Landesamt für Sicherheit in der Informationstechnik

„IT-Sicherheit in der Trinkwasserversorgung und Abwasserentsorgung“

Vorgehensmodell zur Umsetzung

Stand: 28.09.2023

Version: 1.1

Landesamt für Sicherheit in der Informationstechnik, Keßlerstraße 1, 90489 Nürnberg
beratung-kritis@lsi.bayern.de, Telefon: 0911 21549-525

INHALTSVERZEICHNIS

Änderungshistorie

Die folgende Tabelle listet sämtliche Änderungen gegenüber Version 1.0 des Vorgehensmodell auf:

Version	Datum	Stelle	Änderung
1.0	05.02.2022	-	Initialerstellung
1.1	05.09.2022	Inhaltsverzeichnis	Gliederung zur besseren Übersichtlichkeit optimiert und Ablaufplan erstellt
1.1	20.09.2022	Safety	Punkt ergänzt entsprechend Handlungsempfehlung
1.1	07.11.2022	Global	Erweiterung um das Themengebiet Abwasserentsorgung
1.1	28.09.2023	Gesamtes Formular	Editierbare Eingabefelder

Vorwort zum Vorgehensmodell

Wollen Sie die IT-Infrastruktur der Trinkwasserversorgung bzw. Abwasserentsorgung noch besser als bisher vor Hackerangriffen und Angriffen von Cyberkriminellen schützen? Suchen Sie nach einer Vorgehensweise, wie Sie die dafür passenden Sicherheitsmaßnahmen auswählen? Möchten Sie gerne wissen, welche Maßnahmen Sie priorisieren und in welcher zeitlichen Reihenfolge Sie diese umsetzen (lassen) sollten? Im Folgenden finden Sie einen **Vorschlag als Vorgehensmodell** für eine zeitliche Reihenfolge zur Umsetzung empfohlener Informationssicherheitsmaßnahmen. Es richtet sich dabei an kleinere bis mittelgroße Wasserver- bzw. Abwasserentsorger und vermittelt erste bzw. weitere Schritte in Richtung abgesicherte IT-Landschaft.

Eher ungewöhnlich wäre es, wenn in Ihrer Organisation nicht schon bereits technische, organisatorische und einzelne punktuelle Awareness-Maßnahmen umgesetzt worden sind. Vielleicht haben Sie bereits Dokumentationen und Handbücher erstellt, welche die vorhandene IT-Infrastruktur miterfasst und vielleicht einen Plan für das Vorgehen bei IT-Ausfällen erstellt? Ein Backup-Konzept entwickelt und umgesetzt? Möglicherweise schulen Sie bereits regelmäßig Ihre Mitarbeiterinnen und Mitarbeiter?

Falls Sie einzelne Punkte bereits umgesetzt haben, können Sie das folgende Vorgehensmodell verwenden, um noch einmal zu überprüfen, ob Sie an manchen Stellen die vorgeschlagenen Maßnahmen verstärken und erweitern wollen.

Im ersten Schritt identifizieren Sie bitte die für die Sicherheit Ihrer Organisation aktuell relevanten Bedrohungen und ordnen diese nach abnehmender Kritikalität für die Auswahl der in der Folge zu treffenden Maßnahmen. Je nachdem, welche Maßnahmen in der Organisation bereits getroffen wurden, kann die Liste der aktuell relevanten Bedrohungen für Sie und Ihre Organisationsleitung unterschiedlich aussehen.

Bitte stellen Sie hier die für Ihre Organisation aktuell relevanten Bedrohungen/Gefährdungen zusammen (dies können z.B. auch eine veraltete Firewall, teilweise veraltete Serversysteme, ungenügendes Backup, fehlendes Sicherheitsbewusstsein in bestimmten Bereichen etc. sein):

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

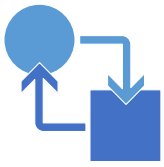
Bitte nutzen Sie dieses Vorgehensmodell und ebenso den Fragenkatalog der Handlungsempfehlung, um die von Ihnen identifizierten aktuell relevanten Bedrohungen/Gefährdungen durch angemessene Gegenmaßnahmen zu adressieren, d.h. um **einen für Sie spezifischen Maßnahmenplan** zu entwickeln. Der sechsstufige Aufbau des Vorgehensmodells orientiert sich an der Kritikalität der Gefährdungen und schlägt daher eine zeitliche Reihenfolge vor.

Stufe 0:
Voraussetzungen
für den Start

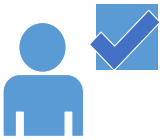
Stufe 1:
Bestandsaufnahme

Stufe 2:
Organisatorische
Maßnahmen

Stufe 3:
Weitere wichtige
Absicherungen, Richtlinien
Und Dokumentation



Stufe 4:
Aufrechterhaltung der
Informationssicherheit und
Kontinuierliche Weiterentwicklung



Stufe 5:
Auditierung und
Zertifizierung

Sobald Sie die für Ihre Organisation aktuell relevanten Bedrohungen/Gefährdungen ermittelt haben, gilt es die Organisationsleitung für den weiteren systematischen Auf- und Ausbau der Informationssicherheit zu gewinnen.

Hinweis 1: Im folgenden Dokument referenzieren die Zahlen am rechten Rand jeweils auf die zugehörigen Fragen in der Handlungsempfehlung. Bei einigen der genannten Maßnahmen wird jeweils auf mehrere Fragen verwiesen. Sie finden die Fragen sowie die dazugehörigen Beschreibungen in der Handlungsempfehlung.

Hinweis 2: Bei Bedarf finden Sie einzelne Fachbegriffe im Glossar der Handlungsempfehlung erläutert.

Hinweis 3: Die Maßnahmen der Handlungsempfehlung sind immer individuell auf Ihre Organisationseinheit zu betrachten, hieraus können sich gegebenenfalls Abweichungen zu den konkret vorgeschlagenen Maßnahmen ergeben.

Stufe 0: Voraussetzung für den Start

Stufe 0:
Voraussetzungen
für den Start

Bevor mit dem systematischen Auf- und Ausbau der Informationssicherheit begonnen werden kann, muss die tatsächliche Unterstützung der Organisationsleitung sichergestellt werden. Dies ist ein beständiger Prozess und kein isoliertes, einmaliges Projekt.

Hierfür muss die Organisationsleitung

- ☐ die Gesamtverantwortung für die Informationssicherheit bzw. den Informationssicherheitsmanagementprozess übernehmen und die kontinuierliche Weiterentwicklung der Informationssicherheit fördern. 1.1a
- ☐ die Informationssicherheitsziele glaubhaft nach innen und außen vermitteln und die Umsetzung der Informationssicherheitsziele verantworten. 1.1c

- ☐ die für die Aufrechterhaltung und Verbesserung der Informationssicherheit benötigten Ressourcen bereitstellen und den Informationssicherheitsprozess aktiv unterstützen. 1.1d
- ☐ einen Verantwortlichen für die Umsetzung des von der Leitungsebene zu initiierenden ISMS schriftlich ernennen und diesem seine Verantwortlichkeiten zuweisen. Diese Aufgabe kann einem bereits ernannten Informationssicherheitsbeauftragten (ISB) übertragen werden. 1.1h
- ☐ einen internen oder externen ISB ernennen, falls noch kein ISB bestellt wurde, welcher aktiv den Sicherheitsprozess leitet. 1.2a
- ☐ im Falle eines externen ISB einen internen Ansprechpartner zur Verfügung stellen. 1.2e

Stufe 1: Bestandsaufnahme

Sie können mit Stufe 1, der Bestandsaufnahme beginnen, sobald Sie die Stufe 0 vollständig umgesetzt haben.

Stufe 1: Bestandsaufnahme

Bevor Veränderungen initiiert werden können, ist eine Bestandsaufnahme der erste Schritt zur Verbesserung der Informationssicherheit. Es sollte zuerst abgeklärt werden, wo Ihre Organisation steht und welche Systeme etc. eingesetzt werden. So besteht die Möglichkeit, komplexe Zusammenhänge zu verstehen und einen ganzheitlichen Überblick über die IT-Infrastruktur mit den jeweiligen Systemen zu schaffen. So können zum Beispiel frühzeitig Gefährdungen erkannt und Verbesserungspotentiale genutzt werden. Die Informationssicherheit kann nur verbessert werden, wenn ein hinreichender Überblick über die IT-Infrastruktur gegeben ist.

Ein Beispiel für einen möglichen Aufbau eines IT-Netzstrukturplans finden Sie im Anhang.

I.1 Bestandsaufnahme

Zunächst muss eine Bestandsaufnahme der eingesetzten Systeme/Netze etc. durchgeführt und sich ein Überblick verschafft werden, der die Aufgaben und die Relevanz der erfassten Systeme übersichtlich darstellt:

- ☐ Vollständig erfassen und dokumentieren, aus welchen maßgeblichen Systemen/Komponenten/Anwendungen bzw. Applikationen die IT-Infrastruktur besteht (inkl. Leitebene (SCADA, PLS), Steuerungsebene (SPS, PLC) und Feldebene; Verwaltungs-IT, Server, etc.). 2.1a
- ☐ Die Verkabelung der Systeme vollständig dokumentieren (physischer Netzplan / Verkabelungsplan inkl. Redundanzen). 2.1b
- ☐ Für den IT-Netzstrukturplan ähnliche Objekte sinnvoll gruppieren, damit dieser übersichtlich bleibt und dabei alle relevanten Aspekte (u.a. IP-Adressen, VLANs, Firewall-Schutzzonen etc.) enthält. 2.1c, 2.1d
- ☐ Erfassen und dokumentieren, wie die Außenstellen angebunden sind. 2.1e
- ☐ Erfassen und dokumentieren der Schnittstellen zu externen weiteren Netzen (z.B. Internet, Bayerisches Behördennetz, dauerhafte freigeschaltete Wartungszugänge (nicht empfohlen), ausgelagerte Dienstleistungen z.B. Cloud). 2.1f
- ☐ Definieren, welche Systeme als kritisch eingestuft werden. 3.1a

Falls keine unmittelbaren Gefahren während der Bestandsaufnahme erkannt wurden, wird empfohlen mit dem Vorgehensmodell weiter fortzufahren. Wurden kritische Schwachstellen identifiziert, welche ein sofortiges Handeln erfordern, sollten Sie die jeweilige Gefährdung betrachten, diese bewerten und in Abstimmung mit der Organisationsleitung angemessene Gegenmaßnahmen treffen.

Stufe 2: Organisatorische Maßnahmen und erste dringliche Absicherungen

Stufe 2: Organisatorische Maßnahmen

Sie können mit Stufe 2 zum systematischen Auf- und Ausbau der Informationssicherheit beginnen, sobald Sie die Stufe 0 und 1 vollständig umgesetzt haben.

Vorhandene und zukünftige potentielle Bedrohungen der Informationssicherheit können im schlimmsten Fall die Sicherheit der Organisation gefährden.

Der Informationssicherheitsbeauftragte (ISB) muss die Organisationsleitung über diese aktuell relevanten Bedrohungen/Gefährdungen informieren. Es soll dokumentiert werden, wann und zu welchen Inhalten die Organisationsleitung informiert wurde und welche Entscheidungen diese dazu getroffen hat (z.B. als Maßnahmen-Umsetzungsplan inkl. der dafür benötigten Ressourcen).

II.1 Organisation des Informationssicherheitsmanagements

Mit der Unterstützung der Organisationsleitung muss nun das Informationssicherheitsmanagement (ISM) so organisiert werden, dass es handlungsfähig wird. Insbesondere muss der ISB mit ausreichenden Kompetenzen und Ressourcen ausgestattet werden.

II.1.A Rolle des Informationssicherheitsbeauftragten

Eine zentrale Rolle im Informationssicherheitsmanagement obliegt dem ISB. Daher muss die Organisationsleitung

- ☐ die Stellung des ISB entsprechend der Maßnahmenbeschreibung (siehe: Handlungsempfehlung, Spalte E/Beschreibung) regeln. 1.2b
- ☐ dem ISB ausreichende Ressourcen zur Erfüllung seiner Aufgaben zur Verfügung stellen. 1.2c
- ☐ für den ISB einen Vertreter ernennen bzw. eine Vertretungsregelung vereinbaren. 1.2d
- ☐ konkrete Handlungsanweisungen und Verantwortlichkeiten festlegen und dokumentieren. 1.2f
- ☐ den Mitarbeitern die Handlungsanweisungen und Verantwortlichkeiten bekannt machen. 1.2g

II.1.B Ausbildung und Qualifikationserhalt des Informationssicherheitsbeauftragten

Zur adäquaten Erfüllung seiner Aufgaben muss

- ☐ der ISB über eine angemessene Qualifikation verfügen. 1.3a
- ☐ dem ISB eine den Anforderungen angemessene Fortbildung ermöglicht werden. 1.3b

II.1.C Unterstützung des Informationssicherheitsbeauftragten

Der ISB benötigt Unterstützung sowohl von der Organisationsleitung als auch von allen Beschäftigten. Hierbei sollte(n)

- ☐ die Verantwortlichen und der ISB bei der Planung von Projekten rechtzeitig und im notwendigen Umfang eingebunden werden. 1.4a
- ☐ im Haushalt (z.B. Wirtschaftsplan bzw. Budgetplan) und im Stellenplan für die Aufgaben des ISB angemessene Ressourcen zur Verfügung gestellt werden. 1.4b
- ☐ der ISB, der Datenschutzbeauftragte, der technische Leiter und der Verantwortliche für die IT sowie die Organisationsleitung vertrauensvoll zusammenarbeiten. 1.4c

II.1.D Einbindung Datenschutzbeauftragter

Die Zusammenarbeit mit dem Datenschutzbeauftragten (DSB) soll klar geregelt sein:

- ☐ Den Datenschutzbeauftragten in alle Informationssicherheitsprozesse einbinden und umgekehrt den ISB in die Datenschutzprozesse einbinden. 1.5b

II.2 Leitlinie

Die Organisationsleitung muss

- ☐ eine Leitlinie zur Informationssicherheit verabschieden, die folgende Punkte beschreibt: 1.1b
  - ☐ Stellenwert der Informationssicherheit. 1.1e
  - ☐ Geltungsbereich der Informationssicherheits-Leitlinie. 1.1f
- ☐ die Informationssicherheits-Leitlinie allen Mitarbeitern bekannt machen. 1.1g

II.3 IT-Notfallmanagement

Die Integration eines Notfallmanagements in die Organisation ist essentiell. Durch das Notfallmanagement wird ein Vorgehen definiert, wodurch im Ernstfall, von den Einflüssen unabhängig, die Ausfallzeit und der Schaden so gering wie möglich gehalten werden soll. Das IT-Notfallmanagement nutzt den entwickelten Überblick über die vorhandenen Informationsverbünde zur Ableitung von Maßnahmen, definiert verantwortliche Personen und beschreibt Meldewege. Wenn Mitarbeiter und die verantwortlichen Fachkräfte wissen, was zu tun ist, kann strukturiert und schnell reagiert werden.

II.3.A Verfügbarkeit kritischer Systeme

Die Verfügbarkeit der für die Versorgungssicherheit mit Trinkwasser bzw. der für die sichere Entsorgung von Abwasser relevanten Systeme und Komponenten muss stets gewährleisten sein. Dazu sind gewisse Vorkehrungen zu treffen:

- ☐ Die für den Betrieb direkt oder indirekt notwendigen IT-/OT-Systeme und IT-/OT-Infrastruktur-Komponenten angemessen redundant auslegen. 5.1a
- ☐ Die Wirksamkeit der Redundanzen für einen unterbrechungsfreien Betrieb der IT-/OT-Systeme und IT-/OT-Infrastruktur-Komponenten ausreichend testen. 5.1b
- ☐ Voraussetzungen schaffen, dass bei einem Ausfall der Systeme gegebenenfalls auf Handsteuerung umgeschaltet werden kann. 5.1c
- ☐ Für wichtige IT-/OT-Systeme und Komponenten angemessene technische bzw. organisatorische Ersatzverfahren vorhalten. 5.1d
- ☐ Relevante Personen mit Ihren Kontaktdaten im Notfallplan erfassen. 5.1e
- ☐ Mit gegebenenfalls benötigten externen Stellen entsprechende Erreichbarkeiten und Reaktionszeiten vereinbaren. 5.1f
- ☐ Die maximalen Ausfallzeiten der Verwaltungsprozesse definieren und dokumentieren. 5.1g
- ☐ Technische bzw. organisatorische Maßnahmen (Erstellung eines Notfallplans) definieren und erproben, um Systeme innerhalb der maximalen Ausfallzeit wieder verfügbar zu machen. 5.1h
- ☐ IT-Notfallpläne und Wiederanlaufpläne erstellen und für alle betreffenden Mitarbeiter erreichbar hinterlegen (auch im Notfall erreichbar, z.B. bei einem Ausfall der IT). 5.1i
- ☐ IT-Notfall- und Wiederanlaufpläne den betreffenden Personen bekannt machen. 5.1j
- ☐ Die Ersatzverfahren, die bei einem IT-/OT-Ausfall zum Einsatz kommen etablieren und bekannt machen. 5.3a
- ☐ Sicherstellen, dass die Aufgaben eines Mitarbeiters bei Abwesenheit von anderen Kollegen sachgerecht übernommen werden können. 8.3a
- ☐ Das Thema Safety in der Organisation berücksichtigen 3.2a

II.3.B Alarmierungspläne

Damit auf einen IT-Notfall angemessen reagiert werden kann, müssen Alarmierungspläne vorhanden sein. Hierfür ist es notwendig

- ☐ Kommunikationswege für den IT-Notfall einzurichten. 5.2a
- ☐ dass bei einem Ausfall der IT-/OT-Infrastruktur redundante Kommunikationswege verfügbar sind (z.B. Einsatz von Bereitschaftshandy(s) statt IP-basierter Telefonie). 5.2b
- ☐ dass alle Beteiligten den Alarmierungsplan zur Kenntnis genommen haben und dass dieser im Falle eines IT-Notfalls zugreifbar hinterlegt ist. 5.2c

II.4 Umsetzung weiterer grundlegender Absicherungen

Wurden durch die Bestandsaufnahme neue Bedrohungen/Gefährdungen entdeckt, so können Sie hier Ihre im Vorwort erstellte Liste der Bedrohungen/Gefährdungen aktualisieren:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Die im Folgenden genannten Maßnahmen zur weiteren grundlegenden Absicherung können anhand der aktualisierten Gefährdungsliste und nach interner Risikoabwägung weiter priorisiert werden. Sie können nun mit Hilfe unserer Handlungsempfehlung und Ihrer Gefährdungsliste einen Maßnahmenplan erstellen. Dieser Maßnahmenplan soll zu gegebenem Zeitpunkt mit der Organisationsleitung abgestimmt, deren Entscheidungen dokumentiert und die beschlossenen Maßnahmen umgesetzt werden. Liegen keine akuten Gefährdungen vor, welche ein schnelles Handeln erfordern, können Sie mit dem Vorgehensmodell fortfahren. Falls Sie einen Maßnahmenplan aufgrund von akuten Gefährdungen erstellt haben, müssen Sie die Maßnahmen umsetzen und können zu einem späteren Zeitpunkt wieder zum Vorgehensmodell zurückkehren.

II.4.A Gegen physische Schäden absichern

Es müssen physische Schäden an (insbesondere kritischen) IT-Systemen verhindert werden:

- ☐ Die kritischen Systeme ausreichend gegen physische Manipulationen sichern. 6.7a
- ☐ Die Leitstelle und die IT-Infrastruktur (z.B. Serverräume, Netzwerkschränke, Unterverteiler) gegen unbefugten Zutritt bzw. gegen Manipulation schützen. 9.1b, 9.2a
- ☐ Eine unkritische Lage für die Serverräume wählen (d.h. entfernt von potentiellen Gefahrenquellen oder mit entsprechend geschützt). 9.2b
- ☐ Ein Brandschutzkonzept für den Serverraum erstellen. 9.2c
- ☐ Serverräume (falls mehrere vorhanden) in unterschiedlichen Gebäuden bzw. Brandabschnitten betreiben. 9.2d
- ☐ Den Serverraum (bzw. die kritischen IT-Systeme) vor starken Spannungsschwankungen und Unterbrechungen in der Stromversorgung schützen. 9.2e
- ☐ Den Serverraum über eine ausreichende Entwärmung / Klimatisierung schützen. 9.2f
- ☐ Bei der Raumwahl des Serverraums darauf achten, dass keine Versorgungsleitungen durch diesen verlaufen oder diese ausreichend absichern. 9.2g
- ☐ Analysieren, ob weitere, weniger gängige externe Gefahren- und/oder Fehlerquellen existieren und bei Bedarf geeignete Absicherungsmaßnahmen treffen (z.B. Schutz vor EMV). 9.2h

- ☐ Weitergehende strukturelle Sicherungsmaßnahmen wie umfassende Einbruch-, Brandmelde- und Brandlösch- sowie Rauchabzugsanlage ergreifen und sollte dies notwendig sein, einen erweiterten Überschwemmungsschutz. 9.2i
- ☐ Die IT-Systeme ausreichend gegen physische Manipulationen sichern. 9.4a

II.4.B Zugangs- und Zutrittsrechte

Es muss der Zugriff auf IT-Infrastruktur und -Systeme sowie der Zugang zu schutzbedürftigen Räumen abgesichert werden:

- ☐ Die Befugnisse für die Identitätsprüfung und Rechteerteilung innerhalb der Organisation festlegen. 7.18a
- ☐ Die Prozesse für die Identitätsprüfung und Rechteerteilung definieren, dokumentieren und bekannt machen. 7.18b
- ☐ Ein Rollen- und Berechtigungskonzept nach dem Minimalprinzip einführen, welches die Zugriffsberechtigungen, Systeme und Daten regelt. 7.19a
- ☐ Soweit als möglich personalisierte Accounts verwenden. 7.19b
- ☐ Die Zugangsberechtigten auf den korrekten Umgang mit Zugangsmitteln (z.B. Accounts, Smartcards) hinweisen. 7.19c
- ☐ Eine aktuelle Dokumentation über vergebene Zugangs- und Zugriffsrechte sowie Zugangsmittel pflegen. 7.19d
- ☐ Änderungen bei Zugangs- und Zugriffsrechten von den Verantwortlichen prüfen und bestätigen lassen. 7.19e
- ☐ Ein geregeltes Verfahren für die Vergabe sowie den Entzug von erforderlichen Zugangs- und Zugriffsrechten sowie Zugangsmitteln aufsetzen. 7.19f
- ☐ Zugriffsrechte auf IT-Systeme und Daten über Benutzergruppen vergeben. 7.20a
- ☐ Regeln und dokumentieren, welche Zutrittsrechte zu schutzbedürftigen Räumen an welche Personen im Rahmen ihrer Funktionen aktuell vergeben sind. 9.1a
- ☐ IT-Systeme in öffentlich zugänglichen Bereichen vor unberechtigtem Zugang schützen (und videoüberwachen). 9.3a
- ☐ Informationsdienste für Besucher abgrenzen. 9.3b
- ☐ Die Netzanschlüsse angemessen vor unberechtigtem Zugang schützen (z.B. durch Deaktivierung nicht benötigter LAN-Anschlüsse, Port-Security / NAC). 9.3c

II.4.C Administratoren

Für die Umsetzung weiterer Absicherungen werden qualifizierte Administratoren mit entsprechenden Ressourcen benötigt:

- ☐ Administrations-Accounts nur für administrative Zwecke nutzen. 7.21a
- ☐ Standardpasswörter (auch für externe Firmen-Wartungszugänge) bei der ersten Nutzung ändern. 7.21b
- ☐ Sicherstellen, dass lokale Administrationsrechte nur von den dafür registrierten Personen nutzbar sind. 7.21c
- ☐ Für eine Notfalladministration einen lokalen, gesichert verwalteten und an sicherer Stelle hinterlegten Admin-Notfall-Account einrichten. 7.21d
- ☐ Gute Rahmenbedingungen für qualifizierte Mitarbeiter und Administratoren schaffen. 8.1a

II.4.D Allgemeine Netzwerksicherheit

Maßnahmen zur allgemeinen Absicherung des Netzwerks müssen ergriffen werden:

- ☐ Das Prozessleittechnik-Netz von allen anderen Netzwerken getrennt betreiben (empfohlen, falls realisierbar). 6.1a
- ☐ Die unterschiedlichen Netzbereiche angemessen voneinander trennen. 7.1a
- ☐ Umsetzung einer IT-Netzwerk-Segmentierung in unterschiedliche Schutzzonen. Falls die empfohlene physikalische Trennung nicht möglich sein sollte, die kritischen IT-Netzbereiche logisch trennen und die Kommunikation zwischen Netzbereichen unterschiedlicher Kritikalität gezielt steuern. 7.2a, 7.2b, 7.2c
- ☐ Für kritische Funktionen - soweit als möglich - Kabelverbindungen anstelle von Funkverbindungen verwenden. 6.3b
- ☐ Kritische Verbindungen mit alternativen Kommunikationswegen redundant absichern. 6.3c
- ☐ Sicherstellen (regelmäßig prüfen), dass bei Ausfall der primären Anbindungen die redundanten Anbindungen funktionieren und nach Fehlerbehebung wieder automatisch zurückgeschaltet wird. 6.3d
- ☐ Die Netzzugänge und die Kommunikationskanäle so gut wie möglich absichern (Sicherheitssysteme, sichere Konfiguration usw.). 6.3a
- ☐ Die Sicherheitsgateways (z.B. Firewalls) zur Regelung und Überwachung des Netzwerkverkehrs an den Übergangspunkten zwischen den einzelnen Netzsegmenten und zum Internet auf Stand der Technik implementieren und sicher konfigurieren. 7.3a
- ☐ Sicherstellen, dass die Konfiguration, die Pflege (z.B. die Anpassung der Regeln) und die Wartung (z.B. ein Update der Firmware) der Sicherheitsgateways zeitnah und sicher durch dafür qualifiziertes Personal durchgeführt wird. 7.3b
- ☐ Das Regelwerk auf den Sicherheitsgateways nach dem Minimalprinzip konfigurieren (u.a. nur erforderliche Quell- / Zieladressen, Ports, Anwendungen), dokumentieren und dieses regelmäßig prüfen. 7.3c
- ☐ Einen sicheren Betrieb der Sicherheitsgateways gewährleisten (z.B. redundante Auslegung, automatische Updates der Erkennungssignaturen, schnelles Update der Firmware insbesondere bei Bekanntwerden von Schwachstellen). 7.3d
- ☐ Auf den Betrieb eines WLANs im Prozessleittechnik-Netz verzichten (empfohlen). 7.37a

  Beim Einsatz von WLAN Folgendes beachten:
  - ☐ Das WLAN, das in den jeweiligen Sicherheitskontext des zugehörigen Netzwerks eingebunden ist, von allen anderen Netzen physikalisch trennen. 7.37b
  - ☐ Die Kommunikation im WLAN nach aktuellem Stand der Technik verschlüsseln. 7.37c
- ☐ Falls Zugriffe aus anderen Netzen auf das Prozessleittechnik-Netz nötig sind (nicht empfohlen) eine bereits bei Systemstart des Clients aktivierte VPN-Verbindung ohne Split-Tunneling ("Always On") mit Zwei-Faktor-Authentifizierung nutzen. 7.37d
- ☐ Den Mitarbeitern in der Leitstelle einen separaten, an ein geeignetes, Nicht-Prozessleittechnik-Netzwerk angeschlossenen, PC für weitere Aufgaben z.B. für Office und Email bereitstellen. 8.1c
- ☐ Generell alle Steuerungskomponenten gehärtet betreiben (z.B. Abschalten nicht benötigter Dienste, Ändern von Standardpasswörtern, falls möglich durch Vorab-Funktionstests gesichertes zeitnahes Einspielen von Patches, Betrieb in eigenen Netzbereichen, geschützt mit Firewalls etc.). 6.4b
- ☐ Den Internetzugang für Steuerungssysteme und produktionsnahe Systeme deaktivieren. 8.1b

  Beim Einsatz von Funknetzen Folgendes beachten:
  - ☐ Einen Netzplan, welcher unter anderem alle verwendeten Funk-Systeme enthält, erstellen. 7.38a
  - ☐ Für die Konfiguration und Einstellung der Funk-Systeme auf dafür qualifiziertes Fachpersonal zurückgreifen. 7.38b
  - ☐ Die Übertragungsanlagen vor Manipulation schützen. 7.38c
  - ☐ Eine verschlüsselte Datenübertragung bei Nutzung der Funkverbindung nutzen. 7.38d
  - ☐ Eine Fallback-Lösung bei Ausfall der Funkverbindung haben. 7.38e

- ☐ Regelmäßig prüfen, wie lange die eingesetzte Funktechnik bzw. die Frequenzbänder noch genutzt werden können. 7.38f
- ☐ Regelmäßig prüfen, dass keinerlei ungeschützte und ungewollte Verbindungen mit dem Internet vorhanden sind. 6.4a

II.4.E Fernzugriffe (Telearbeit, Fernwartung) absichern

- ☐ Prozesse und Regelungen zur Fernwartung definieren und dokumentieren. 13.1a
- ☐ Für Wartungszwecke durch externe Dienstleister: Organisationsinterne IT-/OT-Geräte zur Verfügung stellen oder im Sonderfall besondere Maßnahmen gegen Schadcodeeintrag treffen. 6.1b
- ☐ Die Fernwartung im Regelfall erst nach Freischaltung durch eine autorisierte Person und nur während der durchzuführenden Tätigkeiten ermöglichen. 13.1b
- ☐ Den Fernwartungszugang hinreichend absichern und die Übertragung sicher verschlüsseln. (Nutzung von VPN und angemessen sicherem Authentifizierungsverfahren) 13.1c
- ☐ Sicherstellen, dass auf allen Systemen keine Default-Zugänge mit Standardpasswörtern oder festkodierten Passwörtern existieren. 13.1d
- ☐ Für Administrator-Fernzugriffe eine besonders sichere Authentifizierung einrichten. 7.5a
- ☐ Ein sicheres Konzept für die Nutzung von Fernzugriff via VPN entwickeln und dieses dokumentieren. 7.6a
- ☐ Fernzugriffe restriktiv handhaben und protokollieren. 7.6b
- ☐ Falls Telearbeit in bestimmten Bereichen zugelassen ist, eine Richtlinie hierfür erstellen. 7.6c
- ☐ Einen Freigabeprozess für Telearbeitsplätze etablieren und regelmäßig sicherstellen, dass diese die IT-sicherheitstechnischen Anforderungen erfüllen (ausschließlich berufliche Nutzung, Aufbau der VPN-Verbindung gleich bei Systemstart ("Always-On"), Datenfluss ausschließlich zum Unternehmensnetzwerk, d.h. auch kein Split-Tunneling bei VPN, etc.). 7.6d
- ☐ Die VPN-Zugangskomponenten in einer eigenen vorgelagerten Schutzzone (eigene IDMZ) betreiben. 7.4a
- ☐ Die Firewall-Regeln für den Fernzugang nach dem Minimalprinzip konfigurieren. 7.4b
- ☐ Die Sicherheitssysteme für den Fernzugriff so konfigurieren, dass über den jeweils personalisierten Fernzugriff nur die von der Person benötigten Systeme und keine weiteren Systeme erreicht werden können. 7.4c

II.4.F Backups absichern

- ☐ Ein Datensicherungskonzept und -wiederherstellungskonzept erstellen, umsetzen und dokumentieren. 7.13a
- ☐ Regelmäßig mehrstufige Datensicherungen inkl. Offline-Backups durchführen. 7.13b
- ☐ Die Backup-Medien nur bei Sicherung und Rücksicherung mit dem Netzwerk bzw. Systemen verbinden. 7.14a
- ☐ Backups physisch sicher lagern, d.h. derart, dass diese nicht durch Feuer, Wassereinbruch, Sabotage, etc. zerstört werden können. 7.15a
- ☐ Die Vertraulichkeit der Backups sicherstellen. 7.16a
- ☐ Die Funktionsfähigkeit der Rücksicherung von Backups regelmäßig in Recovery-Tests überprüfen und diese Tests dokumentieren. 7.17a

II.4.G Schutz vor Schadsoftware

Maßnahmen zum Schutz vor Schadsoftware müssen ergriffen werden:

- ☐ Die Endgeräte (Clients und Server) mit einem Virenscanner bzw. einer angemessenen Endpoint-Protection-Lösung (Malware-Schutz) ausstatten. 7.11a
- ☐ Die Endpoint-Protection-Lösung automatisiert auf aktuellem Stand halten. 7.11b

☐	Zentrale Mechanismen zum Schutz vor Spam- und Phishing-Mails (z.B. Blockierung unerwünschter Anhänge, wie ausführbare Dateien (.exe, .scr, .chm, .bat, .com, .msi, .jar, .cmd, .hta, .pif, .scf, .ps1, etc.), Dateien mit Makros (wie z.B. .docm), oder auch Archiv-Dateien wie .zip und, falls es für Ihre Organisationsgröße Sinn ergibt, evtl. Sandboxing) einführen.	7.12a
☐	Den Mail-Client sicher konfigurieren.	7.12b
☐	Die Schnittstellen (USB, CD/DVD etc.) schützen, damit von dort aus keine Schadprogramme auf die IT-Systeme übertragen werden können.	7.12c
☐	Mitarbeiter im Umgang mit der Überprüfung von externen Dateien und Datenträgern sensibilisieren.	7.12d
☐	Die Ausführung von Makros und OLE-Objekten in Microsoft Office auf allen IT-Systemen deaktivieren bzw. nur die Ausführung digital signierter Makros mit geprüft vertrauenswürdiger Digitaler Signatur zulassen.	7.12e
☐	Sichere technische Verfahren für den Zugriff auf Informationen/Daten aus dem Internet einsetzen.	7.12f
☐	Eine Personal Firewall (z.B. Windows-Firewall, z.B. „uncomplicated firewall“ bei Linux) aktivieren.	7.12g
☐	Dateiendungen anzeigen lassen.	7.12h

II.4.H Software mit Updates und Patchmanagement sichern

Verwendete Software muss mittels Updates und einem geeigneten Patchmanagement abgesichert werden:

☐	Mittels Sicherheits- und Konfigurationsmanagement für die Systeme im Prozessleittechnik-Netz klare Vorgaben definieren und dokumentieren.	6.2a
☐	Patch- und Update-Prozess regeln.	6.5a
☐	Verfahren etablieren, um gegebenenfalls den Systemzustand vor dem Patch wiederherstellen zu können.	6.5b
☐	Veraltete, nicht patchbare Systeme bzw. Systeme, welche aus technischen Gründen nicht mehr geupdatet werden können, als Insellösung betreiben oder durch den Betrieb einer vorgeschalteten Firewall schützen.	6.6a
☐	Regeln, wie und wann veraltete Systeme durch neue, IT-sicherheitstechnisch bessere Systeme abgelöst werden.	6.6b
☐	Sicherstellen, dass die eingesetzte Software aus vertrauenswürdigen Quellen stammt.	7.9a

II.4.I Accounts absichern

Die Sicherheit aller Accounts muss gewährleistet werden (Minimalprinzip der Rechte):

☐	Angemessene Zugriffssicherheit auf Daten und IT-Systeme durch die gewählten Authentifizierungsverfahren gewährleisten.	7.22a
☐	Komplexität eines Passworts in der Passwortrichtlinie angemessen definieren.	7.23a
☐	Nutzer zur Geheimhaltung ihrer Authentifizierungsdaten verpflichten.	7.23b
☐	Die Änderung von Standardpasswörtern nach Erstanmeldung erzwingen.	7.23c
☐	Ausgeschiedene Mitarbeiter zeitnah sperren.	8.2c
☐	Automatische Bildschirmsperre nach einem angemessenen Inaktivitätszeitraum aktivieren.	9.4b
☐	Authentifizierungsversuche nach mehreren falschen Eingaben verzögern oder Benutzerkonten sperren.	9.4c

II.4.J Personal in Informationssicherheit einbinden

Sämtliches Personal muss in die Informationssicherheit mit einbezogen werden. Dafür muss ein Schulungs- und Sensibilisierungskonzept erstellt werden:

- ☐ Sicherstellen, dass geeignete Maßnahmen zur Schulung und Sensibilisierung der Organisationsleitung und der Beschäftigten regelmäßig eingeplant sind und umgesetzt werden. 8.8a
- ☐ Mitarbeiter für den Umgang mit mobilen Geräten schulen und auf die entsprechenden Gefahren sensibilisieren. 8.5c

Stufe 3: Weitere wichtige Absicherungen, Richtlinien und Dokumentation

Stufe 3:
Weitere wichtige
Absicherungen, Richtlinien
Und Dokumentation

Sie können mit Stufe 3 beginnen, sobald Sie die Stufen 0, 1 und 2 vollständig umgesetzt haben.

Nachdem auf Stufe 2 bereits erste dringliche Maßnahmen umgesetzt wurden, müssen nun weitere Absicherungen für andere wichtige Teilbereiche umgesetzt werden.

Gegen die bisher ermittelten Gefährdungen haben Sie wahrscheinlich in Stufe 2 bereits Abwehrmaßnahmen treffen können. Falls trotz der bisher getroffenen Maßnahmen weiterhin akute Gefährdungen vorhanden sein sollten, so können diese hier nochmals notiert werden. Die Liste kann verwendet werden, um damit eine Priorisierung geeigneter Stufe 3 - Maßnahmen vorzunehmen:

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Die im folgenden genannten Maßnahmen können parallel bearbeitet werden und bauen nicht zwingend aufeinander auf. Bei Auswahl der Maßnahmenreihenfolge kann gegebenenfalls die oben erneut aktualisierte Gefährdungsliste herangezogen werden.

III.1 Technische Vorkehrungen

Mit weiteren technischen Vorkehrungen müssen die bereits getroffenen Absicherungen weiter gestützt werden, um die Sicherheit deutlich zu verbessern.

III.1.A Weitere Absicherung von Servern, Clients und mobilen Geräten

- ☐ Die Software nach dem Minimalprinzip auswählen (d.h. nur notwendige Software und Dienste installieren), und die Softwarekomponenten inventarisieren. 7.8a
- ☐ Kritische Software vor ihrem Einsatz bewerten, freigeben und dies dokumentieren. 7.8b
- ☐ Veraltete/nicht mehr genutzte Systeme isolieren und nicht mehr benötigte Software deinstallieren. 7.8c
- ☐ IT-basierte Maßnahmen ergreifen, um die Sicherheit exponierter Server zu gewährleisten. 7.7a
- ☐ Den Webserver ausschließlich über https mit einer Verschlüsselung nach aktuellem Stand der Technik betreiben. 7.36a
- ☐ Sicherstellen, dass die mobilen Geräte IT-sicherheitstechnisch ausreichend abgesichert sind. 8.5a

III.1.B Absicherung der Cloud-Nutzung

☐	Mögliche Risiken sammeln, abwägen und die Ergebnisse dokumentieren.	7.24c
☐	Vor der Inbetriebnahme des Cloud-Dienstes einen Testlauf durchführen.	7.31a
☐	Regelmäßiges Testen der Notfallkonzepte.	7.32c
☐	Ein eigenes, separates Backup zusätzlich zu dem vereinbarten Backup des Cloud-Dienstanbieters erstellen.	7.34b
☐	Die Zugriffe aus der Cloud ins interne Netz auf das Nötigste beschränken und überwachen.	7.35b
☐	Ein geeignetes Sicherheitskonzept für die Cloud-Nutzung erstellen.	7.28a
☐	Das Sicherheitskonzept regelmäßig prüfen und bei Änderungen aktualisieren.	7.28b

III.1.C Virtualisierung sicher konzipieren

☐	Die Auslastung des Virtualisierungsservers bei Dimensionierung der Hardware berücksichtigen und regelmäßig überwachen.	7.39a
☐	Die Konfiguration des Systems soll eine ausreichende Isolation der virtuellen Maschinen gewährleisten.	7.39b
☐	Die virtuelle Infrastruktur in den bestehenden Sicherheitsmechanismen berücksichtigen.	7.39c
☐	Auf dem Virtualisierungsserver nur notwendige Dienste betreiben.	7.39d
☐	Die Virtualisierungsumgebung redundant auslegen.	7.39e

III.1.D Protokollierung einrichten

☐	Log-Dateien kritischer Systeme in ausreichendem Umfang erstellen.	7.40a
☐	Die Log-Dateien sicher ablegen.	7.40b
☐	Die Log-Dateien regelmäßig auf ungewöhnliche Aktivitäten prüfen und gegebenenfalls Warnmeldungen generieren und versenden.	7.40c
☐	Die zur Protokollierung gehörende Infrastruktur ausreichend dimensionieren.	7.40d
☐	Eine einheitliche Referenzzeitquelle (Zeitserver) für alle relevanten Informationssysteme einrichten.	7.40e
☐	Die Anforderungen des Datenschutzes bei gesammelten Protokolldaten erfüllen und den Betriebsrat bzw. die Personalvertretung mit einbinden.	7.40f

III.1.E Schwachstellenscans aus dem Internet und von intern

☐	Die aus dem Internet erreichbaren Systeme von außen regelmäßig und anlassbezogen auf Sicherheitslücken und vorhandene Schwachstellen prüfen.	11.1a
☐	Die IT-Infrastruktur regelmäßig und anlassbezogen mit einem Schwachstellenscanner von innerhalb des eigenen Netzes auf vorhandene Sicherheitslücken prüfen (Achtung: bei Systemen für die Trinkwasserversorgung / Abwasserentsorgung diese nicht direkt scannen, sondern erst als geklontes Testsystem nachbauen und dieses anschließend scannen).	11.1b

III.1.F Verwendung von Datenträgern absichern

☐	Eine Richtlinie zum ordnungsgemäßen Umgang mit mobilen Datenträgern sowie entsprechende Meldewege bei Verlust oder Diebstahl den Mitarbeitern bekannt machen.	8.6a
☐	Sicherstellen, dass mobile Datenträger für den Transport nach aktuellem Stand der Technik verschlüsselt sind.	8.6b
☐	Mitarbeiter für den Umgang mit mobilen Datenträgern schulen und auf die entsprechenden Gefahren sensibilisieren.	8.6c

III.1.G Datenschutzkonforme Löschung von Daten

Die Vorgehensweise bei der Löschung von Daten muss geregelt werden:

- ☐ Eine organisatorische Regelung in Kraft setzen, die sicherstellt, dass keine schützenswerten Daten von ausgesonderten Datenträgern gelesen werden können. 8.7a
- ☐ Technisch sicherstellen, dass keine schützenswerten Daten von ausgesonderten Datenträgern oder Geräten gelesen bzw. rekonstruiert werden können. 8.7b
- ☐ Verhindern, dass bei der Reparatur von Systemen sensible Daten ausgelesen bzw. rekonstruiert werden können (evtl. vorherige Entnahme der Festplatte und dies im Vorfeld zusätzlich vertraglich regeln). 8.7c
- ☐ Bei der Löschung sensibler Daten eine dazugehörige Protokollierung erfolgen lassen. 8.7d

III.2 Informationssicherheitsvorfälle

Informationssicherheitsvorfällen muss unter Berücksichtigung der Versorgungs- bzw. Entsorgungsnotwendigkeiten höchste Priorität eingeräumt werden, um die Informationssicherheit und den ordnungsgemäßen IT-Betrieb wieder zu gewährleisten, sowie ähnliche Vorfälle in Zukunft zu vermeiden.

III.2.A Umgang mit Informationssicherheits-Vorfällen

- ☐ Regeln, wie bei einem Verdacht auf einen Informationssicherheitsvorfall weiter vorgegangen wird (zu informierende Personen, insbesondere den ISB, wer macht die weiteren Analysen). 10.1a
- ☐ Die zu informierenden Ansprechpartner für Informationssicherheitsvorfälle definieren. 10.1b
- ☐ Meldeketten etablieren. 10.1c
- ☐ Den Informierten ermöglichen, Rückmeldungen zu geben. 10.1d

  Verfahren etablieren
  - ☐ wie Ausmaß und Tragweite eines Informationssicherheitsvorfalls ermittelt werden. 10.2a
  - ☐ mit denen sich der Verlust der Vertraulichkeit der Daten aufgrund Datenabfluss überprüfen lässt. 10.2b
  - ☐ mit denen sich die Integrität der Daten überprüfen lässt. 10.2c
  - ☐ mit denen sich die Verfügbarkeit der Daten überprüfen lässt. 10.2d
  - ☐ mit welchen sich nach einem Informationssicherheitsvorfall die Integrität und die Verfügbarkeit der Daten wiederherstellen lassen. 10.5a
- ☐ Kriterien und Entscheidungsprozesse definieren, um bei einem Informationssicherheitsvorfall festzustellen, wann es sich um einen IT-Notfall handelt. 10.3a
- ☐ Die wichtigsten Wiederanlaufparameter evaluieren und definieren. (MTA, WAZ, MTN, Wiederanlauf-Niveau) 10.5b
- ☐ Einen Plan mit einer Priorisierung der Meldewege sowie der dann einzuleitenden Maßnahmen vorhalten. 10.3b
- ☐ Klären, wo im Fall eines Informationssicherheitsvorfalls, der die eigenen Kapazitäten übersteigt, extern Hilfe angefordert werden kann. 10.4a

III.2.B Nachbehandlung von Informationssicherheitsvorfällen

- ☐ Nach Sicherheitsvorfällen prüfen, wie sich ähnliche Sicherheitsvorfälle in Zukunft vermeiden lassen. 10.6a
- ☐ Im Rahmen von Sicherheitsvorfällen erkannte Schwachstellen zeitnah beheben. 10.6b

III.3 Organisatorische Maßnahmen

III.3.A Zugangs- und Zugriffsrechte regeln

☐	Nachvollziehbare Prozesse für alle Beteiligten bei Personalwechsel einführen und dokumentieren.	8.2a
☐	Ein geregeltes Verfahren für die Vergabe sowie den Entzug von erforderlichen Zugangs- und Zugriffsrechten bei Wechsel der Aufgabenbereiche bzw. Ausscheiden aus der Organisation (z.B. Laufzettel) einführen.	8.2b

III.3.B Nutzung von Cloud-Diensten

☐	Eine Strategie für die Cloud-Nutzung erarbeiten.	7.24a
☐	Dokumentieren welche Cloud-Dienste in welcher Form im Einsatz sind.	7.24b
☐	Eine Sicherheitsrichtlinie für die Cloud-Nutzung erstellen.	7.25a
☐	Sicherstellen, dass der Sitz des Dienstleisters, sowie die Standorte der Server sich ausschließlich in Europa befinden oder anderweitige Maßnahmen mit dem Dienstleister vereinbaren, die zum Schutz der Infrastruktur vor staatlichen Zugriffen (aufgrund gesetzlicher Zugriffsrechte anderer Staaten mit unterschiedlicher Gesetzgebung) dienen.	7.25b
☐	Die relevanten Schnittstellen und Verantwortlichkeiten für die Cloud-Dienste eindeutig abgrenzen.	7.26a
☐	Die Rollen und Rechte für die Cloud-Dienste regelmäßig überprüfen.	7.26b
☐	Ein Migrationskonzept für die Einführung des Cloud-Dienstes erstellen und die (Rück-)Migration anschließend regelmäßig prüfen.	7.27a
☐	Existiert ein geeignetes Sicherheitskonzept für die Cloud-Nutzung?	7.28a
☐	Wird das Sicherheitskonzept regelmäßig geprüft und bei Änderungen aktualisiert?	7.28b
☐	Verschiedene Anbieter und Umsetzungsmöglichkeiten betrachten und entsprechend vordefinierter Kriterien miteinander vergleichen	7.29a
☐	Prüfen ob Zertifikate (sofern vorhanden) auf den relevanten Geltungsbereich ausgestellt wurden.	7.29b
☐	Ein detailliertes Anforderungsprofil für den Cloud-Dienstleister erstellen.	7.29c
☐	Prüfen ob der Cloud-Dienstanbieter dem Anforderungsprofil der Organisation entspricht.	7.29d
☐	Alle relevanten und wichtigen Anforderungen schriftlich in einem Vertrag regeln.	7.30a
☐	Die Vertragsgestaltung auf Rechtsgültigkeit prüfen (relevante Personen/Abteilungen mit einbeziehen z.B. Rechtsabteilung, DSB, etc.).	7.30b
☐	Die Erfüllung aller vertraglich vereinbarten Anforderungen an den Cloud-Dienst prüfen.	7.31b
☐	Ein separates Notfallkonzept für jeden Cloud-Dienst erstellen.	7.32a
☐	Das Notfallkonzept in der Organisation bekannt geben und zugänglich machen.	7.32b
☐	Ein Konzept für die Beendigung des Vertragsverhältnisses bzw. den Wechsel zu einem anderen Anbieter erstellen.	7.33a
☐	Die Durchführung von regelmäßigen Backups durch den Cloud-Dienstleister, entsprechend der vertraglich geregelten Anforderungen, prüfen.	7.34a
☐	Die vertraglich festgelegten Regelungen regelmäßig prüfen.	7.35a

III.3.C Aufrechterhaltung des Qualifikationsniveaus der Mitarbeiter und ausreichende Ressourcen

Alle Mitarbeiter, insbesondere die Systemadministratoren müssen über fachliche Qualifikationen, Fortbildungsmöglichkeiten sowie über ausreichend Ressourcen verfügen. Ihre Qualifikationen müssen zudem mit Ihrer Tätigkeit übereinstimmen:

☐	Alle Mitarbeiter bzw. externe Dienstleister müssen über die für ihre Aufgaben notwendigen Qualifikationen verfügen.	12.1a

☐	Allen Mitarbeitern müssen genügend Ressourcen für die ihnen übertragenen Aufgaben zur Verfügung stehen.	12.1b
☐	Alle Mitarbeiter regelmäßig schulen und passend zu den sich weiterentwickelnden Aufgaben / Herausforderungen fortbilden.	12.1c
☐	Administratoren müssen sich über bekannt gewordene Schwachstellen und Updates informieren.	12.2a
☐	Regelmäßig Maßnahmen durchführen, um das Bewusstsein der Mitarbeiter für die Informationssicherheit und den sicheren Betrieb nachhaltig zu stärken.	8.1g

III.3.D Auf sichere Programmierung achten

☐	Ein abgestimmtes Vorgehensmodell für die sichere Programmierung (gegebenenfalls beim Dienstleister) etablieren.	7.10a
☐	Informationssicherheit in allen Aspekten der Programmierung berücksichtigen (lassen).	7.10b
☐	Bei der Programmierung der speicherprogrammierbaren Steuerungen bzw. der Prozessleittechnik möglichst nur standard-konforme Software-Bausteine der Hersteller einsetzen.	7.10c
☐	Stets bei der Integration eines neu erstellten/geänderten Codes in die speicherprogrammierbaren Steuerungen bzw. der Prozessleittechnik einen vollständigen Funktionstest durchführen (lassen).	7.10d

III.3.E Zusammenarbeit mit externen Partnern regeln

☐	Sicherstellen, dass das Informationssicherheitsniveau durch das Auslagern von Bereichen, Prozessen oder Systemen an externe Dienstleister nicht vermindert wird.	13.2a
☐	Richtlinien mit Anforderungen an den externen Partner für den sicheren Umgang beim Datenaustausch zur Verfügung stellen.	13.3a
☐	Die Informationssicherheits-Leitlinie sowie die weiteren relevanten Regelungen für alle Lieferanten, Dienstleister und Dritte (inkl. den Inhabern von Altverträgen) verbindlich gestalten.	13.3b
☐	Richtlinien zur Aufrechterhaltung der eigenen Informationssicherheit im Umgang mit Lieferanten, Dienstleistern und Dritten erstellen, intern bekanntgeben und dies dokumentieren.	13.3c
☐	Prüfen, dass der externe Dienstleister für die durchzuführenden Arbeiten über eine ausreichende Qualifikation verfügt (z.B. Nachweis über Zertifizierungen und Bescheinigungen) insbesondere auch bezüglich Informationssicherheitsanforderungen.	13.3d
☐	Die externen Dienstleister hinsichtlich der Einhaltung der vertraglichen Regelung überprüfen.	13.3e
☐	Vertraulichkeitsvereinbarungen abschließen.	13.3f
☐	Regelungen bezüglich des Ausscheidens von Mitarbeitern bei externen Dienstleistern sowie für die Beendigung von Vertragsverhältnissen mit externen Dienstleistern einführen.	13.3g
☐	Die Wartung durch externes Personal detailliert vertraglich regeln.	13.4a
☐	Für Wartungsarbeiten spezielle Zeitfenster vorhalten.	13.4b
☐	Externe vor Beginn der Wartungsarbeiten angemessen authentifizieren (z.B. Ausweiskontrolle)	13.4c
☐	Wartungsarbeiten angemessen überwachen.	13.4d
☐	Externe Partner ausreichend auf die einzuhaltenden Informationssicherheitsaspekte hinweisen und dementsprechend eine Schulung und Sensibilisierung des Personals des externen Partners durchführen.	13.5a
☐	Die Auftragsverarbeitung vertragsmäßig und in Übereinstimmung mit der DSGVO regeln.	13.6a
☐	Die Dokumentation des Dienstleisters über das Schutzniveau regelmäßig überprüfen.	13.6b

III.3.F Beschaffung absichern

- ☐ Den ISB bei informationssicherheitsrelevanten Planungs- und Beschaffungsprozessen einbinden. 13.7a
- ☐ Bei Planungs- und Beschaffungsprozessen die Anforderungen der Informationssicherheit berücksichtigen. 13.7b
- ☐ Prüfen, ob vom Hersteller Informationen zur Informationssicherheit des Systems zur Verfügung gestellt werden. 13.7c
- ☐ Mögliche physikalische Störeinflüsse und Gefahren überprüfen. 13.7d
- ☐ Eine Richtlinie bezüglich Informationssicherheit für den Beschaffungsprozess erstellen. 13.7e

III.3.G Vorgaben und Richtlinien zur Aufrechterhaltung der Sicherheit erstellen

Die Reihenfolge bei der Erstellung der Richtlinien soll anhand der erfassten Situation bewertet werden. Es sind diverse Richtlinien zu erstellen und den Mitarbeitern vertraut zu machen:

- ☐ Richtlinien für den Umgang der Mitarbeiter mit technischen Systemen (z. B. Handhabung von Wechseldatenträgern), zum Kommunikationsverhalten bei E-Mail und in sozialen Netzwerken, Passwort-Richtlinien, Installation von Software, etc. 8.1d
- ☐ Eine Richtlinie für kritische Prozesse im Prozessleittechnik-Netz. 8.1e
- ☐ Ein grundsätzliches Nutzungsverbot für nicht freigegebene Hard- und Software. 8.4a
- ☐ Richtlinien zum Umgang mit dienstlicher Hard- und Software. 8.5b
- ☐ Eine Richtlinie zum Schutz personenbezogener Daten (z.B. Datenschutzkonzept) und diese mit der Leitlinie zur Informationssicherheit abstimmen. 1.5a

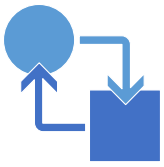
III.3.H Externe Kooperation für Informationssicherheit aufbauen

Die externe Informationsversorgung und die externe Unterstützung werden sichergestellt:

- ☐ Relevante Informationen aus vertrauenswürdigen Quellen beziehen und die Informationswege zur schnellen zielgerichteten Weiterverteilung an die verantwortlichen Personen etablieren. 12.3a
- ☐ Für die Informationssicherheit relevante Informationen austauschen. 12.4a

Stufe 4: Aufrechterhaltung der Informationssicherheit und kontinuierliche Weiterentwicklung

Stufe 4 stellt sicher, dass das durch Umsetzung der Maßnahmen in den Stufen 0, 1, 2 und 3 erreichte Sicherheitsniveau aufrechterhalten und weiter gesteigert werden kann.



Stufe 4: Aufrechterhaltung der Informationssicherheit und Kontinuierliche Weiterentwicklung

IV.1 Risikoanalyse

- ☐ Regelmäßig eine Gefährdungsanalyse insbesondere bezogen auf die für die Organisation kritischen Systeme durchführen, d.h. potentielle Schwachstellen und Bedrohungen regelmäßig auf ihre möglichen Auswirkungen und Eintrittswahrscheinlichkeiten überprüfen. 3.1b
- ☐ Regelmäßig angemessene Maßnahmen zur IT-Risikominimierung definieren, umsetzen und die Wirksamkeit der Maßnahmen prüfen. 3.1c

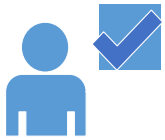
IV.2 Notfallübung

- ☐ Regelmäßig Notfallübungen in Bezug auf kritische Prozesse und Systeme durchführen. 5.3b

IV.3 Kontinuierliche Verbesserung

☐	Ein Konzept bzw. eine Regelung für die kontinuierliche Verbesserung der Informationssicherheit einführen und dies dokumentieren.	4.1a
☐	Änderungen zeitnah in die Dokumentationen einpflegen und die Aktualität der Dokumentationen regelmäßig überprüfen.	2.1g
☐	Regeln und dokumentieren, wie nicht mehr benötigte Systeme identifiziert werden und wie mit diesen umgegangen wird.	2.1h
☐	Durch fortlaufende Kontrolle sicherstellen, dass die Informationssicherheit auf aktuellem Stand gehalten wird.	4.1b
☐	Eine automatische Überwachung von Systemzuständen und -konfigurationen durchführen.	8.1f

Stufe 5: Auditierung und Zertifizierung



Stufe 5: Auditierung und Zertifizierung

Nach erfolgreicher Umsetzung der Handlungsempfehlung haben Sie einen Basis-Schutz für die Absicherung Ihrer Organisation erreicht. Dies ist als Vorstufe zu einer Zertifizierung zu sehen und speziell auf die Bedürfnisse von kleineren und mittleren Trinkwasserversorgern bzw. Abwasserentsorgern ausgerichtet. Die Handlungsempfehlung ersetzt weder eine Zertifizierung zu einem ISMS-Standard, noch hat sie den Anspruch, einen ISMS-Standard vollständig abzudecken. Sollten Sie sich für eine Zertifizierung entscheiden, haben Sie mit dieser Handlungsempfehlung einen Teil der Maßnahmen, welche später für eine Zertifizierung nach dem branchenspezifischen Sicherheitsstandard Wasser/Abwasser bzw. nach der IEC/ISO 27001 Norm oder nach IT-Grundschutz gefordert werden, umgesetzt. Ähnliches gilt für ISIS12 bzw. die überarbeitete Version CISIS12.

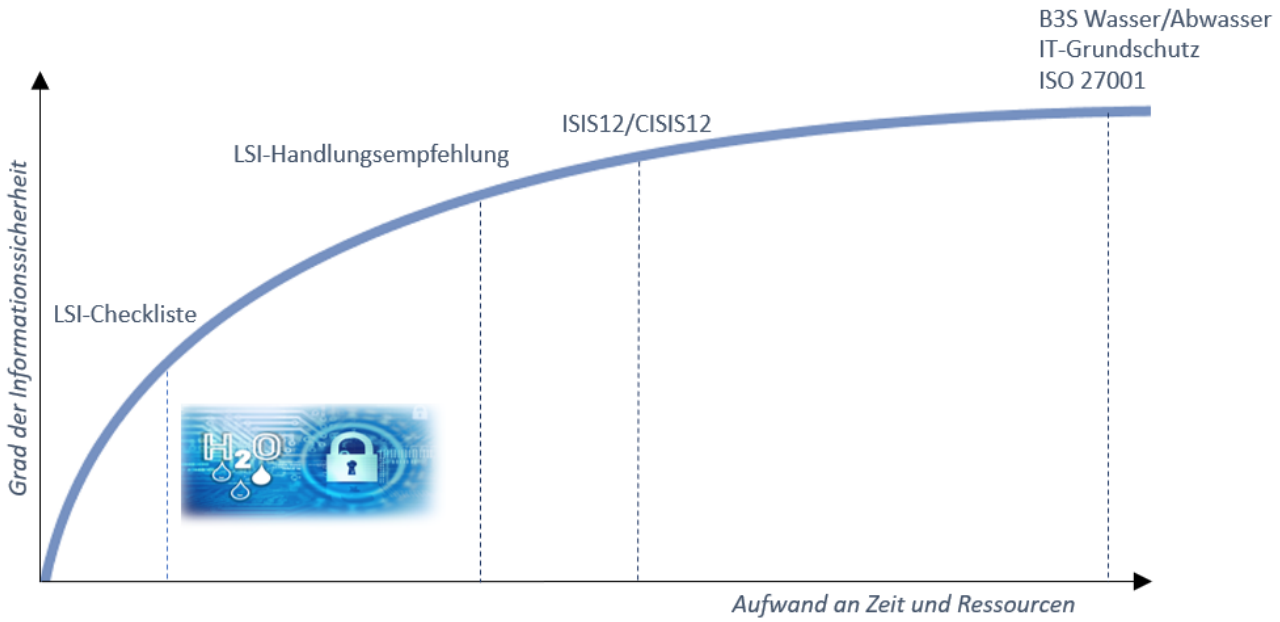
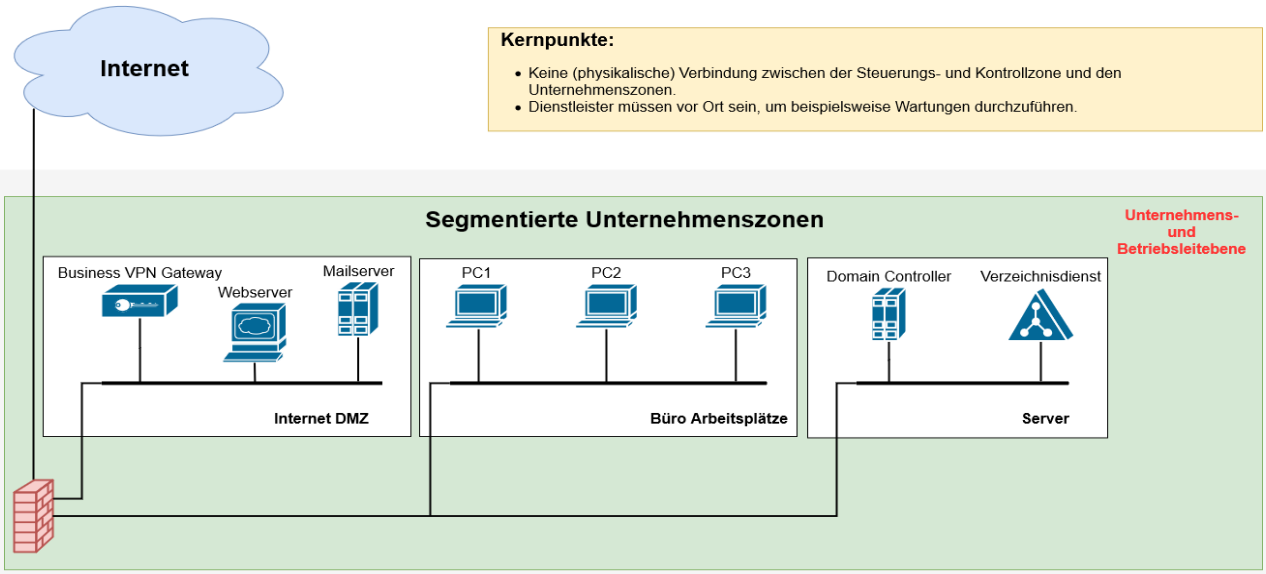


Abbildung 1: Einordnung der Handlungsempfehlung im Vergleich zu bekannten Standards nach Aufwand und Zuwachs an Informationssicherheit

Für den weiteren Ausbau der Informationssicherheit in Ihrer Organisation empfehlen wir mit einem Standard Ihrer Wahl weiterzuarbeiten. Bei allen Fragen rund um Informationssicherheit beraten wir Sie gerne.

Anhang

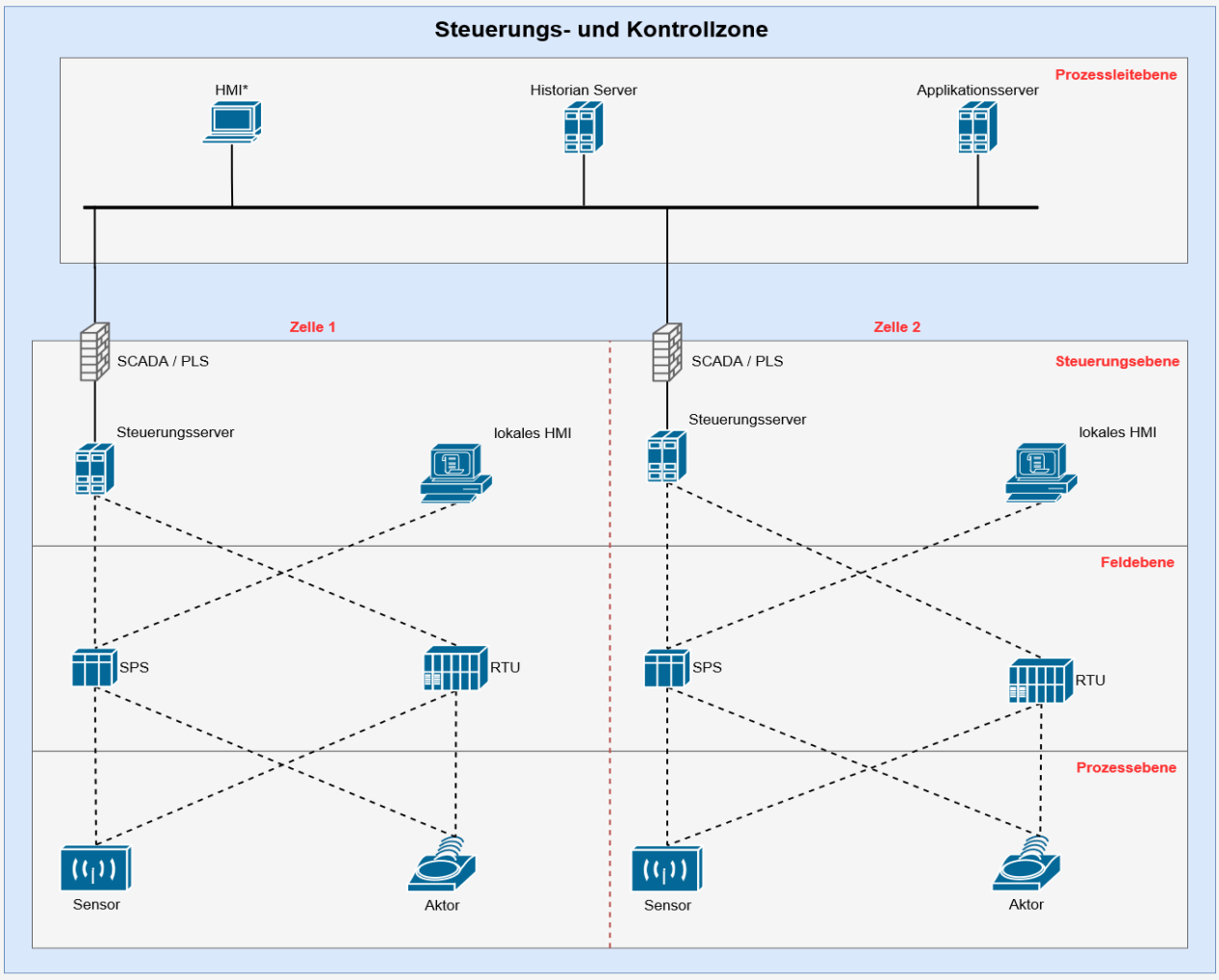
A1 – Physische Netztrennung



Kernpunkte:

- Keine (physikalische) Verbindung zwischen der Steuerungs- und Kontrollzone und den Unternehmenszonen.
- Dienstleister müssen vor Ort sein, um beispielsweise Wartungen durchzuführen.

Keinerlei Netzübergänge jeglicher Art



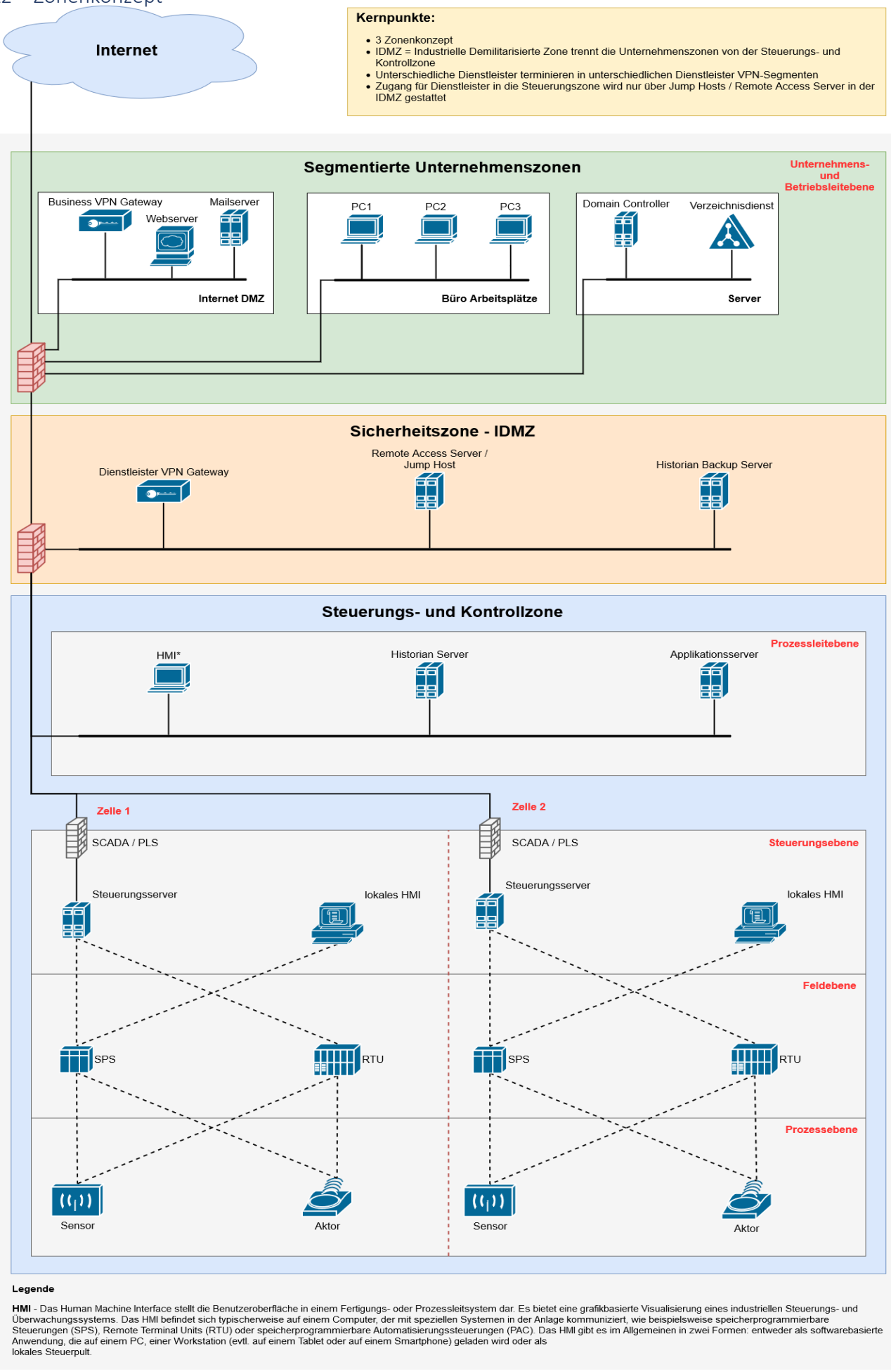
Legende

HMI - Das Human Machine Interface stellt die Benutzeroberfläche in einem Fertigungs- oder Prozessleitsystem dar. Es bietet eine grafikbasierte Visualisierung eines industriellen Steuerungs- und Überwachungssystems. Das HMI befindet sich typischerweise auf einem Computer, der mit speziellen Systemen in der Anlage kommuniziert, wie beispielsweise speicherprogrammierbare Steuerungen (SPS), Remote Terminal Units (RTU) oder speicherprogrammierbare Automatisierungssteuerungen (PAC). Das HMI gibt es im Allgemeinen in zwei Formen: entweder als softwarebasierte Anwendung, die auf einem PC, einer Workstation (evtl. auf einem Tablet oder auf einem Smartphone) geladen wird oder als lokales Steuerpult.

A2 – Zonenkonzept

Kernpunkte:

- 3 Zonenkonzept
- IDMZ = Industrielle Demilitarisierte Zone trennt die Unternehmenszonen von der Steuerungs- und Kontrollzone
- Unterschiedliche Dienstleister terminieren in unterschiedlichen Dienstleister VPN-Segmenten
- Zugang für Dienstleister in die Steuerungszone wird nur über Jump Hosts / Remote Access Server in der IDMZ gestattet



Legende

HMI - Das Human Machine Interface stellt die Benutzeroberfläche in einem Fertigungs- oder Prozessleitsystem dar. Es bietet eine grafikbasierte Visualisierung eines industriellen Steuerungs- und Überwachungssystems. Das HMI befindet sich typischerweise auf einem Computer, der mit speziellen Systemen in der Anlage kommuniziert, wie beispielsweise speicherprogrammierbare Steuerungen (SPS), Remote Terminal Units (RTU) oder speicherprogrammierbare Automatisierungssteuerungen (PAC). Das HMI gibt es im Allgemeinen in zwei Formen: entweder als softwarebasierte Anwendung, die auf einem PC, einer Workstation (evtl. auf einem Tablet oder auf einem Smartphone) geladen wird oder als lokales Steuerpult.