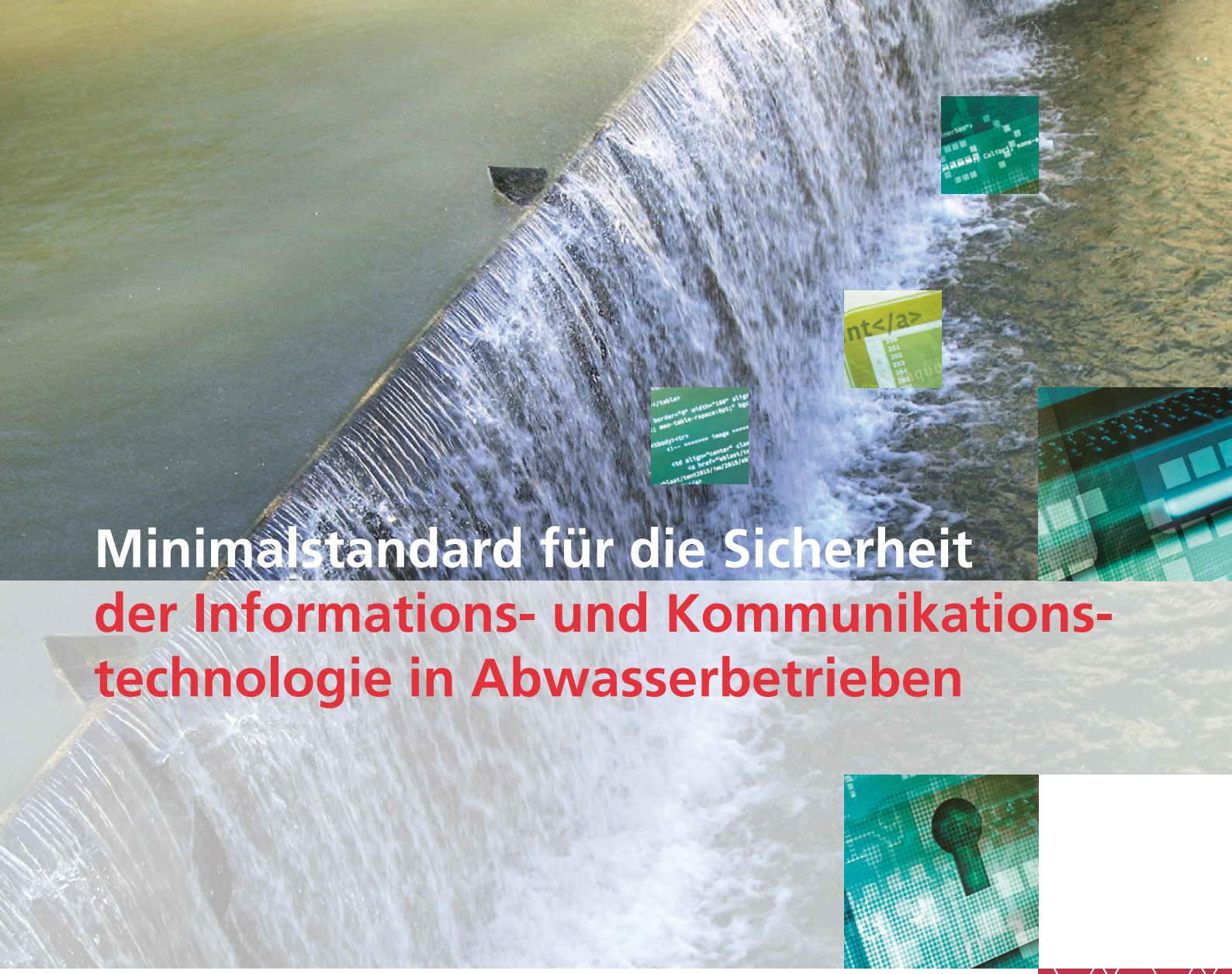

Minimalstandard für die Sicherheit der Informations- und Kommunikations-technologie in Abwasserbetrieben

VSA

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF
Bundesamt für wirtschaftliche Landesversorgung BWL

step by STEP

Inhaltsverzeichnis

Vorwort

Liebe Nutzerinnen und Nutzer des Branchendokumentes IKT-Minimalstandard Abwasser

Sie betreiben eine Kläranlage oder ein Versorgungsunternehmen. Ihre Anlage hat 365 Tage im Jahr reibungslos zu funktionieren. Sie als Fachperson kümmern sich versiert um den reibungslosen Ablauf aller Prozesse.

Durch die zunehmende Digitalisierung der Abwasserbetriebe, der Sonderbauwerke und des Abwassernetzes entstehen neue Risiken welche frühzeitig erkannt und adressiert werden müssen. Denn die Gefahr, dass gezielte Cyberangriffe auf die Prozess- (PLS-Netz-Umgebung) und Verwaltungstechnologie (Büro-Netz-Umgebung) der Abwasserbetriebe ausgeübt werden, steigt zunehmend.

Das Eidgenössische Departement für Wirtschaft, Bildung und Forschung WBF mit seinem Bundesamt für wirtschaftliche Landesversorgung BWL hat im Jahr 2018 den Informations-Kommunikations-Technologie (IKT)-Minimalstandard zur Verbesserung der IKT-Resilienz herausgegeben. Der IKT-Minimalstandard richtet sich insbesondere an IKT-Verantwortliche und an die Betreiber kritischer Infrastrukturen [1]. Resilienz bezieht sich in diesem Zusammenhang auf die Widerstandsfähigkeit, dass die Anlage bei einem Teilausfall von verschiedenen IKT-Systemen nicht vollständig versagt.

Der vorliegende «Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie in Abwasserbetrieben» (nachfolgend genannt «IKT-Minimalstandard Abwasser») ist im Handbuch «step by STEP» ebenfalls enthalten.

Die Abwasserbetriebe zählen zu den kritischen Infrastrukturen. Kritische Infrastrukturen zeichnen sich dadurch aus, dass Ausfälle an diesen sehr problematisch für eine moderne Gesellschaft sind. Die IKT-Systeme sind dabei ein neuer Aspekt, der sehr anfällig für Störungen sein kann. Der Branchenstandard **IKT-Minimalstandard Abwasser** soll entsprechend Unternehmen aus der Abwasserbranche dabei unterstützen, IKT-Störungen zu vermeiden, bzw. diese rasch zu beheben. Es ist ein Branchendokument, welches anerkannte Richtlinien und Empfehlungen zur Verbesserung der IKT-Sicherheit beinhaltet. Es verfolgt einen praxisorientierten Ansatz und richtet sich primär an die Betreiber bestehender Anlagen. Beim Neubau von Anlagen sollte zusätzlich der IKT-Minimalstandard des BWL verwendet werden.

Der vorliegende Branchenstandard wurde von step by STEP ausgearbeitet und wird bei Bedarf aktualisiert. Der IKT-Minimalstandard Abwasser richtet sich grundsätzlich an alle Unternehmen die an der Klärung von Abwasser beteiligt sind. Die Empfehlungen werden von den Unternehmen der Branche im Sinne einer «Selbstregulierung» freiwillig umgesetzt.

Das BWL, das BAFU, der VSA/FES, GRESE und die Kantone unterstützen den IKT-Minimalstandard Abwasser und die Anwendung in der gesamten Schweiz.

Max Schachtler

Hinweis
Bei step by Step sind unterstützende Dokumente für die Inventur, Bestandesaufnahme wie die Integration im Leistungsmodell SIA erhältlich.

1 Abgrenzung und Aufbau Branchendokument

Der Branchenstandard soll ein einheitliches Verständnis unter den Betrieben fördern und gleichzeitig einen einfachen Einstieg in die Thematik ermöglichen und ein hohes Schutzniveau gewährleisten. Das Branchendokument IKT-Minimalstandard Abwasser versteht sich explizit nicht als Konkurrenz zu existierenden internationalen Standards, sondern ist mit diesen kompatibel, bei gleichzeitig auf die Abwasserbetriebe abgestimmtem Umfang.

Die Fachinformation und Praxisbeispiele in den Kapiteln 2 bis 4 dienen als Grundlage für die Prävention (Vorsorgemassnahmen und Überlegungen vor Eintreten eines Ereignisses). Die Selbstbeurteilungscheckliste in Kapitel 5 dient als Planungshilfe bei der IST-Analyse, und gibt Hinweise zu Verantwortlichkeiten sowie für die Priorisierung und Umsetzung von Massnahmen. In Kapitel 6 finden sich Anweisungen für alle Benutzer von IT-Systemen. Kapitel 7 bietet Hilfestellung bei konkreten Vorfällen.

Das Branchendokument IKT-Minimalstandard Abwasser ermöglicht dem Benutzer konkrete Verhaltensweisen und Handlungsanweisungen, z. B. der SOMA (Sofortmassnahmen) Vorfallreaktionsplan, bereits im Vorfeld eines Ereignisses anhand der Vorlagen von step by STEP zu erstellen [2].

Dies ermöglicht im Ereignisfall eine rasche Beurteilung der Situation und die Auslösung von überlegten und zielführenden Handlungen.

Der IKT-Minimalstandard Abwasser richtet sich vor allem an die Betreiber von Anlagen. Bei der Planung von neuen Anlagen und grossen Erweiterungen empfiehlt es sich zusätzlich den IKT-Minimalstandard heranzuziehen. Dabei sollte dessen Einhaltung beim Bewilligungsverfahren als Voraussetzung definiert und die Ausführungsprojekte mittels Assessment auf diese Einhaltung überprüft werden.

2 IKT-Minimalstandard in Abwasserbetrieben

Die IKT-Sicherheit in Abwasserbetrieben bedingt ein risikobasiertes Verhalten und den Einsatz sicherer Systeme im Verantwortungsbereich der jeweiligen Betreiber. Der IKT-Minimalstandard Abwasser hat zum Ziel, den Abwasserbetrieben und Organisationen ein vielseitig einsetzbares Hilfsmittel zur Hand zu geben, wodurch sie individuell die Resilienz (Widerstandsfähigkeit bei einem Teilausfall von Systemen nicht vollständig zu versagen) ihrer IKT-Infrastruktur verbessern können. Der Fragebogen im Kapitel 5 erlaubt dem Betreiber, erste Erkenntnisse über den Sicherheitsstand seiner Anlage zu gewinnen, und zeigt mögliche Mängel auf. Der risikobasierte Ansatz des Standards ermöglicht die Umsetzung unterschiedlich ambitionierter Schutzniveaus, angepasst an die Bedürfnisse der jeweiligen Abwasserbetriebe.

Informationssicherheitsrisiken und deren möglichen Auswirkungen (wie: Gewässerverschmutzung oder Datenpannen) werden mit vertretbarem Aufwand minimiert, und kontinuierliche Prozesse werden etabliert, um die Sicherheit der Anlage periodisch zu überprüfen, und bei Bedarf zu verbessern.

Die Umsetzung von bewährten Massnahmen, wie sie in diesem Dokument dargestellt werden, können eine Vielzahl von IKT-Störungen und -Angriffen mit vertretbarem Aufwand abwenden.

2.1 Prozess-Effizienz und Sicherheit

Die fortschreitende Digitalisierung in den Abwasserbetrieben, des gesamten Abwassernetzes, in der Bewirtschaftung des Kanalisationsnetzes und der Sonderbauwerke ab der Leitzentrale erhöhen gleichermassen die Effizienz und Reinigungsleistung wie auch den Grad der Abhängigkeit von IKT-Systemen. So basiert zum Beispiel die Kanalnetzbewirtschaftung auf Sensoren, die u. a. den Durchfluss messen und kontrollieren und mittels unterschiedlicher Kommunikationsnetze der Zentrale die notwendigen Informationen liefern, so dass sich diese auf wechselnde Verhältnisse vorbereiten kann. Das gesamte System verlässt sich auf stabile Kommunikationsnetze und die Messwerte der unterschiedlichsten Sensoren. Das Prozessleitsystem (PLS) steuert, kontrolliert, überwacht, signalisiert und protokolliert die Prozesse.

Ebenso nimmt im Verwaltungsbereich in Abwasserbetrieben das Informationsbedürfnis stetig zu. Die Kommunikation zwischen PLS-Netz-Umgebung, nachfolgend OT genannt und der Verwaltung (Büro-Netz-Umgebung), nachfolgend IT genannt, ist sicherzustellen und gleichzeitig die Sicherheit zu gewährleisten. Letztere Aufgabe erfordert ein klares Verständnis der aktuellen Sicherheitsherausforderungen sowie der zu treffenden Massnahmen.

2.2 OT- und IT-Umgebung

Im Kontext eines Abwasserbetriebes gilt es zwischen der OT (**O**peration **T**echnology; PLS-Netz-Umgebung) und der klassischen IT (**I**nformation **T**echnology; Büro-Netz-Umgebung) zu unterscheiden, da diese zwei Systeme unterschiedliche Funktionen erfüllen und dementsprechend verschiedenen Ansprüchen unterliegen. Diese Unterschiede haben einen Einfluss auf die möglichen Sicherheitsmassnahmen, die getätigt werden können. Im Folgenden werden diese beiden Systeme kurz beschrieben.

Da OT- und IT-Umgebungen verschiedene Vorgaben bezüglich Sicherheit und Verfügbarkeit haben, muss den Schnittstellen zwischen diesen Umgebungen besondere Aufmerksamkeit gegeben werden. Es gilt, die Systeme netzwerktechnisch zu trennen, und nur die für den Betrieb notwendigen Datenflüsse zu erlauben.

OT (Operation Technology; PLS-Netz-Umgebung)

Das OT-Netz dient in erster Linie dazu Verbindungen zwischen den verschiedenen Komponenten der Automations-Prozesse herzustellen, damit diese die für die Prozessteuerung notwendigen Daten austauschen können. Auf den PCs im OT-Netzwerk sind meist eine Visualisierungs-Software für die Prozess-Automation installiert, sowie verschiedene Software, die von den Automations-Ingenieuren benötigt werden. Ebenfalls im OT-Netz vorhanden sind die Steuerungen, die die Prozesse kontrollieren. Das OT-Netz kann weiter aufgetrennt werden, falls Anlagen mit unterschiedlicher Kritikalität betrieben werden. Verbindungen zum OT-Netz sollten möglichst reduziert, gut kontrolliert und ständig überwacht werden.

Der Lebenszyklus der diversen Komponenten des OT-Netzes ist in der Regel relativ lang (mehrere Jahre). Updates können nicht immer zeitnah durchgeführt werden, da diese die Funktionalität gewisser (älterer) Komponenten beeinträchtigen können. Ausfälle im OT-Netz können zu Betriebsunterbrüchen führen, was gravierende Konsequenzen für die Abwasserbetriebe und somit das Unternehmen haben kann.

IT (Information Technology; Büro-Netz-Umgebung)

Das IT-Netz eines Abwasserbetriebes dient dazu, die Effizienz von administrativen Aufgaben zu steigern und deren Erledigung zu erleichtern. Auf einem typischen PC im Büro-Netz sind Software wie Microsoft Office (Word, Excel, etc.) und Outlook vorhanden. Das IT-Netz hat in den meisten Fällen direkten Internet-Zugriff.

Der Lebenszyklus der diversen Komponenten des IT-Netzes ist in der Regel eher kurz. Updates können und müssen zeitnahe durchgeführt werden, da diese in der Regel keine negativen Auswirkungen auf die Funktionalität der Systeme haben. Sollten durch ein Update dennoch Funktionen verloren gehen sind diese Auswirkungen selten gravierend. Auch der Einsatz von Schutzsoftware wie Endpoint Security ist wichtig.

2.3 Verantwortung

Betreiber

Die Verantwortung bezüglich Cybersicherheit liegt in letzter Instanz beim Betreiber. Nur er kann die Risikobereitschaft des Unternehmens festlegen und entsprechende Massnahmen veranlassen. Sind diese Massnahmen definiert, gilt es sicherzustellen, dass alle Betroffenen (Mitarbeiter, Systemlieferanten, Partner) diese kennen und sich ihrer Verantwortung diesen gegenüber bewusst sind.

Um die OT- und IT-Sicherheit zu gewährleisten, ist der Austausch des Betreibers mit dem Sicherheitsexperten und den Systemlieferanten OT und IT notwendig. Es gilt Verantwortungen klar zu definieren und diese möglichst vertraglich festzuhalten, z. B. indem sich die Systemlieferanten OT und IT verpflichten, ihrerseits den IKT-Minimalstandard zu erfüllen.

Die Erarbeitung von Massnahmen zur Prävention von Cyberrisiken initiiert der Betreiber. Der Betreiber stellt den IST-Zustand und die notwendigen Grundlagen (Netzwerk-Topologie, IKT-Inventar etc.) anhand den Dokumentenvorlagen und Formularen von step by STEP, sowie der Checklisten im Kapitel 5 dieses Standards, zusammen. Bei Bedarf kann hier auch die OT- und IT-Firma beigezogen werden.

Cybersicherheit ist eine ständige Aufgabe, die unabhängig von einer Erweiterung oder einem Ausbau umzusetzen ist.

Unabhängiger Sicherheitsexperte (Cyberexperte)

Der Sicherheitsexperte beweist seine Kompetenz durch Zertifizierungen, die eine kontinuierliche Weiterbildung voraussetzen (z. B. CISA), sowie seine berufliche Erfahrung im Bereich Cybersicherheit [3]. Ebenfalls wichtig ist, dass die beauftragte Cybersecurityfirma **neutral und unabhängig** agiert und keine Interessenskonflikte mit Lieferanten des Abwasserbetriebes aufweist. Idealerweise kann der Sicherheitsexperte bereits erste Erfahrungen im Bereich Industrie-Automation nachweisen. Andernfalls muss sichergestellt werden, dass er sich den unterschiedlichen Anforderungen von OT- und IT-Umgebungen bewusst ist.

Der vom Betreiber beigezogene Sicherheitsexperte erfasst den Sicherheits-Zustand der Systeme, falls diese der Betreiber nicht bereitstellt, und prüft die Cybersecurity-Massnahmen unabhängig von OT- und IT-Lieferanten. Er zeigt Risiken auf und unterbreitet Lösungsvarianten.

Hier ist es wesentlich, dass der Betreiber den Umfang der vom **Sicherheitsexperten** zu erbringenden Arbeit sowie die erwarteten Ergebnisse klar definiert, z. B. Audit des IST-Zustands anhand des IKT-Minimalstandard Abwasser, das zu einer klaren Dokumentation von Risiken und Massnahmen führt.

OT-Lieferant

Der OT-Lieferant kennt die von ihm gelieferten und gewarteten Systeme und deren Funktionalität. Er kann beim Erstellen des Inventars sowie beim OT-Netzwerk-Diagramm den Betreiber und/oder den Sicherheitsexperten unterstützen, und bei Ungewissheiten bezüglich der funktionalen Anforderungen der OT-Komponenten Klarheit schaffen.

IT-Lieferant

Der IT-Lieferant kennt die von ihm gelieferten und gewarteten Systeme und deren Funktionalität. Er kann beim Erstellen des Inventars sowie beim IT-Netzwerk-Diagramm den Betreiber und/oder den Sicherheitsexperten unterstützen, und kennt die aktuellen Sicherheitsmassnahmen und möglicherweise -Risiken der IT-Systeme.

Aufgaben des Planers in Bezug Cybersicherheit

Der Betreiber kann einem Planer (z. B. Verfahrensplaner, Elektroplaner) die Rolle erteilen, das Bindeglied zwischen dem Cybersicherheitsexperten (der das Gesamtsystem überwacht) und der OT- und IT-Firma zu sein. Bei Neubauten hat er sicherzustellen, dass die OT- und IT-Sicherheit von Anfang an berücksichtigt wird, und dass die entsprechenden Budget-Position bereits im Vorprojekt erstellt werden.

2.4 Sicherheit

Sicherheit ist kein Zustand sondern ein ständiger Prozess. Der Sicherheitsexperte führt den Betreiber durch den Prozess. Er kann technische und organisatorische Massnahmen empfehlen und bei deren Umsetzung zwischen den verschiedenen Akteuren koordinieren, begleiten und diese überprüfen. Das Excel-Tool des BWL [4] und die Umsetzungs-Tools von step by STEP stehen unterstützend für die Arbeit des Sicherheitsexperten zur Verfügung [5].

3 Risikoanalyse und Gefährdung

Der nachfolgende Risikokatalog umfasst die hauptsächlichen Gefahren, die auf Abwasserbetriebe einwirken. Er dient als Basis für eine auf die eigene Anlage abgestimmte Risikoanalyse.

Als grösstes Risiko muss sicher eine mögliche Gewässerverschmutzung betrachtet werden. Zu diesem Toprisiko können auch Cyberrisiken führen. Diese Risiken steigen in jüngster Zeit rasant an.

3.1 Hohe Anforderungen an die Verfügbarkeit

In den Abwasserbetrieben ist ein modernes OT-Netzwerk (**O**peration **T**echnology; PLS-Netz-Umgebung) und IT-Verwaltungsnetzwerk (**I**nformation **T**echnology; Büro-Netz-Umgebung) üblich. Basierend auf einer sicheren OT und IT werden Automationsprozesse gesteuert, Prozessdaten archiviert, Wartungsplanungen organisiert und sämtliche administrative Aufgaben realisiert. Je nach Grösse und Organisationsform des Abwasserbetriebes werden auch Verwaltungstätigkeiten, wie Buchhaltung oder Personalverwaltung, durch die Betreiber selbst erbracht.

Auf Grund der heutigen Verfahrensprozesse ist es nicht mehr möglich, den Abwasserbetrieb über einen längeren Zeitraum ohne Automation aufrecht zu erhalten. Zu dieser Automation zählen beispielsweise geregelte Pumpwerke, ein umfassendes biologisches Verfahren oder die Steuerung von Produktionsprozessen und Anlagen.

Die Leittechnik (PLS) überwacht eine Vielzahl automatisierter Prozesse und stellt die aktuellen Zustände visuell übersichtlich dar. Der Betreiber kann aufgrund dieser Informationen die Anlagenprozesse überprüfen, aktiv eingreifen, optimieren und den Pikettdienst anfordern.

Aufgrund dieser Anforderung ist eine hohe Verfügbarkeit der OT- und IT-Systeme zwingend notwendig.

3.2 Zunehmende Vernetzung und Benutzer

Die erforderliche Kommunikation für den Fernzugriff auf die Leittechnik, um beispielsweise den Pikettdienst zu vereinfachen oder die Meteo- oder Kanalnetzdaten miteinzubeziehen, birgt grosse Sicherheitsrisiken. Die wachsende Anzahl an Akteuren (wie: Gemeinden, Lieferanten, Dienstleister) die Zugriff auf die Systeme und Daten des Betriebs wünschen, erhöhen logischerweise die möglichen Einfallstore, die einem Angreifer zu Verfügung stehen.

Aufgrund dieser Vernetzungen moderner Betriebe und der Vielzahl an Akteuren muss ein angepasstes Sicherheitskonzept zum Schutz vor Cyberangriffen entwickelt und immer wieder überprüft werden. Der technische Fortschritt bringt immer wieder neue Cyberrisiken hervor und erfordert ein Bewusstsein für diese Gefahren, sowie der zu treffenden Massnahmen.

Das Branchendokument **IKT-Minimalstandard Abwasser** dient dazu das Sicherheitssystem aktuell zu halten. Die Einsatz- und Präventionsdokumente von step by STEP und in dessen Handbuch, sowie die nachfolgenden **Checklisten** nehmen Bezug auf den IKT-Minimalstandard des BWL.

3.3 Cyberangriff

Hackerangriffe haben sich von Teenagerstreichen zu einem milliardenschweren Wachstumsmarkt für die organisierte Kriminalität bis zu Terrorangriffen entwickelt. Steuerungen und Überwachungen von industriellen Anlagen waren bisher meist isoliert und blieben somit lange von den Folgen dieser Tendenz verschont. Durch die zunehmende Vernetzung werden diese Systeme jedoch für Manipulationen und Hackerangriffe anfälliger.

Gründe für einen Cyberangriff

Gründe für einen Cyberangriff auf ein Unternehmen können sein:

- Erpressung von Geld
- Ausnützung der Rechen-Power (CryptoMining, Botnetz, Trittbrett für weitere Angriffe)
- das Unternehmen als Versuchsziel/Angriffstest (zufällig oder gezielt)
- Manipulation oder Diebstahl von Prozessdaten
- Sabotage (Beeinträchtigung oder Zerstörung der Anlage oder Teile der Anlage)
- Spionage (Prozesswissen von Verfahren)
- Diebstahl durch Auslösen oder Umleiten von Zahlungen

Wie Angriffe erfolgen können

Es gibt eine Vielzahl von Möglichkeiten, wie ein Cyberangriff auf Unternehmen erfolgen kann. Dies kann über folgende Angriffsvektoren geschehen (nicht abschliessende Aufzählung):

- USB-Sticks
- E-Mails
- Internetseiten (durch Eingabe von Benutzerdaten oder ausführen von schädlichem Programmcode)
- mitgebrachte IT-Geräte (Notebooks, Smartphones, Tablets, etc.)
- WirelessLan-Accesspoints
- IoT-Devices u.a.m.

Folgen von Angriffen

Ebenso vielzählig wie die Angriffsmöglichkeiten sind auch die Auswirkungen solcher Angriffe:

- Befall der Systeme mit Viren oder Ransomware (Verschlüsseln der Daten)
- Beeinträchtigung einzelner Systeme oder der ganzen Anlage
- Ausfall einzelner Systeme oder der ganzen Anlage
- unsachgemässer Eingriff/Manipulationen am Automationsprozess der Anlage
- Manipulation oder Zerstörung von historischen Daten

3.4 Risiken für den Abwasserbetrieb

Finanzielle Risiken

Finanzielle Risiken stehen im Vordergrund, wenn sich ein Abwasserbetrieb selbst verwaltet. Durch die direkte Internetverbindung des IT-Netzes und die Nutzung von E-Mails ist es für Angreifer einfach, sich über die Benutzer Zugang zum System zu verschaffen.

Mögliche Risiken für den Betreiber sind:

- finanzielle Schäden durch Diebstahl über E-Banking-Anwendungen
- finanzielle Schäden durch Erpressung oder vorgetäuschte Erpressung
- finanzielle Schäden durch Betrug
- Haftung für Schäden an der Anlage und an Dritten
- Reputationsschaden durch negative Wahrnehmung der Öffentlichkeit und den für die Medienarbeit nötigen Aufwand

Risiken physischer Ereignisse

Bei physischen Ereignissen (Brand, Überflutung) ist Materialschaden oft nicht vermeidbar. Datenverlust und Ausfallzeit können jedoch stark reduziert werden, wenn wirkungsvolle technische und organisatorische Vorsorgemassnahmen vorhanden sind, wie:

- regelmässige Datensicherung,
- gesicherte Daten separat lagern (an entferntem Standort),
- im Voraus vereinbarte Hardware-Lieferungszeiten,
- im Voraus vereinbarte Wiederherstellungszeiten.

Risiken für die Anlage

Der Angriff auf einen Abwasserbetrieb hat oft nicht primär die Zerstörung von Anlagenteilen zur Folge sondern meist einen Ausfall oder Fehlfunktionen des Systems.

Mögliche Risiken für die Anlage sind:

- Anlagenschaden durch Ausfall des Automationsprozesses
- Anlagenschaden durch Fehlmanipulation am System
- Anlagenschaden durch Fehlfunktion des Systems

Risiken für die Gewässer

Je nach Dauer der technischen Beeinträchtigung und des betroffenen Anlageteils kann sich dies auf den Betrieb auswirken. Im Zweifelsfall ist entsprechende Hilfe anzufordern, respektive die Behörde zu avisieren.

Mögliche Risiken für die Gewässer sind:

- Ausfall relevanter Anlageteile
- verminderte Reinigungsleistung
- Gewässerverschmutzung

4 Prävention

Der IKT-Minimalstandard des BWL zur Verbesserung der IKT-Resilienz basiert auf dem NIST Cybersicherheit Framework Core [6], was die Anpassung an Unternehmen unterschiedlicher Grössen und unterschiedlicher Risikobereitschaft ermöglicht. Ziel dieses Ansatzes ist die Risiken, denen die Anlage ausgesetzt ist, zu identifizieren und diese auf ein akzeptables Niveau zu senken, wobei der Betreiber den Umfang der Massnahmen anhand seiner Sicherheitsbedürfnisse definiert. Diese wiederum sind von seiner Risikoeinschätzung und -bereitschaft abhängig.

Dies setzt die Kenntnis seiner Anlage, seiner IKT-Systeme und die in seinem Umfeld vorliegenden IKT-Systeme voraus um ein aktives Risiko-Management im Bereich Cybersicherheit zu betreiben. Dieses Risiko-Management ist schlussendlich ausschlaggebend, um zu entscheiden, welche Sicherheitsmassnahmen getroffen werden sollen.

4.1 Eigenschaften des Betriebes

Um Massnahmen für einen Betrieb festlegen zu können, muss dieser zunächst genauer eingeschätzt werden. Dazu sollten folgende Fragen beantwortet werden:

- Was wird getan?
  Aufgaben, Kompetenzen und Verantwortung des Abwasserbetriebes kennen und definieren.
- Wie wird es getan?
  Prozesse, Verfahren, Funktionen, Kommunikationsnetze, Erfordernisse kennen und definieren.
- Welche Rahmenbedingungen müssen dabei eingehalten werden?
  Gewässerschutzverordnung (GSchV) vom 28. Oktober 1998 (Stand 1. Juni 2018) verordnet in Art. 16 und 17 Massnahmen im Hinblick auf ausserordentliche Ereignisse, Einleitbedingungen.
- Wer ist dafür verantwortlich?
  Zuständigkeiten definieren, wer für die verschiedenen Aufgaben innerhalb des Betriebs verantwortlich ist. Darunter können die Gemeinde, der Zweckverband, der Gemeindeverband, die IKA oder die AG fallen.
- Welche Kommunikationsnetze werden verwendet?
  Z. B. für den Abwasserbetrieb, den Pikettdienst, das Abwassernetz, mit Gemeinden und mit Dritten.
- Welche Vorsorgemassnahmen sind vorhanden?
  Wird der Branchenstandard IKT-Minimalstandard Abwasser umgesetzt?
  Werden regelmässige Mitarbeiterschulungen durchgeführt?
  Wird Schutz-Software eingesetzt?
  Welche internen Regelwerke sind vorhanden und sind diese aktuell?
- Wie werden die Vorsorgemassnahmen kontrolliert?
  Z. B. führt der Cybersicherheitsexperte regelmässig ein Sicherheit-Audit durch?
- Welche Rahmenbedingungen liegen vor?
  Budget, Zeitaufwand. Abhängig des Sicherheitsbedürfnisses und der Risikobereitschaft; gute OT- und IT-Sicherheitsmassnahmen benötigen Zeit im täglichen Betrieb; z. B. durch Logins mit Passwörtern u. ä. Demgegenüber steht die Forderung nach Einfachheit und schneller Bedienung.

Die Antworten auf diese Fragen bilden die Grundlage für eine Unternehmensdokumentation und das nachfolgende Risikomanagement.

4.2 Risikomanagement

Die Verbesserung der IKT-Resilienz (Widerstandsfähigkeit) ist ein langfristiges Vorhaben. Dies gelingt mittels eines Risikomanagementprozesses, der sich in drei Teilprozesse gliedert und die Risikobereitschaft und -bewertung des Abwasserbetriebes mitberücksichtigt:

- Risikoanalyse
- Risikobewertung und
- Risikobewältigung

Die Risikobewertung bezüglich Angriffen umfasst hauptsächlich drei Faktoren:

- Wie wahrscheinlich ist es, dass die Anlage als Ziel eines Angriffs gewählt wird?
- Wie wahrscheinlich ist es, dass ein Angriff erfolgreich ist?
- Welcher Schaden würde für die Anlage entstehen, falls ein Angriff erfolgreich ist?

Das Schadenpotential eines erfolgreichen Angriffs ist schwer abzuschätzen und hängt vom Vorhaben des Angreifers ab. Handelt es sich um Spionage, so wird kaum ein direkter Schaden für die Anlage entstehen, da die Angreifer unerkannt bleiben möchten. Bei politischem Aktivismus wird ein grösstmöglicher Schaden angerichtet, um viel Aufmerksamkeit zu generieren.

Ungezielte Angriffe, die täglich flächendeckend via E-Mail oder durch Besuche von Internetseiten erfolgen, können bereits durch einfache Sicherheitsmassnahmen massiv eingeschränkt oder sogar ganz verhindert werden.

Die analysierten Risiken sind zu bewerten (auf einer Skala von 1 bis 5) und Massnahmen zu priorisieren und auszulösen, die das Gesamtrisiko auf ein für den Betrieb tragbares Niveau senken. Dies heisst, die IKT-Sicherheitsstrategie des Abwasserbetriebes ist darauf auszurichten, die für die Geschäftsprozesse notwendigen kritischen IKT-Betriebsmittel zu schützen. Dazu braucht es einen mehrschichtigen Ansatz, welcher international als Defense-in-Depth-Strategie bekannt ist.

4.3 Schutzmassnahmen mit Defense-in-Depth-Strategie implementieren

Der IKT-Minimalstandard des BWL beruht auf dem Prinzip von Defense-in-Depth. Darunter ist ein koordinierter Einsatz mehrerer Sicherheitsmassnahmen zu verstehen, um die IKT-Betriebsmittel in einem Unternehmen zu schützen. Die Strategie basiert auf dem militärischen Prinzip, dass es schwieriger ist ein komplexes und mehrschichtiges Abwehrsystem zu überwinden als eine einzige Barriere. Zu diesem Zweck wird das IKT-System in verschiedene Abstraktionsebenen unterteilt (Anlage, Netzwerk, Computer, Benutzer, etc.). Für jede dieser Ebenen sind sinnvolle Sicherheitsmassnahmen vorzusehen.

Zu den Sicherheitsmassnahmen einer Defense-in-Depth-Strategie gehören unter anderem:

- Schulung der Mitarbeiter,
- Antiviren-Software,
- Firewalls,
- Zugriffs-Überwachung sowie
- ein abgestuftes Passwortsystem.

Früher schien eine Firewall als erste und letzte Sicherheitsmassnahme gegen Angriffe ausreichend. Inzwischen haben sich weitere Massnahmen durchgesetzt, von denen im Folgenden eine Auswahl aufgezeigt werden:

- segmentierte Netzwerke,
- mit Endpoint Protection abgesicherte Computer,
- automatisierte Systemaktualisierungen,
- überwachen des Benutzerverhaltens und
- aktives Netzwerk-Monitoring u.a.m.

Diese Sicherheitsmechanismen erschweren und verzögern das Eindringen eines Angreifers. Zusätzlich wird dadurch Zeit verschafft, um den Angriff zu erkennen, Gegenmassnahmen zu implementieren und Wiederholungen zu verhindern.

5 Fragebogen IKT-Minimalstandard Abwasser

Dieser step by STEP-Fragebogen wurde entwickelt, um den IKT-Minimalstandard des BWL in die Praxis zu überführen.

Der IKT-Minimalstandard des BWL teilt den Prozess zur Verbesserung der Widerstandsfähigkeit gegen IKT-Risiken (IKT-Resilienz) in fünf Funktionen auf. Die Checklisten des IKT-Minimalstandards Abwasser übernehmen diese Gliederung. Die Funktionen lauten:

1. Identifizieren (Identify)
2. Schützen (Protect)
3. Erkennen (Detect)
4. Reagieren (Respond)
5. Wiederherstellen (Recover)

Der Fragebogen erlaubt es Betreibern eine IST-Analyse vorzunehmen, ohne sich in den IKT-Minimalstandard des BWL einarbeiten zu müssen. Werden bei dieser Selbsteinschätzung Mängel festgestellt, sollte dies als Anregung dienen den Sicherheitsstand der Anlage zu verbessern.

Wir empfehlen die Grundlagenerarbeitung selbstständig, unter Beizug der zuständigen OT- und IT-Firma, zu erarbeiten. Danach ist der neutrale Sicherheitsexperte für Informationssicherheit, zur Prüfung des IST-Zustandes mittels dem IKT-Minimalstandard Abwasser und Abgabe des Prüfberichtes, zu beauftragen.

Von der IST-Analyse bis zur Umsetzung von Massnahmen

Der Betreiber ist verantwortlich für die Sicherheit seines Betriebs und definiert die Massnahmen und Prioritäten. Dazu steht ihm der Fragebogen zur Verfügung, deren Fragen jeweils auf den IKT-Minimalstandard des BWL verweisen.

Es wird folgendes Vorgehen vorgeschlagen:

1. Der Betreiber beantwortet die Fragen mit JA oder NEIN. Sollten Sie mehrere Fragen nicht mit einem klaren JA beantworten können, besteht Handlungsbedarf.

2. Der Betreiber vervollständigt seine Dokumentation, um Lücken soweit wie möglich zu schliessen. Vorlagen Tools von step by STEP stehen ihm dazu zur Verfügung [5].

   In Ihrem Betrieb tätige Firmen (wie OT und IT) können unterstützend wirken, um die notwendigen Informationen zu vervollständigen. Offensichtliche Lücken im Grundschutz können allenfalls durch einfache Massnahmen bereits behoben werden.

3. Der beauftragte Sicherheitsexperte (SE) prüft Massnahmen mittels dem IKT-Minimalstandard, zeigt Risiken auf und unterbreitet Lösungsvarianten. Er stellt technische und organisatorische Massnahmen zusammen.

   Wesentlich ist, dass die beauftragte Cybersecurityfirma interessenneutral und unabhängig agiert und der Prüfer über ein nachgewiesenes und aktuelles Fachwissen verfügt – diesen Nachweis kann er beispielsweise mit der Zertifizierung zum Certified Information Systems Auditor (CISA) [3] erbringen.

4. Der Betreiber definiert die Prioritäten der Massnahmen und setzt deren Umsetzungstermin fest.

5. Der Sicherheitsexperte koordiniert, begleitet und überprüft die Umsetzung.

   Zwecks Berücksichtigung der betrieblichen Spezifitäten unterstützen die in Ihrem Betrieb tätigen Firmen den Sicherheitsexperten bei der Umsetzung der Sicherheits-Massnahmen.

6. Der Betreiber legt die regelmässige Überprüfung und Kontrolle der Sicherheitsmassnahmen fest. Leistungsverträge (Serviceverträge) mit dem Sicherheitsexperten und der OT- und IT-Firma sind notwendige Instrumente um die Cybersicherheit aktuell zu halten.

5.1 Inventar (Bestandesaufnahme) und Identifizierung (Identify)

Zur Analyse und Planung der Massnahmen muss ein Inventar (Bestandesaufnahme) der verschiedenen Systeme und Netzwerkverbindungen erstellt werden. Bei step by STEP sind Vorlagen erhältlich [5].

Nach der Inventur ist pro Position die Bewertung der damit verbundenen Risiken (Kritikalität) in Bezug des zu erfüllenden Geschäftsprozesses vorzunehmen.

Unter «Kritikalität» wird die Bedeutung einer Ressource verstanden, deren Wegfall eine existentielle Gefährdung darstellen würde. Zur Einstufung der Kritikalität ist nicht allein die Betrachtungseinheit, sondern auch die von ihr berührte Umgebung zu berücksichtigen.

So sind z. B. bei einem Fehlverhalten der Software eines IT-Systems potenzielle Auswirkungen in Betracht zu ziehen, die sowohl das System selbst als auch in der Folge dessen Umwelt (Umfeld) betreffen.

Die **Bewertung der Kritikalität** soll hinsichtlich der zu erfüllenden Geschäftsprozesse sowie der Risikostrategie des Abwasserbetriebes entsprechen. Jede Position, welche mit «hoch» eingestuft wird erfordert Massnahmen. Die Summe der Massnahmen ergibt die auf den Abwasserbetrieb angepasste Sicherheitsstrategie.

In einem weiteren Schritt sind die Rollen und Aufgaben der Benutzer zu katalogisieren und Vorgaben und Regelungen für diese vorzunehmen.

Zu ID.AM-5: Mögliche Kritikalitätseinstufung

Kritikalität	Art des Fehlverhaltens
hoch	OT-Fehlverhalten führt zu Störungen in den Prozessen oder Datenarchivierung. IT-Fehlverhalten macht sensitive Daten für unberechtigte Personen zugänglich oder verhindert administrative Vorgänge (z. B. Gehaltsauszahlung, Mittelzuweisung) oder führt zu Fehlentscheidungen infolge fehlerhafter Daten.
niedrig	Fehlverhalten, das zum Ausfall von Komponenten/Anlagenteilen oder Verlust von Daten führen kann.
keine	Alle übrigen Arten von Fehlverhalten

Legende zu den Tabellen

Die Checklisten sind in sieben Spalten unterteilt: Die erste Spalte beinhaltet die Frage zur Selbsteinschätzung, zwei weitere dienen zum Eintrag der Antwort JA oder NEIN.

Danach folgen drei Spalten, die anzeigen, wer Sie bei den jeweiligen Schritten (Fragestellung) am besten unterstützen kann. Die Spalte Referenz-IKT zeigt den Verweis zum entsprechenden Punkt im IKT-Minimalstandard des BWL.

Legende
SE = Sicherheitsexperte (Cyberexperte)
OT = Leitsystem-Lieferant (PLS-Umgebung)
IT = IT-Lieferant (Büro-Umgebung)

Schritt: Inventar Management (Asset Management)

Die Daten, Personen, Geräte, Systeme und Anlagen einer Organisation sind identifiziert, katalogisiert und bewertet. Die Bewertung soll ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse sowie der Risikostrategie der Organisation entsprechen.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Inventur Hardware OT Haben Sie eine Inventur aller OT-Systeme (Server, Netzwerkkomponenten, Bedientableaus, mindestens alle Geräte mit einer IP-Adresse)?			(x)	x		ID.AM-1
Inventur Software OT Haben Sie eine Inventur der benutzten Software (Betriebssystem, Office, Programme etc.)?			(x)	x		ID.AM-2
Inventur Hardware IT Haben Sie eine Inventur aller IT-Systeme (PCs, Drucker, Routers, Tablets, Smartphones, etc., mindestens alle Geräte mit einer IP-Adresse)?			(x)		x	ID.AM-1
Inventur Software IT Haben Sie eine Inventur der benutzten Software (Betriebssystem, Office, Programme etc.)?			(x)		x	ID.AM-2
Inventar Netzwerkverbindungen und Datenflüsse (OT und IT) Haben Sie ein Inventar aller Netzwerkverbindungen und der Datenflüsse, welche über diese Verbindungen geleitet werden?			(x)	x	x	

Kritikalität

Stufen Sie die Inventarpositionen ein.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Kritikalität einstufen OT Haben Sie Hardware, Software und Datenflüsse bezüglich ihrer Kritikalität eingestuft? Wie wichtig sind die verschiedenen Systeme für ihren Betrieb?			x	(x)		ID.AM-5
Kritikalität einstufen IT Haben Sie Hardware, Software und Datenflüsse bezüglich ihrer Kritikalität eingestuft? Wie wichtig sind die verschiedenen Systeme für ihren Betrieb?			x		(x)	ID.AM-5

Rollen und Aufgaben

Definieren Sie die Rollen und Aufgaben der Benutzer. Beachten Sie dabei, dass Mitarbeiter von Dienstleistern als Benutzer agieren.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Rollen und Aufgaben Benutzer OT Haben Sie die Rollen und Aufgaben der Mitarbeiter und Benutzer in Bezug auf Sicherheit klar definiert und dokumentiert? Ist es Dritten gestattet auf Prozesse und Daten Ihrer Anlage direkt zuzugreifen?			x	(x)		ID.AM-6
Rollen und Aufgaben Benutzer IT Haben Sie die Rollen und Aufgaben der Mitarbeiter und Benutzer in Bezug auf Sicherheit klar definiert und dokumentiert? Ist es Dritten gestattet auf Ihr IT-System direkt zuzugreifen?			x		(x)	ID.AM-6

Schritt: Vorgaben (Governance)

Die Governance regelt Zuständigkeiten, überwacht und stellt sicher, dass regulatorische, rechtliche und operationelle Anforderungen eingehalten werden.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Vorgaben und Regelungen Benutzer OT Haben Sie Vorgaben und Regelungen in Bezug auf Sicherheit erstellt und den Benutzern/Mitarbeitern kommuniziert? Verantwortung und Folgen, sind diese klar geregelt? Erfolgt eine Überprüfung und Aktualisierung regelmässig?			x	(x)		ID.GV-1
Vorgaben und Regelungen Benutzer IT Haben Sie Vorgaben und Regelungen in Bezug auf Sicherheit erstellt und den Benutzern/Mitarbeitern kommuniziert? Verantwortung und Folgen, sind diese klar geregelt? Erfolgt eine Überprüfung und Aktualisierung regelmässig?			x		(x)	ID.GV-1

Schritt: Risikomanagement (Risk Assessment)

Der Betreiber kennt die Auswirkungen von Cyberrisiken auf den Betrieb.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Risiken System OT Haben Sie die Risiken, denen ihre Systeme ausgesetzt sind, erfasst und priorisiert und sind diese akzeptierbar?			x	(x)		ID.RA-5
Risiken System IT Haben Sie die Risiken, denen ihre Systeme ausgesetzt sind, erfasst und priorisiert und sind diese akzeptierbar?			x		(x)	ID.RA-5

Schritt: Lieferketten Risikomanagement

Der Betreiber legt die maximalen Risiken fest, die der Betrieb im Zusammenhang mit Lieferantenrisiken zu tragen gewillt ist und berücksichtigt diese bei der Ausschreibung, der Beschaffung und im Ersatzwesen.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Enthalten Ihre Beschaffungsrichtlinien für OT-Lieferanten (Leitsystem) Vorgaben bezüglich IKT-Sicherheit?			(x)	x		ID.SC-3
Enthalten Ihre Beschaffungsrichtlinien für Messtechnik-Lieferanten Vorgaben bezüglich IKT-Sicherheit?			(x)	x		ID.SC-3
Enthalten Ihre Beschaffungsrichtlinien für Zusatzdienstleister (Drittsteuerung, Drucker, Kameras, etc.) Vorgaben bezüglich IKT-Sicherheit?			(x)	x	x	ID.SC-3
Enthalten Ihre Verträge mit IT-Lieferanten Vorgaben bezüglich IKT-Sicherheit, wie Betriebs-, Reaktions- und Wiederherstellungsprozesse?			(x)		x	ID.SC-3

Schritt: Zusatz

Überprüfen Sie die Sicherheitsmassnahmen.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Prüfung der Sicherheit OT Lassen Sie den Stand der Informationssicherheits-Massnahmen durch eine unabhängige Instanz regelmässig überprüfen?			x	(x)		Zusatz
Prüfung der Sicherheit IT Lassen Sie den Stand der Informationssicherheits-Massnahmen durch eine unabhängige Instanz regelmässig überprüfen?			x		(x)	Zusatz

5.2 Schützen (Protect)

Als nächstes gilt es, die identifizierten Systeme zu schützen, um Infektion durch Schadsoftware zu verhindern und deren Auswirkung zu minimieren. Die Schutzmassnahmen müssen den Aufgaben der Systeme angepasst werden und dürfen deren Betrieb nicht behindern.

Schritt: Zugriffsmanagement und -steuerung (Access Control)

Stellen Sie sicher, dass der physische und logische Zugriff auf IKT-Betriebsmittel und -Anlagen nur für autorisierte Personen, Prozesse und Geräte möglich ist, und dass der Zugriff nur für zulässige Aktivitäten möglich ist.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Benutzerrechte OT Haben Sie die Benutzerrechte (Lese-/Schreibe-Zugriff auf Dateien, auf die Veränderungen der Systemeinstellungen, etc.) auf den Systemen limitiert? Haben Sie ein Berechtigungskonzept verfasst, in welchem die Rechte auf die Aufgaben der Mitarbeiter im Betrieb angepasst sind? Wird dabei der Grundsatz «so wenig Rechte wie möglich, so viele wie nötig» eingehalten?			x	(x)		PR.AC-4
Benutzerrechte IT Haben Sie die Benutzerrechte (Lese-/Schreibe-Zugriff auf Dateien, auf die Veränderungen der Systemeinstellungen, etc.) auf den Systemen limitiert? Haben Sie ein Berechtigungskonzept verfasst, in welchem die Rechte auf die Aufgaben der Mitarbeiter im Betrieb angepasst sind? Wird dabei der Grundsatz «so wenig Rechte wie möglich, so viele wie nötig» eingehalten?			x		(x)	PR.AC-4
Trennung OT und IT Haben Sie das Leitsystem- und Automations-Netz (OT) von der restlichen IKT-Infrastruktur (IT-Büro-Netz) entweder physisch oder mit einer Firewall getrennt?			x	(x)	(x)	PR.AC-5
Trennung unterschiedlicher OT Haben Sie das Leitsystem- und Automations-Netz (PLS) von weiteren, weniger kritischen OT-Netzen (beispielsweise zur Steuerung des BHKW, …) entweder physisch oder mit einer Firewall getrennt?			x	(x)		PR.AC-5

Schritt: Sensibilisierung und Ausbildung (Awareness and Training)

Stellen Sie sicher, dass Ihre Mitarbeitenden und externen Partner regelmässig bezüglich aller Belange der Cybersicherheit angemessen geschult und ausgebildet werden. Stellen Sie sicher, dass Ihre Mitarbeitenden und externen Partner ihre sicherheitsrelevanten Aufgaben gemäss den zugehörigen Vorgaben und Prozessen ausführen.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Schulung Mitarbeiter OT Werden ihre Mitarbeiter regelmässig bezüglich Cyberrisiken geschult und informiert?			x	(x)		PR.AT-1
Schulung Mitarbeiter IT Werden ihre Mitarbeiter regelmässig bezüglich Cyberrisiken geschult und informiert?			x		(x)	PR.AT-1

Schritt: Informationsschutzrichtlinien (Information Protection Processes and Procedures)

Erstellen Sie Richtlinien zum Schutz von Informationssystemen und Betriebsmitteln.
Nutzen Sie diese Richtlinien, um die Informationssysteme und Betriebsmittel zu schützen.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Datensicherung OT Werden Daten regelmässig an einem entfernten Standort gesichert?			x	(x)		PR.IP-4
Test Datensicherung OT Wird die Datensicherung regelmässig getestet?			x	(x)		PR.IP-4/PR.IP-10
Datensicherung IT Werden Daten regelmässig an einem entfernten Standort gesichert?			x		(x)	PR.IP-4
Test Datensicherung IT Wird die Datensicherung regelmässig getestet?			x		(x)	PR.IP-4/PR.IP-10

Schritt: Aktualisierungen, Unterhalt (Maintenance)

Stellen Sie sicher, dass Aktualisierungen den von Ihnen geltenden Richtlinien und Prozessen durchgeführt werden.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Softwareaktualisierung OT Installieren Sie, wo möglich, Softwareaktualisierung zeitnah nach deren Veröffentlichung?			(x)	x		PR.MA-1
Softwareaktualisierung IT Installieren Sie, wo möglich, Softwareaktualisierung zeitnah nach deren Veröffentlichung?			(x)		x	PR.MA-1

Schritt: Zusatz-Kriterium

Stellen Sie den regelmässigen Service sicher.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Regelmässiger Service OT Führt die OT-Firma einen regelmässigen Service und eine Überwachung ihrer gelieferten Produkte durch? Ist der Service dokumentiert, wie auch der Leistungsumfang?			(x)	x		Zusatz
Regelmässiger Service IT Führt die IT-Firma einen regelmässigen Service und eine Überwachung ihrer gelieferten Produkte durch? Ist der Service dokumentiert, wie auch der Leistungsumfang?			(x)		x	Zusatz
Regelmässige Prüfung SE (Sicherheitsexperte Cyber) Wird die Wirksamkeit der Sicherheitsmassnahmen regelmässig von unabhängiger und interessenneutraler Stelle überprüft? Und führt sie die Überwachung ihrer gesamten Sicherheits-massnahmen durch? Sind seine Leistungen vertraglich definiert und festgelegt?			x			Zusatz

Schritt: Einsatz von Schutztechnologie (Protective Technology)

Installieren Sie technische Sicherheits-Lösungen, um die Sicherheit und Resilienz Ihrer IKT-Systeme und Ihrer Daten gemäss den Vorgaben und Prozessen zu garantieren.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Konfigurieren OT Konfigurieren Sie Ihre Systeme so, dass nur die für den Betrieb nötige Funktionalität gewährleistet ist?			(x)	x		PR.PT-3
Schutztechnologien OT Setzen Sie Schutztechnologien ein (Intrusion-Detection & Protection, Webfilter, etc.)?			(x)	x		PR.PT-4
Prüfen Aktualität OT Prüfen Sie die Aktualität von Schutztechnologien regelmässig?			(x)	x		PR.PT-4
Konfigurieren IT Konfigurieren Sie Ihre Systeme so, dass nur die für den Betrieb nötige Funktionalität gewährleistet ist (kein WLAN für Drucker wenn nicht benötigt, keine Fernverbindungsmöglichkeit wenn nicht benötigt, etc.)?			(x)		x	PR.PT-3
Schutztechnologien IT Setzen Sie Schutztechnologien ein (Endpoint Detection & Response, Webfilter, Spamfilter mit Sandbox und Monitoring, ...)?			(x)		x	PR.PT-4
Prüfen Aktualität IT Prüfen Sie die Aktualität von Schutztechnologien regelmässig?			(x)		x	PR.PT-4

Schritt: Zusatz-Kriterium

Stellen Sie das Vier-Augen-Prinzip sicher.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
IT Stellen Sie im E-Banking sicher, dass Zahlungen durch zwei Personen freigegeben werden müssen?			(x)			Zusatz

5.3 Erkennen (Detect)

Lange Zeit beschränkte man sich auf den Schutz von Informationen. Heute sind Angriffe so ausgeklügelt, dass das Erkennen von Angriffen eine eigene Disziplin der Informationssicherheit darstellt.

Die Frage ist nicht mehr, ob man angegriffen wird, sondern, wann man erkennt, dass man angegriffen wurde. Wie der Fall bei RUAG zeigt, kann dies Jahre dauern [7].

Mit diesem Bewusstsein müssen Massnahmen zu einer zeitnahen Detektion des Angriffes getroffen werden, um den Schaden zu minimieren.

Detektionsmassnahmen sollten mit dem Sicherheitsexperten ausgearbeitet und durch den Betreiber ausgeführt werden.

Schritt: Überwachung (Sicherheit Continous Monitoring)

Stellen Sie sicher, dass das IKT-System inkl. aller Betriebsmittel in regelmässigen Intervallen überwacht wird, um einerseits Cybervorfälle zu entdecken und anderseits die Effektivität der Schutzmassnahmen überprüfen zu können.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Zugriff OT Werden Zugriffe und Systemmeldungen auf Netzwerk- und Daten-Ebene so aufgezeichnet, dass für eine angemessene Zeitspanne geklärt werden kann, wer wann welches System genutzt und auf welche Daten zugegriffen hat?			x	(x)		DE.CM-1 bis DE.CM-3
Software gescannt OT Falls es der Systemlieferant erlaubt: Werden Systeme regelmässig mit einer aktuellen Antivirus-Software gescannt?			x	(x)		DE.CM-7
Verwundbarkeitanalyse OT Werden regelmässig Verwundbarkeitsanalysen durchgeführt?			x	(x)		DE.CM-8
Zugriff IT Werden Zugriffe und Systemmeldungen auf Netzwerk- und Daten-Ebene so aufgezeichnet, dass für eine angemessene Zeitspanne geklärt werden kann, wer wann welches System genutzt und auf welche Daten zugegriffen hat?			x		(x)	DE.CM-1 bis DE.CM-3
Software gescannt IT Wird ein modernes Endpoint-Protection-Tool eingesetzt, welches Angriffe erkennt, blockiert und deren Analyse erlaubt?			x		(x)	DE.CM-7
Verwundbarkeitanalyse IT Werden regelmässig Verwundbarkeitsanalysen durchgeführt?			x		(x)	DE.CM-8

Schritt: Zusatz-Kriterien

Schulen Sie Ihre Mitarbeiter und stellen Sie Kontrolllisten bereit.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Werden Mitarbeiter dazu animiert, Verdacht und Vorfälle aktiv zu melden?			x	(x)	(x)	Zusatz
Wird regelmässig geprüft, ob Passworte von Mailaccounts des Betriebs in einem Data-Breach veröffentlicht wurden [8]?			x		(x)	Zusatz

5.4 Reagieren (Respond)

Zu den Kernkompetenzen von Reagieren gehört die Reaktionsplanung, die die Kommunikation und Koordination während eines Angriffes, sowie die Analyse und Mitigation der Attacke berücksichtigt.

Wird ein Angriff erkannt, geht es darum, möglichst schnell und besonnen darauf reagieren zu können. Dazu müssen Ausmass und Auswirkungen möglichst schnell erfasst werden können. Dazu hilft ein **Vorfallreaktionsplan** [5], der in den «Formularen» und der Vorlage «Individuelle Einzelfälle» im step by STEP Handbuch abgebildet ist.

Die Reduktion von Folgeschäden, wie die Ausbreitung auf weitere Netzwerksegmente, kann nur erfolgen, wenn entsprechende «Formulare» und «Individuelle Einzelfälle» (Reaktionspläne) im Vorfeld eines Ereignisses bereits erstellt wurden und griffbereit (als Papierausdruck) vorliegen.

Um eine Infektion wirkungsvoll eindämmen zu können, müssen die auszuführenden Sofortmassnahmen (SOMA Vorfallreaktionsplan) durch den Betreiber selbst durchgeführt werden können, da zeitnahes Handeln hier von grosser Wichtigkeit ist.

Die Sofortmassnahmen (SOMA Vorfallreaktionsplan) werden sich in vielen Fällen auf zwei Punkte begrenzen:

- betroffene Maschine(n) vom Netzwerk trennen, WLAN-Verbindung (physisch, nicht Stromkabel ziehen!)
- zuständige Personen informieren

Danach wird die zuständige Person das weitere Vorgehen bestimmen (bestenfalls anhand der detaillierten Sofortmassnahmen SOMA). Wichtig ist, dass die Sofortmassnahmen (SOMA Vorfallreaktionsplan) und die nötigen Kontaktinformationen offline (auf Papier) vorliegen, da bei einem Cyberangriff IT-Ressourcen eventuell nicht mehr verfügbar sind.

Testen Sie die Abläufe und Handlungsanweisungen mit den step by STEP Formularen und Dokumenten bezüglich einem bekannten Fall oder eines eingetretenen Vorfalls. Die im Vorfeld eines Ereignisses erstellten Dokumente dienen als Richtlinie im Ereignisfall. Der Betreiber kann diese im Vorfeld selbst erstellen und zur Vervollständigung diese gemeinsam mit dem Sicherheitsexperten (Cyber) durchführen, situativ mit den Systemlieferanten.

Schritt: Reaktionsplanung (Response Planning)

Erarbeiten Sie einen Reaktionsplan (Formular Sofortmassnahmen SOMA) zur Adressierung erkannter Cybervorfälle. Stellen Sie sicher, dass dieser Reaktionsplan im Ereignisfall korrekt und zeitgerecht ausgeführt wird.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
SOMA Vorfallreaktionsplan verfügbar OT Wurde der Vorfallreaktionsplan (Incident Response Plan) ausgearbeitet? (Dieser muss 'offline' auf Papier verfügbar sein.)			x	(x)		RS.RP-1
SOMA Vorfallreaktionsplan verfügbar IT Wurde der Vorfallreaktionsplan (Incident Response Plan) ausgearbeitet? (Dieser muss 'offline' auf Papier verfügbar sein.)			x		(x)	RS.RP-1

Schritt: Schadensminderung (Mitigation) und Verbesserungen (Improvements)

Handeln Sie so, dass die weitere Ausbreitung eines Cybervorfalls verhindert und der mögliche Schaden verringert wird.

Stellen Sie sicher, dass die Reaktionsfähigkeit Ihrer Organisation auf eingetretene Cyberereignisse laufend verbessert wird, indem die Lehren aus vorangegangenen Vorfällen gezogen werden.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
SOMA Vorfallreaktionsplan OT Beinhaltet der Vorfallreaktionsplan Sofortmassnahmen, mit denen Sie das Ausbreiten des Vorfalls selbständig eingrenzen können?			x	(x)		RS.MI-1
Testen Sie den SOMA Vorfallreaktionsplan OT Wird der Vorfallreaktionsplan regelmässig überprüft, die beschriebenen Vorgehensweisen getestet und der Plan verbessert?			x	(x)		RS.RP-1, RS.IM-2
Reaktionszeiten OT Wurden garantierte Reaktionszeiten mit den System-Lieferanten vereinbart?			x	(x)		RS.CO-3
SOMA Vorfallreaktionsplan IT Beinhaltet der Vorfallreaktionsplan Sofortmassnahmen, mit denen Sie das Ausbreiten des Vorfalls selbständig eingrenzen können?			x		(x)	RS.MI-1
Testen Sie den SOMA Vorfallreaktionsplan IT Wird der Vorfallreaktionsplan regelmässig überprüft, die beschriebenen Vorgehensweisen getestet und der Plan verbessert?			x		(x)	RS.RP-1, RS.IM-2
Reaktionszeiten IT Wurden garantierte Reaktionszeiten mit den System-Lieferanten vereinbart?			x		(x)	RS.CO-3

5.5 Wiederherstellen (Recover)

Nach einem Angriff werden die Daten und Systeme anhand des getesteten Plans wiederhergestellt. Zunächst muss der Zeitpunkt des Angriffs eingegrenzt werden, um die Datenwiederherstellung auf Basis von nicht infizierten Backups zu gewährleisten. Ausserdem gilt es, die Ursache des Vorfalles zu untersuchen, um gezielt Vorkehrungen gegen weitere Angriffe treffen zu können.

Auch hier ist es wichtig, dass der Plan in Papierform vorliegt, da digitale Kopien zu diesem Zeitpunkt eventuell nicht verfügbar sind.

Die Wiederherstellungsphase bezieht sich auf den ganzen Betrieb. Sie ist erst abgeschlossen, wenn dieser wieder normal funktioniert.

Schritt: Wiederherstellungsplanung (Recovery Planning)

Stellen Sie sicher, dass die Wiederherstellungsprozesse so gepflegt und durchgeführt werden (können), dass eine zeitnahe Wiederherstellung der Systeme gewährleistet werden kann.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Log-Dateien OT Können Sie anhand der vorhandenen Log-Dateien den Zeitpunkt des Vorfalls eruieren?			x	(x)		RC.RP-1
Wiederherstellen OT Können Sie nach einem Vorfall alle notwendigen Daten und Systeme anhand eines Wiederherstellungsplanes wiederherstellen (lassen)?			x	(x)		RC.RP-1
Log-Dateien IT Können Sie anhand der vorhandenen Log-Dateien den Zeitpunkt des Vorfalls eruieren?			x		(x)	RC.RP-1
Wiederherstellen IT Können Sie nach einem Vorfall alle notwendigen Daten und Systeme anhand eines Wiederherstellungsplanes wiederherstellen (lassen)?			x		(x)	RC.RP-1

Schritt: Verbesserungen (Improvements)

Stellen Sie sicher, dass Sie Ihre Wiederherstellungsprozesse laufend verbessern, indem Lehren aus vorangegangenen Wiederherstellungen gezogen werden.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Vorfall eruieren OT Können Sie den Grund eines Vorfalles eruieren und endsprechende Verbesserungen bezüglich Schutzmassnahmen, Datensicherung und Reaktionsplan vornehmen?			x	x		RC.IM-1, RC.IM-2
Vorfall eruieren IT Können Sie den Grund eines Vorfalles eruieren und endsprechende Verbesserungen bezüglich Schutzmassnahmen, Datensicherung und Reaktionsplan vornehmen?			x		x	RC.IM-1, RC.IM-2

Schritt: Kommunikation (Communications)

Koordinieren Sie Ihre Wiederherstellungsaktivitäten mit internen und externen Partnern.

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Vorfall OT Haben Sie festgelegt wem (beispielsweise Geschäftsleitung, Behörden, Mitarbeiter) Sie Angaben zum Vorfall mitteilen müssen?			x			RC.CO-1 bis RC.CO-3
Vorfall IT Haben Sie festgelegt wem (beispielsweise Geschäftsleitung, Behörden, Mitarbeiter) Sie Angaben zum Vorfall mitteilen müssen?			x			RC.CO-1 bis RC.CO-3
Anzeige Haben Sie in den Plänen vorgesehen, bei der Polizei und dem Nationalen Zentrum für Cybersicherheit NCSC [10], Anzeige zu erstatten?			x			RC.CO-1 bis RC.CO-3

6 Handlungsanleitung für Benutzer von IT-Systemen

Die folgenden konkreten Handlungsanweisungen dienen als Ergänzung der konzeptuellen Sicherheitsmassnahmen, die in den step by STEP-Checklisten in Kapitel 5 angegeben werden. Sie beziehen sich vor allem auf das Verhalten der Benutzer und veranschaulichen, wo Potential zur Optimierung und zur Erhöhung der Cybersicherheit besteht.

6.1 Grundsätzlich

- Lassen Sie sich weder durch E-Mails, Telefonanrufe noch durch Fehlermeldungen Ihres Computers unter Druck setzen.
- Holen Sie bei Verdacht auf einen Cybersecurity-Vorfall oder Unklarheiten eine Zweitmeinung eines Kollegen oder Ihres IT-Dienstleisters ein.

6.2 Passwort

- Passwörter sind persönlich und dürfen niemals weitergegeben werden. Seriöse Anbieter brauchen das persönliche Passwort nicht um Ihnen zu helfen.
- Nutzen Sie für verschiedene Applikationen und Internetseiten verschiedene Passwörter. So sind Sie sicher, dass beim Ausspähen eines Passwortes nicht alle Dienste kompromittiert werden.
- Nutzen Sie zur Verwaltung von Passwörtern sogenannte Passwortmanager wie KeePass oder LastPass.
- Nutzen Sie lange Passwörter. Idealerweise solche, die aus Buchstaben, Ziffern und Sonderzeichen bestehen. Mit Passwortmanagern können Sie diese automatisch generieren.
- Nutzen Sie bei Internetdiensten die 2-Faktorauthentifizierung, falls diese angeboten wird.

6.3 Internet

- Nutzen Sie ihnen bekannte Anbieter und stellen sie sicher, dass Sie deren Angebote über die offizielle Webseite nutzen. Leider sind nicht alle im Internet angebotenen Dienste seriös.
- Prüfen Sie die Adresse von Links über die Statusleiste Ihres Browsers.
- Melden Sie sich bei Internetdiensten nicht nur mit Benutzername und Passwort an, sondern nutzen Sie wo möglich einen weiteren Faktor (Einmal-Passwort per SMS, Autenticator-App oder Hardware Token)
- Bestellen Sie Software bei Ihrem IT-Verantwortlichen und laden Sie diese nicht selbst aus dem Internet herunter.
- Installieren Sie keine Software eigenständig auf dem Geschäftscomputer. Die Installation sollte aus Sicherheitsgründen immer durch den IT-Verantwortlichen erfolgen.

6.4 E-Mail

- Löschen Sie verdächtige E-Mails. Falls die verdächtige Nachricht von einem bekannten Kontakt gesendet wurde, fragen Sie telefonisch nach. Verdächtig sind E-Mails, wenn:

  – der Inhalt merkwürdig ist: Er verspricht ein zu gutes Angebot? Beim Lesen schleicht sich Misstrauen ein?
  – keine persönliche Anrede vorhanden ist.
  – sie Links zu offiziell aussehenden Seiten zur Dateneingabe (Passwort, Vertrauliches, …) enthält.
  – Sie unerwartete E-Mails mit konkreten persönlichen Informationen erhalten. Diese Informationen können über soziale Netzwerke gesammelt werden. Phishing-E-Mails wirken damit besonders überzeugend.
  – sie Reizwörter enthalten, beispielsweise «Ihre Kreditkartendaten wurden gestohlen».
  – der Text zeitlichen Druck aufbaut (Dringlichkeit).
  – Sie zur Bestätigung Ihres Passwortes aufgefordert werden.
  – Sie Links zu gefälschten Internetseiten enthalten, beispielsweise statt www.google.com www.g00gle.com. Prüfen Sie Links in E-Mails vor dem Klicken, indem Sie mit der Maus über den Link fahren und die dann angezeigte Internetadresse überprüfen.

6.5 Hardware und USB-Sticks, USB-Anschluss

- Schliessen Sie nur vom Unternehmen freigegebene Hardware an Ihren Computer an.
- Prüfen Sie USB-Sticks mit Ihrer Antiviren-Software.
- Prüfen Sie, ob der USB-Anschluss in den Netzwerken geschlossen oder deaktiviert ist.

7 Einzelfallbetrachtung

Die Erfahrungen aus Einzelfällen ermöglichen die Massnahmen laufend anzupassen und Simulationen durchzuführen, um einen Vorfallreaktionsplan zu testen. Jedes Unternehmen kann die Einzelfälle für ihre Verhältnisse abändern und weitere Einzelfälle ergänzen [5].

Die konkreten Massnahmen sind abhängig von der Situation im betreffenden Unternehmen.

7.1 Beispiele für Angriffe

Computervirus

Stuxnet ist ein Computervirus, der 2010 entdeckt wurde, der speziell zum Angriff auf ein System zur Überwachung und Steuerung des Herstellers Siemens (Simatic S7) entwickelt wurde. Die Schadsoftware konnte in isolierte Netze eindringen und modifizierte Bausteine auf ein Steuerungssystem laden, um den Prozess gezielt zu manipulieren und die Anlage zu sabotieren.

Es ist eher unwahrscheinlich, Opfer eines solchen Szenarios zu werden, da der Entwicklungsaufwand ausserordentlich hoch ist. Die rasante Entwicklung in der Cyberkriminalität erhöht jedoch das Risiko eines Angriffs unaufhaltbar.

Ransomware

Ransomware-Angriffe sind weniger dramatisch, jedoch weit verbreitet und können ebenso grossen Schaden anrichten. Dazu kommt, dass staatliche Anlagen ein beliebtes Ziel für Ransomware sind, da sich die Angreifer eine grössere Chance auf die Bezahlung von Lösegeld erhoffen.

Es liegt auf der Hand, dass als erstes der Schutz gegen weitverbreitete und einfach zu verhindernde Angriffe erhöht werden sollte, bevor man sich mit gezielten, technisch fortgeschrittenen Angriffen befasst.

In den nachfolgenden Kapiteln sind einige weitere Beispiele beschrieben. In der Regel basieren diese immer auf einer Kombination von Gründen, Angriffsvektor und Folgen.

7.2 Befall durch Ransomware mittels USB-Stick oder E-Mail

Situation

- Verschlüsseln der Büro-Computer, Pikett-Notebooks, Leittechnikstationen oder Server
- Gelderpressung

Folgen

Eine Verschlüsselung aller Daten kann die Bedienbarkeit des Leitsystems einschränken oder diese sogar verunmöglichen. Solange die Steuerungen nicht betroffen sind, sollte die Anlage jedoch funktionstüchtig bleiben.

Erkennung

Ein Ransomware-Angriff kann durch moderne Endpoint-Protection-Systeme erkannt werden. Anzeichen eines Angriffs können auch die Beeinträchtigung der Funktionalität des Leitsystems (oder anderer Software), eine Änderung der Fileendungen (z. B. CRYPTED) oder ein Erpresserbrief sein.

Massnahmen bei Cybervorfall

OT-Massnahmen	IT-Massnahmen
Zuständige Person(en) informieren.	Zuständige Person(en) informieren.
Maschine physisch vom Netzwerk trennen (Netzwerk-Stecker ziehen). **Achtung: nicht Stromkabel ziehen!**	Maschine physisch vom Computer-Netzwerk trennen (WLAN-Verbindung, Netzwerk-Stecker ziehen). **Achtung: nicht Stromkabel ziehen!**
Netzwerk-Stecker des betroffenen Segmentes beim Haupt-Switch/der Firewall ziehen, damit das betroffene Segment keinen Zugriff mehr auf den Rest der Anlage hat.	Netzwerk-Stecker des betroffenen Segmentes beim Haupt-Switch/der Firewall ziehen, damit das betroffene Segment keinen Zugriff mehr auf den Rest des Systems hat.
Korrektes Funktionieren der kritischen Aufgaben der Unternehmung visuell prüfen (dem Leitsystem kann zu diesem Zeitpunkt nicht mehr vertraut werden).	Keine Anmerkungen.
Anweisungen der zuständigen Person(en) befolgen.	Anweisungen der zuständigen Person(en) befolgen.

Massnahmen die im Einverständnis mit der zuständigen Person getätigt werden können:

- Eine Kopie mindestens einer Maschine zur Analyse erstellen.
- Maschinen neu aufsetzen.
- Wiederherstellung der Daten von Back-ups, oder, falls nicht möglich, überprüfen, ob ein Schlüssel für diese Variante von Ransomware vorhanden ist, z. B. auf www.nomoreransom.org
- Eruieren der Ursache des Befalls (z.B. Mithilfe der Logs) und Anpassung des Sicherheitskonzeptes, um solche Fälle in Zukunft zu vermeiden.

Prävention

- Die Benutzung von USB-Laufwerken sollte, falls betriebstechnisch möglich, unterbunden werden («Least Privilege»). Zudem sollte die Prozessor-Last überwacht werden, um ein schnelles Erkennen eines Angriffs zu ermöglichen.
- Es sollten regelmässige Backups der Anlage oder zumindest der betriebskritischen Daten, gemacht werden.
- Schutzsoftware welche die Verschlüsselung erkennt und blockiert sollte installiert und genutzt werden.

7.3 Botnet-Infizierung durch 'verseuchte' Software

Situation

- Missbrauch des Netzwerkes oder der Rechenleistung als Teil eines Botnets
- Infizierung anderer IT-Geräte

Folgen

Ausser dem Missbrauch (und der evtl. Nichtverfügbarkeit) von Netzwerk- oder Prozessor-Last der betroffenen Systeme, kann ein solcher Angriff auch zur Folge haben, dass der Internet-Provider die Internetverbindung der Anlage kappt, da er die Anlage als schädliches System sieht. Ebenfalls können Ordnungskräfte die Anlage (fälschlicherweise) als Ausgangspunkt eines Angriffs sehen, was zu Fehleinsätzen und den damit verbundenen Betriebsstörungen führen kann.

Erkennung

Infektionen durch Botnets können durch erhöhte CPU- und/oder Netzwerklast, sowie Verbindungen auf bekannte «Command and Control»-Domänen erkannt werden. Diese werden von den Angreifern benötigt, um Befehle an die infizierten Systeme («Bots») zu schicken.

Massnahmen die im Einverständnis mit der zuständigen Person getätigt werden können:

- Eine Kopie mindestens einer Maschine zur Analyse erstellen.
- Maschine neu aufsetzen.
- Eruieren der Ursache des Befalls (z. B. Mithilfe der Logs) und Anpassung des Sicherheitskonzeptes, um solche Fälle in Zukunft zu vermeiden.

Prävention

Software sollte nur von vertrauenswürdigen Quellen bezogen werden.

Das Netzwerk sollte in verschiedene, betriebsrelevante Segmente unterteilt sein, was die Verbreitung solcher Infektionen eindämmen und den daraus resultierenden Schaden minimieren kann.

Benutzer sollten nur mit minimalen Rechten ausgestattet werden, was die erfolgreiche Installation des Botnet-Trojaners erschwert.

Netzwerk- und Prozessor-Last sollten überwacht werden, um eine schnelle Erkennung des Angriffs zu ermöglichen.

7.4 Manipulation der Prozessdaten

Situation

- Falsche Prozesswerte auf dem Leitsystem
- Falsches Verhalten der Automationsprozesse
- Manipulation oder «ausser Gefecht» setzen der Steuerung.

Folgen

Abhängig vom Ausmass des Angriffs kann dieser kleine Störungen bis hin zu grossen Schäden verursachen. In Bezug auf den Hardwareschaden sollte jedoch das System durch entsprechende Hardwareverriegelungen geschützt sein.

Die Definition der Hardwareverriegelungen erfolgt in der Regel während dem Engineering des Prozesses im Rahmen der Risikoanalyse.

Erkennung

Die Erkennung kann schwierig sein, da der Grund der nicht logischen (inkohärenten) Daten mehrere Ursachen haben kann (Fehlfunktion der Sensoren, Fehler bei der Datenübertragung, Fehler bei der Datenverarbeitung, etc.). Mitarbeiter, die ein «Gefühl» für die Anlage haben, sind in solchen Fällen sehr wertvoll.

Da diese Art von Angriff ein sehr spezialisiertes Know-How benötigt, kann davon ausgegangen werden, dass es sich um einen gezielten Angriff handelt. Daher sollte auch die Melde- und Analysestelle Informationssicherung MELANI informiert werden [9].

Ist der Angriff einmal bewältigt, gilt es die Ursache des Befalls zu eruieren (z. B. Mithilfe der Logs) und das Sicherheitskonzept anzupassen, um solche Fälle in Zukunft zu vermeiden, oder zumindest schneller zu erkennen.

Prävention

Da die Art des Angriffs auf einen kompetenten, gut organisierten Angreifer hindeutet, ist es sehr schwierig, sich vor solchen Angriffen zu schützen.

7.5 Diebstahl und Betrug

Situation

Manipulation durch «Social Engineering»: Durch eine geschickt formulierte Nachricht (per Phishing-Mail oder telefonisch) wird das Opfer dazu gebracht, persönliche Daten preiszugeben oder Geld zu überweisen.

Folgen

Je nach Stellung des Opfers in der Hierarchie des Unternehmens und je nach Geschick des Täters, wird das Opfer dazu gebracht, einen hohen Geldbetrag an die Täter zu überweisen. Dazu werden dem Opfer falsche Tatsachen vorgetäuscht. Die Täter nutzen oft fremde Identitäten, beispielsweise durch Fälschen von Telefonnummern und Mailadressen.

Erkennung

Die Erkennung ist schwierig. Das Opfer wird zeitlich unter Druck gesetzt und angewiesen, die Aktion aus geschäftlichen Gründen vertraulich zu behandeln.

Massnahmen bei Vorfall

IT-Massnahmen
Zuständige Person(en) informieren.
Die Institution (Bank, Lieferant, etc.), die für die Überweisung zuständig ist, informieren und dazu bewegen, die Überweisung zu blockieren oder rückgängig zu machen. Bei der Polizei und dem Nationalen Zentrum für Cybersicherheit NCSC [10] Anzeige erstatten.

Prävention

Identifizieren Sie Geschäftspartner und Auftraggeber eindeutig, im Zweifelsfall über einen anderen Kanal als der Auftrag eingegangen ist. Lassen Sie sich durch Nachrichten nicht unter Druck setzen. Besprechen Sie verdächtige Situationen mit Kollegen.

Gegen Social Engineering hilft ein offenes, transparentes Klima und geschulte Mitarbeiter.

8 Schlussfolgerungen

Mit dem Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie in Abwasserbetrieben können die Akteure der Abwasserbetriebe die Widerstandsfähigkeit (Resilienz) ihrer IKT-abhängigen Prozesse stärken. Dazu stehen ihnen ein Fragebogen zur Selbsteinschätzung und Vorlagen für die IST-Analyse, wie für die Risikobeurteilung und Umsetzung zur Verfügung [5].

Mit den Formularen und der Vorlage «Individuelle Einzelfälle» von step by STEP und dessen Handbuch ist es dem Betreiber möglich, umfangreiche Handlungsanweisungen zu Ereignissen zu definieren, genannt Vorfallreaktionspläne. Der IKT-Minimalstandard Abwasser dient den Akteuren zur eigenen Reflektion hinsichtlich Cybersicherheit. Dieser Standard ermöglicht den Abwasserbetrieben mögliche Mängel bereits im Vorfeld eines Audits/Assessments zu erkennen und erleichtert die detaillierte Analyse sowie die allfällige Budgetierung der zu ergreifenden Massnahmen.

Die Verantwortung für die Cybersicherheit bleibt stets beim Betreiber. Er definiert seine Risikobereitschaft, veranlasst Massnahmen zur Verminderung von Risiken und setzt Prioritäten. Der IKT-Minimalstandard Abwasser soll diesen Prozess anstossen und bei der Umsetzung helfen. **Die Cybersicherheit ist kein Zustand sondern ein ständiger Prozess. Als erster Schritt dient der Fragebogen zur Selbsteinschätzung in Kapitel 5.**

Mit der praktischen Anwendung und im Austausch mit andern Betreibern kann die Cybersicherheit bereits mit relativ einfachen Massnahmen deutlich gestärkt werden.

Glossar

Begriff	Bedeutung
Awareness	Wissen und die Achtsamkeit Ihrer Mitarbeiter im Umgang mit OT- und IT-Lösungen zur Reduzierung von Sicherheitsrisiken.
Botnet	Botnetz ist eine Gruppe automatisierter Schadprogramme, sogenannter Bots.
BWL	Bundesamt für wirtschaftliche Landesversorgung
Sicherheitsexperte	Weisen ihr Können und Fachwissen durch Zertifizierungen nach, Bsp. Certified Informations Systems Auditor (CISA). Dies verlangt eine stetige Weiterbildung.
Defense-in-Depth	Koordinierter Einsatz mehrerer Sicherheitsmassnahmen, um die IKT-Betriebsmittel in einem Unternehmen zu schützen.
GRESE	Groupement Romand des Exploitants de Stations d'Epuration
IKT-Infrastruktur	Sämtliche Elemente der Informations- und Telekommunikationsausrüstung wie: Desktop-PC's, Mobiltelefone, Tablets, Überwachungskameras etc.
IoT-Devices	Das Internet der Dinge. Innovations- und Einkaufsführer für IoT-Geräte
Kritikalität	Bedeutung einer Ressource, bei deren Wegfall eine existentielle Gefährdung vorhanden wäre.
PLS	Prozessleitsystem dient zum Führen einer verfahrenstechnischen Anlage, wie Kläranlage.
Ransomware	Schadprogramme (wie: Erpressungstrojaner, Erpressungssoftware)
Resilienz	Widerstandsfähigkeit, dass die Anlage bei einem Teilausfall von verschiedenen IKT-Systemen nicht vollständig versagt.
STEP	Abkürzung von: Stations d'Epuration (Kläranlage)
VSA/FES	Verband Schweizer Abwasser- und Gewässerschutzfachleute und die Groupe romand pour la formation des exploitants de stations d'épuration (FES)
Vorfallreaktionsplan	Sofortmassnahmen SOMA um eine Infektion wirkungsvoll einzudämmen. Vorlagen: Einsatzformulare im Handbuch step by STEP.

Autoren und Fachexperten

Vorname, Name	Firma/Funktion
Max Schachtler	step by STEP, Projektleitung, Hauptautor
Melchior Zimmermann	Chestonag Automation AG, Hauptautor
Lukas Studer	first frame networkers ag, Co-Autor
Reto Steinemann	Chestonag Automation AG, Co-Autor
Daniel Caduff	BWL, Fachexperte
Sven Peter	BWL, Fachexperte
Daniel Bader	Chestonag Automation AG, Netzwerk-Fachexperte
Rolf Roppel	Klein Computer System AG, IT-Fachexperte
Marin Roje	Klein Computer System AG, IT-Fachexperte
Peter Bruderer	Chestonag Automation AG, OT-Fachexperte
Alfred Schaufler	emsrplan AG, OT-Fachexperte
Dominik Landolt	e.e.com elektroanlagen ag, OT-Fachexperte

Haftungsausschluss

Das vorliegende Dokument mit Empfehlungen zur Verbesserung der Sicherheit von Informations- und Kommunikationssystemen der Abwasserbetriebe wurde von den beteiligten Personen, Stellen und step by STEP nach bestem Wissen und Gewissen erstellt. Es wird keine Gewährleistung, weder ausdrücklich noch implizit übernommen. Dies trifft auch auf die involvierten Fachexperten, Unternehmen und Mitarbeitenden zu. Die Verantwortung für den sicheren Betrieb der IKT sowie die Haftung für mögliche Schäden liegt einzig beim Anwender.

Chronologie

Datum	Kurzbeschreibung
September 2018	Arbeitsaufnahme IKT-Minimalstandard Abwasser
Dezember 2018	Erarbeitung und Besprechung Entwurf 0.1 AG
Februar 2019	Besprechung Entwurf 0.2 AG
April 2019	Besprechung Entwurf 0.3 AG
Mai 2019	Besprechung Entwurf 0.4 mit BWL
Juni 2019	IKT-Minimalstandard Abwasser Erstausgabe in step by STEP
August 2019	Erstellen IKT-Minimalstandard Abwasser als Einzeldokument
September 2019	Konsultation der Fachexperten
Oktober 2019	Tagesseminar Branchenstandard IKT-Minimalstandard Abwasser Einführung und Umsetzung in Abwasserbetrieben
Oktober 2019	Veröffentlichung IKT-Minimalstandard Abwasser
Dezember 2020	IKT-Minimalstandard Abwasser durch VSA/FES genehmigt
März 2021	IKT-Minimalstandard Abwasser aktualisiert

Literaturverzeichnis

[1] Bundesamt für wirtschaftliche Landesversorgung BWL; «Minimalstandard zur Verbesserung der IKT-Resilienz», Bern, 2018

[2] step by STEP; «In Abwasserbetrieben der Ereignisschutz», Dübendorf, 2019, https://step-ara.ch

[3] https://www.isaca.ch/de/weiterbildung/ausbildung.html

[4] Bundesamt für wirtschaftliche Landesversorgung BWL; «IKT-Minimalstandard-Assessment Tools», Bern, 2018

[5] step by STEP; «IKT-Minimalstandard-Umsetzung Tools», Dübendorf, 2019, https://step-ara.ch

[6] https://www.nist.gov/cyberframework

[7] https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/berichte/fachberichte/technical-report_apt_case_ruag.html

[8] https://haveibeenpwned.com/DomainSearch

[9] https://www.ncsc.admin.ch/ncsc/de/home/cyberbedrohungen.html

[10] https://www.report.ncsc.admin.ch/de/

Impressum und Kontakt

Herausgeber
step by STEP – in Abwasserbetrieben der Ereignisschutz
step-ara.ch

Ihre Notizen