# CYBERSICHERHEIT BEI ABWASSERBETRIEBEN

## WIE KLÄRANLAGEN DEN IKT-MINIMALSTANDARD ABWASSER UMSETZEN KÖNNEN

**Die Digitalisierung hat in der Abwasserbranche Einzug gehalten: Die dazu verwendeten Computer sind heute vernetzt und die Betriebsprozesse von überall auf der Welt steuerbar. Diese Vorteile nutzen nicht nur die Mitarbeitenden der Abwasserreinigungsanlagen, sondern auch Geschäftsführer von Weltkonzernen, Betriebsleiter von mittleren Produktionsbetrieben, aber auch die organisierte Kriminalität. In diesem Artikel erfahren ARA-Betreiber, wie sie ihre Anlagen schützen können.**

*Lukas Studer*, first frame networkers ag*
*Max Schachtler, step by STEP*
*Melchior Zimmermann, Chestonag Automation AG*

## RÉSUMÉ

### LES EXPLOITANTS DES STEP ET LA CYBERSÉCURITÉ

Pour les entreprises de traitement des eaux usées, le futur ne s'est pas fait attendre. Leur fonctionnement s'effectue de manière automatisée et elles peuvent être commandées à partir de n'importe quel endroit sur la planète. Le niveau élevé d'automatisation, la mise en réseau que ce dernier nécessite ainsi que l'indépendance géographique des collaborateurs et fournisseurs entraînent de nouveaux risques. Ces cyberrisques mettent en danger les processus opérationnels ainsi que l'environnement et doivent donc être identifiés et réduits à un niveau acceptable. C'est à l'exploitant qu'incombe la responsabilité de gérer ces cyberrisques. À cet égard, le standard minimum TIC pour les eaux usées représente une approche adaptée de la situation. La liste de contrôle pour l'auto-évaluation aide à identifier les risques et à mettre en œuvre un processus de cybersécurité. Ce dernier comporte cinq fonctions comprenant toutes les étapes nécessaires allant de l'identification des valeurs et méthodes, leur protection, l'identification des incidents et la manière d'y réagir jusqu'au rétablissement des processus opérationnels.

Les experts en cybersécurité offrent une assistance efficace en matière de cybersécurité. Cependant, il est également nécessaire de responsabiliser les fournisseurs, les prestataires et les utilisa-

> S. 51

## WAS IST CYBERSICHERHEIT UND WESHALB NIMMT IHRE BEDEUTUNG ZU?

Noch vor wenigen Jahren konnte die Zukunft in sogenannten «Future-Häusern» bestaunt werden. Diese zeichneten sich durch die Vernetzung der Haustechnik und den darin verbauten Haushaltsgeräten aus. Rollläden, Heizung, Licht, alles konnte dank Vernetzung und mobiler Steuergeräte von jedem Punkt im Haus aus gesteuert werden. In Wohnhäusern hat sich diese Technologie noch nicht durchgesetzt. In Kläranlagen sind ähnliche Technologien heute meistens Stand der Technik: Sie werden zur Überwachung und Steuerung von Produktionsprozessen eingesetzt. Die Kläranlagenverantwortlichen sind heute in der Lage, die gesamten Anlagenteile von zu Hause oder ab einem anderen Ort aus zu steuern *(Fig. 1)*.

Ein Klick aufs Tablet und die Schneckenpumpe des Einlaufhebewerks ist gestoppt. Ein anderer Klick und ein Regenbecken wird entleert. Heutzutage geht alles ganz einfach und es läuft immer perfekt. Immer?

Neue Möglichkeiten bergen immer auch neue Risiken. Besteht ein Fernzugriff auf eine Anlage, um den Mitarbeitenden die Arbeit von überall aus der Welt zu ermöglichen, bedingt dies, dass

** Kontakt: lukas.studer@firstframe.net*

auch Angreifer von überall aus der Welt versuchen können, diesen Fernzugriff zu missbrauchen.
IKT-Systeme (Informations- und Kommunikations-Technologie, z. B. Steuerungen, PC, Drucker usw.) sind nie zu 100% sicher. Cybersicherheit hat deswegen nicht zum Ziel, eine Anlage zu 100% sicher zu machen, da dies nicht möglich ist. Vielmehr geht es darum, die Risiken der eingesetzten Betriebsmittel und Technologien zu kennen und diese auf ein für den Betrieb verantwortbares Niveau zu senken (z. B. mit Schutz-Technologien wie Anti-Virus, Firewall usw.).
In traditionellen IT-Umgebungen (z. B. Büro) sind diese Risiken oft nur auf Daten bezogen. Geschäfts-Strategie, geistiges Eigentum, Kundendaten usw. müssen vor Zerstörung, Diebstahl und Manipulation ausreichend geschützt sein. Durch die in den letzten Jahren erfolgte Automatisation und Vernetzung der Kläranlagen (OT-Umgebung) beschränken sich diese Risiken heute leider nicht mehr rein auf die digitale Welt der IT-Umgebung.
Hacker-Angriffe haben zunehmend physische Auswirkungen [1], deren Konsequenzen oft nicht nur finanzieller Natur sind. Entsprechend muss der Betreiber von Kläranlagen die Risikoanalyse anpassen, um die physischen und digitalen Konsequenzen eines Ausfalls oder einer Störung von IKT-Betriebsmitteln möglichst zu verhindern.

## SICHERHEIT: DER UMGANG MIT RISIKEN

Wir fühlen uns sicher, wenn es keine für uns unvertretbaren Risiken mehr gibt. Doch wie kann man feststellen, welche Risiken existieren und wie man mit unvertretbaren Risiken umgeht?

### RISIKEN

Für den Begriff Risiko gibt es verschiedene Definitionen. Die bekannteste dürfte die Gleichung «Risiko = Eintretenswahrscheinlichkeit mal Schadenhöhe» sein. Leider ist diese Formel in der Praxis kaum anwendbar: Die Schadenhöhe lässt sich zwar in einigen Fällen berechnen, jedoch unterscheidet sich die Eintretenswahrscheinlichkeit je nach Anlage und ist aufgrund der geringen Anzahl Erfahrungswerte individuell zu bestimmen.
In der Cybersicherheit werden Risiken daher mit einer, auf den ersten Blick, komplizierteren Methode ermittelt. Dabei definiert sich das Risiko aus einem für den Betriebsprozess – hinsichtlich Informationsverarbeitung – wichtigen Wert und einem Gefahrenszenario, welches auf diesen Wert einwirkt *(Fig. 2)*.
Das Gefahrenszenario wird aus Bedrohung und Verwundbarkeit abgeleitet. Existiert für eine Bedrohung keine Verwundbarkeit auf der Anlage, ergibt sich daraus auch kein Gefahrenszenario.
Die Höhe des Risikos wird durch den Wert und das Gefahrenszenario beeinflusst. Mittels entsprechender Massnahmen lässt sich die Auswirkung auf ein für die Kläranlage akzeptables Mass reduzieren.

### RISIKOIDENTIFIKATION

Zur Risikoidentifikation bei Kläranlagen können Analysen verschiedener Bundesämter zur kritischen Infrastruktur und zu Industriesteuerungen herangezogen werden. Das Bundesamt für Bevölkerungsschutz schätzt in seinem Factsheet zum kritischen Teilsektor Abwasser [2] die Auswirkung einer Störung, den Ausfall oder die Zerstörung der Abwasserentsorgung als «gross» ein und sieht Folgen für die Bevölkerung, die Wirtschaft sowie

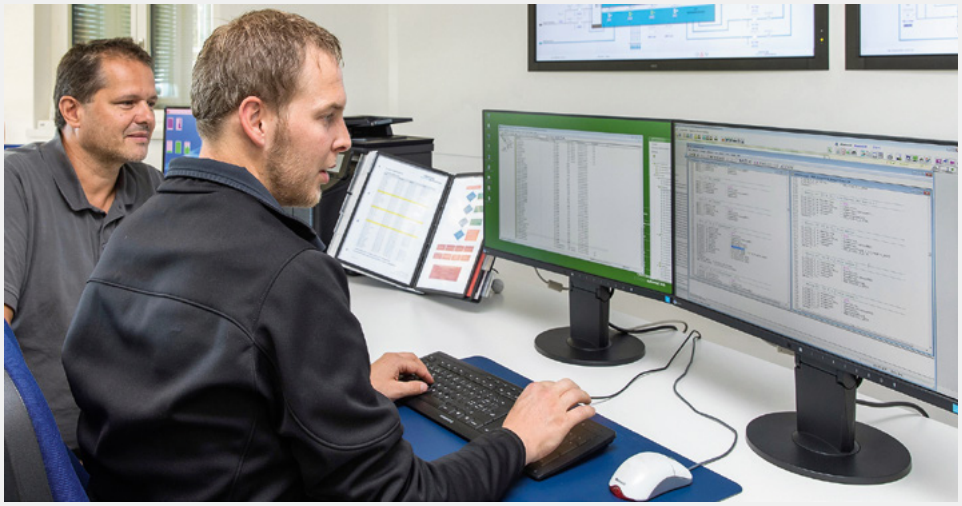

*Fig. 1 Ohne informatikgestützte Automation ist der Betrieb einer Kläranlage heute nicht mehr aufrechtzuerhalten.* *(Bild: Chestonag Automation AG)*

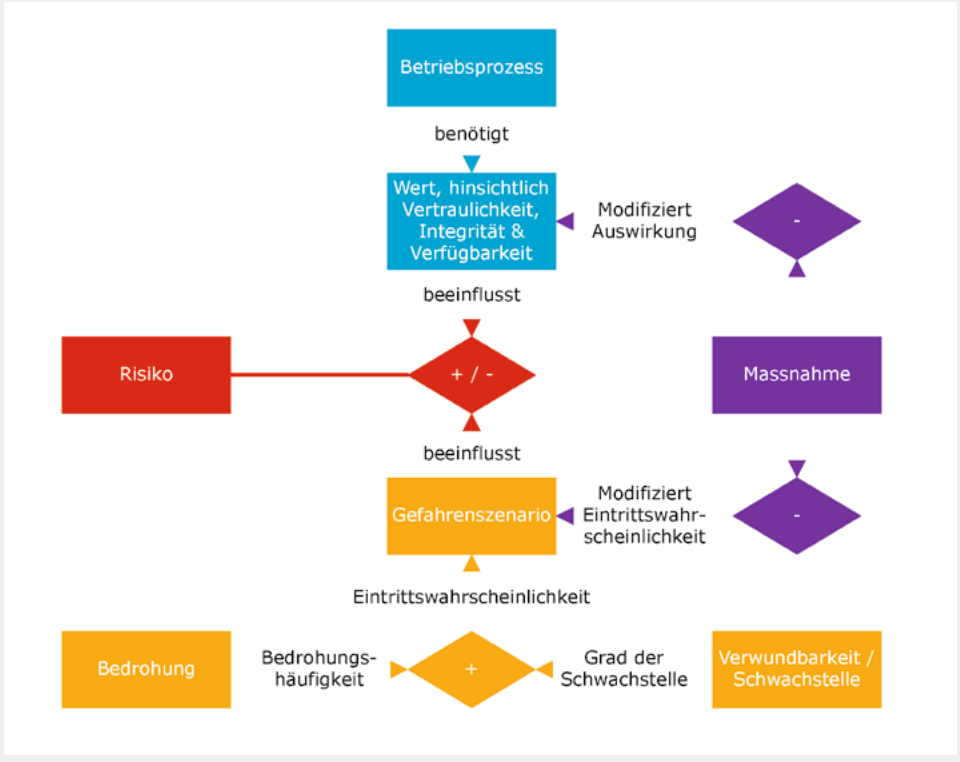


*Fig. 2 Einflussfaktoren auf Cyberrisiken.* *(Quelle: first frame networkers ag)*

andere kritische Infrastrukturen. Cyberrisiken können zu einer Störung oder zum Ausfall der Anlage führen und müssen identifiziert und nach Möglichkeit minimiert werden.
Der erste Schritt der Risikoidentifikation liegt darin, zu erkennen, welche Prozesse durch Cybervorfälle verwundbar sind.

### VERWUNDBARKEIT IN PROZESSEN DER ABWASSERREINIGUNG

Das Bundesamt für wirtschaftliche Landesversorgung BWL hat im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) die Verwundbarkeit von Abwasserreinigungsprozessen beurteilt [3]. Es hat die Prozessphasen Rechenanlage, Öl- und Sandfang, Vorklärung, biologische Reinigung und Filtration sowie die übergreifenden Kommunikations- und Steuerungsprozesse betrachtet und kam zum Schluss, dass die Steuerungsprozesse am verwundbarsten sind. Anhand einer Bedrohungsanalyse lässt sich nun klären, welche Gefahrenszenarien auf der Anlage bestehen.

### BEDROHUNGEN FÜR KLÄRANLAGEN-STEUERUNGEN

Ein Katalog mit Bedrohungen für Industriesteuerungen liefert das deutsche Bundesamt für Sicherheit in der Informationstechnik. Diese lassen sich problemlos auf Steuerungen in Kläranlagen übertragen. Es sieht folgende Bedrohungen als relevant an [4]:

- Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
- Infektion mit Schadsoftware über Internet und Intranet
- Kompromittierung von Extranet und Cloud-Komponenten
- Social Engineering und Phishing
- (D)DoS-Angriffe (Angriff auf die Systemerreichbarkeit über das Internet)
- Internetverbundene Steuerungskomponenten
- Einbruch über Fernwartungszugänge
- technisches Fehlverhalten und höhere Gewalt
- Kompromittierung von Smartphones im Produktionsumfeld

Werden z. B. auf einer Kläranlage keine USB-Sticks oder andere Wechseldatenträger genutzt, besteht diese Bedrohung nicht, es gibt also auch kein gültiges Gefahrenszenario. Ist die Nutzung aber erlaubt und technisch möglich, gilt es abzuschätzen, wie durch deren Nutzung Schadsoftware eingeschleust werden könnte. Dies hängt stark von den mit USB-Sticks ausgeführten Datenübertragungen ab und ist daher anlagenspezifisch. Bei andern Bedrohungsszenarien wie Drittzugriffen usw. sind die Fragestellungen ähnlich.
Natürlich ist obige Liste nicht abschliessend. Anhand des Inventars der zu schützenden Werte lassen sich allenfalls weitere Bedrohungen mit der Frage «Was kann passieren, wenn ich XY damit anstelle?» individuell für jede Anlage ermitteln. Hier hilft es, sich in mögliche Täter hineinzuversetzen, oder einen Cybersicherheits-Experten beizuziehen, der diese Rolle übernimmt.

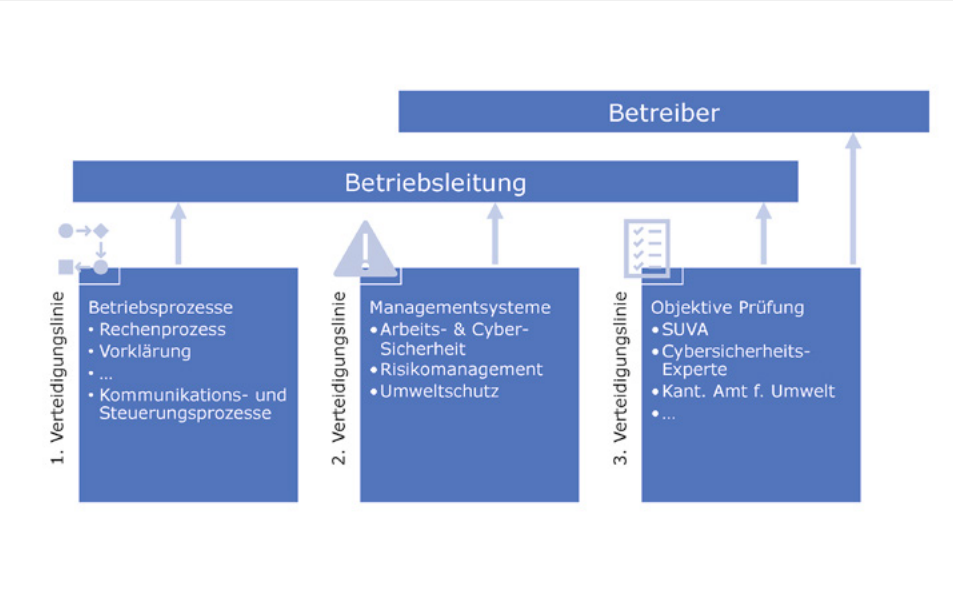


*Fig. 3 Adaption des Modells der drei Verteidigungslinien für Kläranlagen. (Quelle: first frame networkers ag)*

### RISIKOBEWÄLTIGUNG

Am Beispiel Strassenverkehr lässt sich anschaulich aufzeigen, wie Risiken vermieden oder bewältigt werden können:

- Indem die Strasse für bestimmte Verkehrsteilnehmer gesperrt wird.
- Sie lassen sich reduzieren, etwa durch das Tragen heller Kleidung.
- Sie lassen sich übertragen, beispielsweise an eine Unfallversicherung.
- Man kann ein Risiko tragen – durch bewusste Entscheidung wird es als vertretbares Risiko betrachtet und eingegangen.

Dieses Vorgehen lässt sich auch auf Kläranlagen übertragen. Die Bewältigungsstrategie richtet sich oft nach der Höhe des zu schützenden Wertes (beispielsweise Prozess, Objekt oder Anlageteil) und den Kosten, welche für Schutzmassnahmen anfallen. Schutzmassnahmen, die teurer als der zu schützende Wert sind, sind wirtschaftlich nicht sinnvoll. Allerdings können trotzdem Massnahmen, beispielsweise aufgrund gesetzlicher Vorgaben, notwendig sein.

## VERANTWORTLICHKEITEN

Wer ist für die Cybersicherheit und das Risikomanagement verantwortlich? Die Verantwortlichkeiten lassen sich aus dem Modell der drei Verteidigungslinien (bekannt als: *three lines of defense model*) ableiten *(Fig. 3)*. Dieses Modell ist oft in grossen Unternehmen anzutreffen, es lässt sich aber auch auf Kläranlagen und kleinste Organisationen transformieren.
Die erste Verteidigungslinie bilden die Betriebsprozesse. Die Prozesse sollten so gestaltet und umsetzbar sein, dass möglichst wenige Risiken entstehen. Die zweite Verteidigungslinie bildet das Risikomanagement-System, das neue Risiken erkennt und einschätzt und nicht tragbare Risiken mittels entsprechender Massnahmen vermeidet. Die dritte Verteidigungslinie bildet die objektiven Prüfungen, welche die Wirksamkeit der Risikomanagementmethode und der eingesetzten Massnahmen überwachen.
Die zweite und dritte Verteidigungslinie gibt dem Betreiber Auskunft über die Risikolage und die Wirksamkeitsnachweise ermöglichen ihm seine Verantwortung wahrzunehmen. Alle drei Verteidigungslinien sind notwendig, damit die Anlagenverantwortlichen auf Änderungen

an der Risikolage angemessen reagieren können. In Kläranlagen werden diese drei Verteidigungslinien oft direkt durch die Betriebsleitung wahrgenommen.

### VERANTWORTUNG DES BETREIBERS

Die Gewässerschutzverordnung (GSchV) [5] verordnet in Art. 16 und 17 Massnahmen im Hinblick auf ausserordentliche Ereignisse: *«Die Inhaber von Abwasserreinigungsanlagen, die Abwasser in ein Gewässer einleiten, und die Inhaber von Betrieben, die Industrieabwasser in eine Abwasserreinigungsanlage ableiten, müssen zur Verminderung des Risikos einer Gewässerverunreinigung durch ausserordentliche Ereignisse die geeigneten und wirtschaftlich tragbaren Massnahmen treffen.»*

Da ausserordentliche Ereignisse auch aufgrund von Cyberrisiken entstehen können, ist klar, dass diese vom Betreiber beachtet werden müssen. Dieser muss definieren, wie der Betrieb mit Cyberrisiken umgehen soll. Er muss auch nachweisen können, dass er den Umgang mit Risiken angemessen überwacht. Typischerweise regelt er den erwarteten Umgang mit Cyberrisken mittels Schulung der Mitarbeitenden und in den Verträgen mit Dienstleistern, Dritten und Lieferanten.

Dazu legt er fest, welche Tätigkeiten im Riskmanagement von wem durchgeführt werden und unter welchen Bedingungen Risiken nicht mehr tragbar sind. Zusätzlich legt er minimale Verhaltensweisen und Massnahmen zum Schutz der Betriebsprozesse fest.

Der Kläranlagenbetreiber darf Aufgaben an die Betriebsleitung delegieren. Der IKT-Minimalstandard Abwasser *(Fig. 4)* hilft dem Betriebsleiter die Organisation wie die Basis für den Ablauf der Beurteilung des Cyberrisikos anzugehen [6]. Für die weiteren Schritte kann er einen unabhängigen Cybersicherheits-Experten beiziehen.

### VERANTWORTUNG DER BETRIEBSLEITUNG

Welche Aufgaben die Betriebsleitung übernimmt, muss für jede Kläranlage und von jedem Betreiber definiert werden. Typischerweise sind dies die Identifikation und Beurteilung von Risiken und die Überwachung der Sicherheitsmassnahmen. Die Betriebsleitung berichtet dem Betreiber periodisch, wie die Aufgaben ausgeführt werden, welche Risiken aktuell bestehen und wie der Stand der Massnahmenumsetzung ist.

In der Rolle des Vorgesetzten gewährleistet die Betriebsleitung die Cybersicherheit durch Umsetzung und Kontrolle von Massnahmen und ein der Cybersicherheit zuträgliches Arbeitsklima. Dieses sollte sich auch durch einen offenen Umgang mit Risiken und Fehlern und angemessener Arbeitszeit zum überlegten Handeln auszeichnen.

Die Gesamtverantwortung ist nicht delegierbar, sie verbleibt beim Betreiber.

### VERANTWORTUNG DER MITARBEITENDEN

Die Mitarbeitenden haben eine wichtige Rolle, um die Cybersicherheit zu gewährleisten. Sie arbeiten gewissenhaft und schützen die bearbeiteten Daten und Informationen gemäss den Vorgaben. Ausserdem unterstützen sie ihre Kollegen und melden Unregelmässigkeiten, Vorkommnisse und Missgeschicke. Die Aufrechterhaltung eines solchen gewissenhaften Arbeitsklimas ist das Fundament einer guten Cybersicherheit.

### VERANTWORTUNG DRITTER BEI FERNZUGRIFF

Lieferanten und Dienstleister oder Gemeindemitarbeitende von OT- und IT-Systemen oder vernetzten Komponenten, wie z. B. Regenbecken, verfügen teilweise über Fernzugriffsmöglichkeiten, um Systeme zu optimieren oder Fehler zu beheben oder zur reinen visuellen Übersicht. Diese privilegierten Zugriffsmöglichkeiten nutzen Angreifer vermehrt, um über deren Netzwerke und Computer Zugriff auf die Systeme der Kläranlage zu erlangen [7]. Deswegen ist es für die Cybersicherheit zentral, dass die zugriffsberechtigten Personen sich ihrer Mitverantwortung bezüglich der Sicherheit ihrer Kunden bewusst sind und diese wahrnehmen. Der Kläranlagenbetreiber lässt im optimalen Fall keine Drittzugriffe zu oder regelt den Fernzugriff Dritter vertraglich und beschränkt diese mit geeigneten Massnahmen.

## DER CYBERSICHERHEITS-EXPERTE

Der Cybersicherheits-Experte unterstützt den Betriebsleiter mit spezifischem Fachwissen und ist das Bindeglied zwischen den weiteren Beteiligten (OT und IT, Verfahrens- und Elektroplaner usw.). Er koordiniert und steuert den Informationssicherheitsprozess, empfiehlt und verfasst Richtlinien zum Umgang mit Informationen und kann Leitungspersonen, Mitarbeitende und Dienstleister sensibilisieren und schulen. Auch die Prüfung der


*Fig. 4 IKT-Minimalstandard Abwasser [6]*

Wirksamkeit von implementierten Massnahmen gehört zum Aufgabengebiet des Cybersicherheits-Experten.

Um diese Aufgaben erfüllen zu können, muss er über entsprechende Ausbildungen verfügen und sich kontinuierlich weiterbilden. Kläranlagen erteilen diese Aufgabe typischerweise an einen externen Spezialisten. Diese Spezialisten weisen ihre Fähigkeit mit Zertifizierungen wie jener zum *Certified Information Systems Auditor* (CISA) [8] nach.

Der Cybersicherheits-Experte als Bindeglied im Cybersicherheitsprozess und zwischen allen Beteiligten schlägt ein zielführendes Vorgehen vor, vermittelt zwischen den Rollen, informiert die Beteiligten über Bedrohungen und mögliche Schutzmassnahmen und kontrolliert diese. Die Beteiligten geben Informationen an den Cybersicherheits-Experten weiter und der Betriebsleiter veranlasst die Planer zur fachgerechten Umsetzung der von ihm beschlossenen Massnahmen.

## CYBERSICHERHEIT – EIN KONTINUIERLICHER PROZESS

IKT ist ein breites Feld, das sich rasant entwickelt. Der Betreiber ist für die Cybersicherheit in seiner Kläranlage verantwortlich. Er kann Aufgaben des Cybersicherheitsprozesses seinem Betriebsleiter delegieren.


*Fig. 5 Informationssicherheitsprozess mit den fünf Funktionen des NIST Cyber Security Framework Core. (Quelle: NIST)*

Die nachfolgend vorgestellten Hilfsmittel erlauben es dem Betriebsleiter, den Prozess zu starten und erste Schritte selbständig zu unternehmen.

### IKT-MINIMALSTANDARD ABWASSER – EIN EINSTIEG

Ein guter Einstieg bietet der Minimalstandard für die Sicherheit der Informations- und Kommunikationstechnologie in Abwasserbetrieben (IKT-Minimalstandard Abwasser) [6]. Die Fragen im IKT-Minimalstandard Abwasser, Kapitel 5, dienen dem Betriebsleiter als Grundlage, um eine erste Risiko-Einschätzung durchzuführen und sich mit den verschiedenen Aspekten der Cybersicherheit vertraut zu machen. Der Betriebsleiter beantwortet die Fragen in den Checklisten mit JA oder NEIN. Sollte er mehrere Fragen nicht mit einem klaren JA beantworten können, besteht Handlungsbedarf.

Nachfolgend kann der Cybersicherheitsprozess gemäss IKT-Minimalstandard Abwasser eingeleitet werden. Dieser basiert auf dem *NIST Cyber Security Framework Core*, der die Sicherheitsmassnahmen in fünf Funktionen gliedert: Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen *(Fig. 5)*.

Im IKT-Minimalstandard Abwasser ist dieser Informationssicherheitsprozess auf die Abwasserbetriebe zugeschnitten:

- Beim Identifizieren geht es darum, in der ersten Phase das Inventar der OT- und IT-Infrastruktur und die Vernetzung zu dokumentieren. Die Vorarbeiten dazu kann der Betriebsleiter mit seinen Mitarbeitenden selbst durchführen. Danach ist ein Cybersicherheits-Experte beizuziehen und mit ihm die Risiken zu beurteilen.
- Schützen dient dazu, die identifizierten Risiken (IKT-Betriebsmittel) mit entsprechenden Massnahmen zu schützen.
- Erkennen (z.B. Überwachen der Zugriffe) hilft mögliche Angriffe auf die Schutzobjekte zu detektieren.
- Reagieren hilft diese abzuwehren bzw. zu minimieren.
- Wiederherstellen hilft nach einem Angriff wieder in den Normalbetrieb übergehen zu können und Verbesserungen vorzunehmen.

### DIE ROLLEN IM CYBERSICHERHEITSPROZESS

Cybersicherheit ist keine One-Man-Show. Um einen angemessenen Schutz zu gewährleisten, müssen alle Akteure ihre Verantwortung in diesem Bereich wahrnehmen. Der Betriebsleiter übernimmt hier eine organisatorische Rolle, um die Arbeiten der verschiedenen Mitspieler zu koordinieren. Diese unterstützen ihn dabei auf unterschiedliche Weise:

- Mitarbeitende des Betreibers, Lieferanten und Dienstleister helfen dem Betriebsleiter bei der Erstellung der Inventur seiner IKT-Betriebsmittel und Vernetzungen (IST-Zustand).
- Sie informieren ihn über die verschiedenen Schutz- und Sicherheitsmassnahmen, die von ihren Produkten und Dienstleistungen unterstützt werden.
- Die Mitarbeitenden tragen durch ihre tägliche sorgfältige Arbeit zur Cybersicherheit bei und helfen, die Bedürfnisse der Kläranlage zu definieren.
- Die Sicherheitsmassnahmen sollen unter Berücksichtigung des täglichen Betriebs getätigt werden.
- Die Beteiligten liefern dem Cybersicherheits-Experten Informationen aus ihren Fachgebieten.
- Der Cybersicherheits-Experte analysiert den IST-Zustand der Anlage, erarbeitet Lösungen und Verbesserungsvorschläge und priorisiert diese.
- Der Betreiber organisiert die Umsetzung der vom Cybersicherheits-Experten entworfenen Lösungen und Verbesserungsvorschläge.

Diese Tätigkeiten sind regelmässig zu wiederholen (konstant bis zu jährlich), denn Cybersicherheit ist kein Zustand, sondern ein Prozess, der fortlaufend angepasst und optimiert werden muss.

## SCHLUSSFOLGERUNGEN

Cybersicherheit ist ein breites und komplexes Feld. Wie so oft ist auch hier der erste Schritt der schwierigste. Die Antwort auf folgende Fragen bietet dem Betriebsleiter einen guten Anfang:

- Welche IKT-Betriebsmittel habe ich im Einsatz?
- Welche davon sind kritisch für den Betrieb meiner Anlage?
- Wie reagiere ich, wenn diese Systeme ausfallen?
- Sind die vorhandenen Risiken für meine Anlage und mich und den Betreiber tragbar oder gibt es Verbesserungspotenzial?

Diese Fragen zeigen auch den Ablauf eines Sicherheits-Assessments (Bewertung, Beurteilung, Einschätzung):

- Aufnahmen des IST-Zustandes (Inventur von Betriebsmitteln, Verbindungen, Vernetzung usw.).
- Einschätzung der Risiken (zusammen mit einem unabhängigen Cybersicherheits-Experten).

**DANK**

Danke dem BWL für seine Unterstützung, *Daniel Caduff* und *Sven Peter,* dem VSA zur Übernahme des IKT-Minimalstandards Abwasser, den Kläranlagen Neugut und Bachwis, die sich als Vorreiter in der Umsetzung betätigten, und *Johanna Otto* für das Lektorat zu diesem Beitrag.

– Entwicklung und Priorisierung von Massnahmen, um unakzeptable Risiken zu beheben.

Wo immer möglich, sollten wiederkehrende Aufgaben (z. B. Aktualisierung des Inventars, Überprüfung der Konfigurationen usw.) durch angemessene Wartungsverträge abgedeckt sein. Deren Ausführung sollte mindestens jährlich durch den Betriebsleiter überprüft werden.
Zur Erstellung des Inventars und der weiteren Umsetzung stehen den Kläranlagenverantwortlichen ab Sommer 2020 Tools von *step by STEP* zur Verfügung *(step-ara.ch)*, die es der Betriebsleitung ermöglichen, die Umsetzung Schritt für Schritt anzugehen und Massnahmen einzuleiten. Beim VSA werden die Tools ab Sommer 2020 ebenfalls zu beziehen sein. Cybersicherheit ist machbar. Die nötigen Kenntnisse und Technologien, um moderne, digitalisierte Anlagen sicher zu betreiben, sind vorhanden. Der IKT-Minimalstandard Abwasser bietet hierzu einen guten Leitfaden, um das Thema Cybersicherheit auf Kläranlagen Schritt für Schritt einzuführen und die Umsetzung anzugehen. Alles, was es jetzt zu tun gibt, ist zu handeln.

## BIBLIOGRAPHIE


[1] *Dragos Inc. (2017): https://dragos.com/wp-content/uploads/CrashOverride-01.pdf*

[2] *BABS, Bundesamt für Bevölkerungsschutz (2010): Factsheet zum kritischen Teilsektor Abwasser. https://www.babs.admin.ch/content/babs-internet/de/aufgabenbabs/ski/kritisch/_jcr_content/contentPar/accordion/accordionItems/entsorgung/accordionPar/downloadlist_680085480/downloadItems/188_1461240672904.download/abwasser_de.pdf*

[3] *BWL, Bundesamt für wirtschaftliche Landesversorgung (2017): Faktenblatt Abwasser. https://www.bwl.admin.ch/dam/bwl/de/dokumente/themen/ikt/faktenblatt_abwasser.pdf.download.pdf/Faktenblatt%20Abwasser.pdf*

[4] *BSI, Bundesamt für Sicherheit in der Informationstechnik (2019): Industrial Control System Security: Top 10 Bedrohungen und Gegenmassnahmen v1.3. [Online]. Available: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS/BSI-CS_005.pdf?__blob=publicationFile&v=12*

[5] *GschV. Gewässerschutzverordnung (Stand 01.05.2017): https://www.admin.ch/opc/de/classified-compilation/19983281/201705010000/814.201.pdf*

[6] *BWL. Bundesamt für wirtschaftliche Landesversorgung (2019): IKT-Minimalstandard Abwasser. https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abwasser.html*

[7] *webtitan.com (2019): Department of Homeland Security Issues Warning Over Targeted MSP Cyberattacks. https://www.webtitan.com/blog/homeland-security-warning-targeted-msp-cyberattacks/*

[8] *ISACA Switzerland Chapter: Aus- & Weiterbildung. https://www.isaca.ch/de/weiterbildung/ausbildung.html*


## > SUITE DU RÉSUMÉ


teurs tiers. La cybersécurité est réalisable. Nous disposons des connaissances et technologies afin d'exploiter en toute sécurité des installations modernes et numérisées. Il ne reste plus qu'à agir.