispielsweise Firewall-Regeln) regelmäßig überprüft?	EN IEC62443-2-1:2019 CM 1.1 Asset inventory baseline	NET.1.2.A17 Regelmäßiger Soll-Ist-Vergleich im Rahmen des Netzmanagements	4 Festlegung von Verantwortlichkeiten	z.B. mittels Auswertung der Benutzung von Firewall-Regeln (hitcounts)

			ORP.5.A8 Regelmäßige Überprüfungen des Compliance Managements		
	Sind Netzwerkinfrastrukturkomponenten (z. B. Router, Firewalls, Switches) in der Lage, Zustandsmeldungen an ein zentrales System zu senden?	IEC 62443-3-3 SR 2.8 – Auditable events RE (1) Centrally managed, system-wide audit trail SR 3.2 – Malicious code protection RE (2) Central management and reporting for malicious code protection IEC 62443-4-2 CR 2.8 – Auditable events CR 6.2 – Continuous monitoring	NET.1.2.A7 Grundlegende Protokollierung von Ereignissen (B) NET.1.2.A36 Einbindung der Protokollierung des Netzmanagements in eine SIEM-Lösung (H)	Anhang 2 Asset Register und Netzwerkarchitektur	z.B. mittels SNMP, syslog
	Sind Konfigurationsschnittstellen von Netzwerkgeräten geschützt?	EN IEC62443-2-1:2019 NET 1.8: Network	NET.1.2.A9 Absicherung der Netzmanagement-	Kein Detailbezug	z.B. mittels Passwörter

		accessible services CM 1.4: Change control	Kommunikation und des Zugriffs auf Netz-Managementwerkzeuge (B)		
	Sind virtuelle Systeme, die zu unterschiedlichen (Purdue-)Leveln gehören, auf unterschiedlicher physischen Hardware installiert?	EN IEC62443-2-1:2019 NET 1.1: Segmentation from non-IACS networks NET 1.6: Internal network access control	NET.1.1.A23 Trennung von Netzsegmenten (S)	Kein Detailbezug	z.B. keine virtualisierten PIM-Systeme und virtualisierten Datenlieferanten auf gleicher Hardware
	Wird die Systemarchitektur im Rahmen des Beschaffungsprozesses auf Einhaltung der Regelwerke überprüft und das Ergebnis dokumentiert?	EN IEC62443-2-1:2019 ORG 1.6: Supply chain security IEC 62443-2-4 SP.02.01 Solution Components - Verification SP.03.02 Network design - connectivity SP.03.02 RE(1) Network design - connectivity	APP.6.A3 Sichere Beschaffung von Software [Beschaffungsstelle] (B)	4 Regelungen für Fremdpersonal und fremdvergebene Dienstleistungen	z.B. mittels Checkliste

3.) Systemhärtung / Funktionsreduktion	Wird Software, die nicht unbedingt benötigt wird, deinstalliert?	EN IEC62443-2-1:2019: COMP 1.1: Device hardening	APP.6.A4 Regelung für die Installation und Konfiguration von Software IND.2.1.A4 Deaktivierung oder Deinstallation nicht genutzter Dienste, Funktionen und Schnittstellen	Kein Detailbezug	z. B. Microsoft-Spiele auf Workstations
	Werden Dienste, die für eine ordnungsgemäße Funktionsfähigkeit nicht erforderlich sind, deaktiviert?	EN IEC62443-2-1:2019: COMP 1.1: Device hardening	APP.6.A4 Regelung für die Installation und Konfiguration von Software IND.2.1.A4 Deaktivierung oder Deinstallation nicht genutzter Dienste, Funktionen und Schnittstellen	Kein Detailbezug	z. B. Webserver am Controller, Telnet am Netzwerk-Switch, Druckerschnittstelle, Dateifreigabefunktionen
	Sind die Systeme gemäß Herstellervorgaben gehärtet?	EN IEC62443-2-1:2019: COMP 1.1: Device hardening IEC62442-2-4 SP.02.03 BR, RE(1) SP.03.05 BR, RE(1)	APP.6.A6 Berücksichtigung empfohlener Sicherheitsanforderungen	Kein Detailbezug	z.B. Deaktivierung von Autostart-Mechanismen (beispielsweise für USB-Medien), Aktivierung starker Benutzerkontensteuerung (User Account Control)

	Werden technische Maßnahmen am Automatisierungssystem zum Schutz gegen eine missbräuchlichen Verwendung von tragbaren Speichermedien getroffen?	EN IEC62443-2-1:2019: COMP 1.1: Device hardening COMP 2.2: Malware protection	CON.7.A9 Sicherer Umgang mit mobilen Datenträgern SYS.4.5 Wechseldatenträger	Kein Detailbezug	z.B. indem nicht genutzte USB-Ports und CD/DVD-Laufwerke deaktiviert oder physisch gesperrt werden
	Wird für Konten und Benutzer, die zur Änderung von Variablen berechtigt sind, mindestens eine Ein-Faktor-Authentifizierung benötigt?	prEN IEC62443-2-1:2019: USER 1.8: User authentication USER 1.9: Multi-factor authentication	ORP.4.A9 Identifikation und Authentisierung [IT-Betrieb] (B)	4 Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung	z.B. mittels Passwort, RFID-Karte
	Werden auf allen Geräten die Standardpasswörter geändert?	prEN IEC62443-2-1:2019: USER 1.11: Password protection	ORP.4.A1 Regelung für die Einrichtung und Löschung von Benutzern und Benutzergruppen ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme	4 Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung	z.B. als Teil der Konfiguration vor Inbetriebnahme von neuen Netzwerk-, Automatisierungs- und Kontrollkomponenten
	Werden die Zugangs- und Zugriffsrechte für alle Benutzer auf das Notwendigste beschränkt?	prEN IEC62443-2-1:2019: USER 1.5: Least privilege	ORP.4.A3 Dokumentation der Benutzerkennungen und Rechteprofile ORP.4.A4	4 Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung	z.B. Beschränkung von Login-Möglichkeiten (Zugang) und Lese-/Schreib-/Ausführungsrechte

			Aufgabenverteilung und Funktionstrennung		(Zugriff) auf ein notwendiges Minimum ("need to know-Prinzip")
	Werden Härtungsmaßnahmen dokumentiert?	prEN IEC62443-2-1:2019: CM 1.3: Configuration settings CM 1.4: Change control	OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten (S)	4 Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung	z.B. mittels Dokumentation im Pflichtenheft bzw. dem Handbuch, wie man (z.B. während eines Incidents) einen deaktivierten USB Port wieder aktiviert
4.) Schutz vor Malware	Werden bei Automatisierungssystemen Maßnahmen zum Schutz vor Malware wie Viren oder Trojaner getroffen?	prEN IEC62443-2-1:2019: COMP 2 – Malware protection	OPS.1.1.4 Schutz vor Schadprogrammen IND.2.1.A8 Schutz vor Schadsoftware [OT-Betrieb (Operational Technology, OT)] (S)	4 Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung	z.B. Virenscanner, Application-Control, Allowlisting, Monitoring von Datenverkehr und Dateizugriffen
	Werden technische Maßnahmen zur Benachrichtigung von Personen bei Erkennung eines Virus getroffen?	prEN IEC62443-2-1:2019: EVENT 1.2: Event reporting	OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen	4 Zugriffsmanagement auf Prozesssteuerung/Sicherheitssteuerung	z.B. automatische Benachrichtigung per Mail oder Aneigen eines Alarms in einem Überwachungssystem

	Gibt es organisatorische und technische Maßnahmen zur Überprüfung der Integrität von Speichermedien und Überprüfung auf Schadsoftware vor der Nutzung in einem Automatisierungssystem?	EN IEC62443-2-1:2019 ORG 1.4: Security awareness training COMP 1.2: Dedicated portable media COMP 2.1: Malware free DATA 1.2: Protection of data	IND.1.A9 Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen CON.7.A9 Sicherer Umgang mit mobilen Datenträgern	4 Manipulationserkennung und –schutz	z.B. Standard-Betriebsanweisung als organisatorische Maßnahme oder eine Scan-Station als technische Lösung für einen sicheren Datenaustausch
5.) Fernzugriff	Gibt es eine DMZ zwischen OT und Internet/Intranet?	prEN IEC62443-2-1:2019: NET 3.2: Remote access connections NET 1.1: Segmentation from non-IACS networks NET 2.2: Wireless network segmentation	IND.1.A5 Entwicklung eines geeigneten Zonenkonzepts NET.1.1.A4 Netztrennung in Zonen	Anhang 2 Asset Register und Netzwerkarchitektur	z,B. mittels Daten-Zwischenspeicherung auf einem gehärteten Server und der Verwendung unterschiedlicher Netzwerk-Protokolle Richung Internet/Intranet und OT (Protokollwechsel) und Einschränkung des Verkehrs durch Verwendung einer Firewall.
	Werden ausschließlich vom Unternehmen freigegebene	prEN IEC62443-2-1:2019: NET 3.1: Remote	OPS.1.2.5.A1 Planung des Einsatzes der Fernwartung (B)	Anhang 2 Asset Register und Netzwerkarchitektur	z.B. überprüfte Fernzugriffslösungen von

	Fernwartungszugänge verwendet? (Remote Access)	access applications	IND.3.2 Fernwartung im industriellen Umfeld		Automatisierungsherstellern
	Gibt es ein Security-Konzept für Fernwartungszugänge?	prEN IEC62443-2-1:2019: NET 3.2: Remote access connections NET 3.3: Remote access termination NET 1.1: Segmentation from non-IACS networks NET 1.6: Internal network access control NET 1.7: Device connections NET 1.8: Network accessible services USER 1.8: User authentication	IND.3.2 Fernwartung im industriellen Umfeld	Anhang 2 Asset Register und Netzwerkarchitektur	z.B. gemäß NA135 (Protokollwechsel, Jump-Server, Rendezvous-Server oder ähnlichem)
6) Sichere Installation und Modifikation	Gibt es Regelungen zu Patch-Management?	prEN IEC62443-2-1:2019: COMP 3 – Patch management	OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement	Anhang 2 Reaktion auf neue Schwachstellen und Bedrohungen	z.B. eine Regelung ob und wann ein Patch eingespielt wird (das Einspielen von

			IND.1.A12 Etablieren eines Schwachstellen-Managements		Patches wird zwischen Betrieb und dem Automatisierungshersteller koordiniert, damit das Einspielen des Patches nicht die Produktion behindert)
	Gibt es einen sicheren Installationsprozess aus qualifizierten Quellen?	prEN IEC62443-2-1:2019: COMP 3.1: Security patch authenticity/integrity	OPS.1.1.3.A10 Sicherstellung der Integrität und Authentizität von Softwarepaketen (S)	Anhang 2 Reaktion auf neue Schwachstellen und Bedrohungen	z.B. über vom Automatisierungshersteller gestellte Softwarepakete, die mittels Signatur überprüft werden können
7) Zutrittsbeschränkungen	Wird der Zutritt im erforderlichen Umfang geschützt?	prEN IEC62443-2-1:2019: ORG 3.1: Physical access control AVAIL 1.2: Resource management	ORP.4.A5 Vergabe von Zutrittsberechtigungen [IT-Betrieb] (B)	4 Zugangs- und Zutrittsmanagement und -überwachung	z.B. ist der Zugang zu Schalträumen nur für berechtigtes Personal mit speziellem Schlüssel möglich
	Wird der physische Zugriff auf Automatisierungssysteme auf berechtigte Personen beschränkt?	EN IEC62443-2-1:2019 ORG 3.1: Physical access control	ORP.4.A5 Vergabe von Zutrittsberechtigungen [IT-Betrieb] (B)	4 Zugangs- und Zutrittsmanagement und -überwachung	z.B.: indem Schränke, die sich nicht in einem Bereich mit beschränktem Zugang (z.B. Leitwarte) befinden, mittels eingebautem Schloss oder

					Vorhängeschloss verschlossen werden (kein Standard-, sondern spezieller Schlüssel).
8) Überwachung des OT-Systems und seiner Datenkommunikation	Werden Daten der Überwachung ausgewertet?	prEN IEC62443-2-1:2019: EVENT 1.7: Event analysis IEC 62443-4-2 CR 6.2 – Continuous monitoring	DER.1.A6 Kontinuierliche Überwachung und Auswertung von Protokollierungsdaten IND.1.A10 Monitoring, Protokollierung und Detektion	4 Manipulationserkennung und –schutz	z.B. regelmäßige Untersuchung von Logs / Meldungen auf Auffälligkeiten durch geschultes Personal
	Werden (erfolgreiche und nicht erfolgreiche) Authentifizierungsversuche bei Geräten protokolliert?	prEN IEC62443-2-1:2019: EVENT 1.1: Event detection EVENT 1.4: Logging USER 1.13: User login display information IEC 62443-4-2 CR 2.8 – Auditable events	NET.3.2.A9 Protokollierung (B) IND.1.A10 Monitoring, Protokollierung und Detektion	4 Manipulationserkennung und –schutz	z.B. durch Aktivierung der Windows-Logs

9) Training / Sensibilisierung	Wurden die Security Regelwerke im Betrieb bekannt gemacht?	prEN IEC62443-2-1:2019: ORG 1.4: Security awareness training ORG 1.5: Security responsibilities training	ORP.3.A4 Konzeption und Planung eines Sensibilisierungs- und Schulungsprogramms zur Informationssicherheit	4 Sensibilisierung/Schulung eigener Mitarbeiter	z.B. durch verpflichtende Security Awareness Trainings
	Gibt es Awarenessprogramme?	prEN IEC62443-2-1:2019: ORG 1.4: Security awareness training ORG 1.5: Security responsibilities training	ORP.3.A6 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit (S)	4 Sensibilisierung/Schulung eigener Mitarbeiter	z.B. Generelle Schulungen zum Umgang mit USB-Sticks zur Sensibilisierung des Personals
	Gibt es rollenabhängige Schulungen?	prEN IEC62443-2-1:2019: ORG 1.4: Security awareness training ORG 1.5: Security responsibilities training	ORP.3.A6 Durchführung von Sensibilisierungen und Schulungen zur Informationssicherheit (S)	4 Sensibilisierung/Schulung eigener Mitarbeiter	z.B. der Schulung von Betriebspersonal, den Cybersicherheit-Verantwortlichen, wie Sicherheitsbeauftragtem, der Schulung von Senior Management zu Security Aspekten