Bad Oeynhausen

DVGW S&C

FiW

Kennziffer: IT-01/20-BO

Bestandsaufnahme des IT-Sicherheitsniveaus von kleinen und mittelgroßen Kläranlagen in NRW unterhalb des Grenzwertes der KritisV – subKRITIS

Kurzbericht

gefördert vom

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

Bezirksregierung Detmold

KURZBERICHT

Forschungsinstitut für Wasser- und Abfallwirtschaft an der RWTH Aachen (FiW) e. V. / Kackertstraße 15 – 17 / 52056 Aachen
Fon: +49 (0) 241 - 80 2 68 25 / Fax: +49 (0) 241 80 2 28 25 / E-Mail: fiw@fiw.rwth-aachen.de / www.fiw.rwth-aachen.de

„Bestandsaufnahme des Informationssicherheitsniveaus von kleinen und mittelgroßen Kläranlagen in NRW unterhalb des Grenzwertes der KritisV – subKritis“

Kennziffer: IT-01/20-BO

Projektlaufzeit: 01.01.2021 – 31.12.2021

Zuwendungsempfänger:

Stadtwerke Bad Oeynhausen
Weserstraße 23
32547 Bad Oeynhausen

Unterauftragnehmer:

FiW - Forschungsinstitut für Wasser- und Abfallwirtschaft an der RWTH Aachen e. V.
Kackertstraße 15-17
52072 Aachen

DVGW Service & Consult GmbH
Josef-Wirmer-Straße 1-3
53123 Bonn

Fördermittelgeber:

Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes NRW
Emilie-Preyer-Platz 1
40479 Düsseldorf
Ansprechpartnerin: Frau Wienert

Bezirksregierung Detmold
Leopoldstraße 15
32756 Detmold
Ansprechpartner: Herr Krampe

Autoren:

Daniel Löwen M.Sc., Sebastian Kerger M.Sc. (FiW)

Rainer Stecken, Sachverständiger für Informationssicherheit nach ISO 17024 und ISO 27001 Lead Auditor, Björn Boos B.A, ISO 27001 Lead Auditor (DVGW Service & Consult GmbH)

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erläuterung
AWWA	American Water Works Association
B3S WA	Branchenspezifischer Sicherheitsstandard Wasser/Abwasser
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
DVGW	Der Deutsche Verein des Gas- und Wasserfaches e. V.
DWA	Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V.
E	Einwohner
EGW	Einwohnergleichwerte
EW	Einwohnerwerte
FFH	Flora-Fauna-Habitat
GIS	Geoinformationssystem
GK	Größenklasse
IDS	Intrusion Detection System
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik
IT-SiG	Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
Kritis	Kritische Infrastrukturen
KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen
MNQ	Mittlerer Niedrigwasserabfluss
MQ	Mittlerer Abfluss
OT	Steuerungstechnik (Operation Technology)
PLS	Prozessleitsystem
SBR	Sequencing Batch Reaktor
SPS	Speicherprogrammierbare Steuerung
TOM	Technisch-Organisatorischen Maßnahmen

1. Einleitung

Das Informationssicherheitsgesetz vom 25.07.2015 stellt einen Wendepunkt bezüglich der Informationssicherheit kritischer Infrastrukturen (KRITIS) dar. Mit seiner Verabschiedung wurde in unterschiedlichsten Bereichen der Grundversorgung rechtlich verankert, dass Maßnahmen zu ergreifen sind, um die Steuerungstechnik für den Betrieb kritischer Infrastruktur, z.B. von Kläranlagen, Wasserwerken, für die Energieversorgung und Krankenhäuser zu schützen. Dysfunktionalität würde die Grundpfeiler unseres zivilisatorischen Zusammenlebens erschüttern. Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG) und die daran gebundene Verordnung zur Bestimmung Kritischer Infrastrukturen (KritisV) des Bundesamts für Sicherheit in der Informationstechnik (BSI) haben Schwellenwerte aufgenommen, die aus dem Katastrophen- und Bevölkerungsschutz kommen. Kritisch ist, was mindestens 500.000 Einwohner betrifft. Alle Infrastruktur, die diesen abgeleiteten Schwellenwerte überschreitet, wurde zu Maßnahmen zur Steigerung der Informationssicherheit verpflichtet.

Das BSI-Gesetz sieht in §8a (2) die Möglichkeit für Verbände vor, eigene Sicherheitsstandards vorzuschlagen. Mit dem Blick in andere Länder hat deshalb eine gemeinsame Arbeitsgruppe der DWA und des DVGW das Regelwerk des **B**ranchen**s**pezifischen **S**icherheits**s**tandards Wasser/Abwasser (kurz: B3S WA) für die deutsche Wasserwirtschaft, auf Basis einer Grundlage der American Water Works Association (AWWA), erarbeitet. Ziel bei der Entwicklung des B3S WA durch die DWA und den DVGW war es, einen einheitlichen Standard sowohl für KRITIS- als auch kleinere Unternehmen zu schaffen. Der Standard wird alle zwei Jahre weiterentwickelt, um den sich ständig ändernden Herausforderungen zeitnah angepasst zu sein. Zudem hat der Standard von Anfang an Maßnahmen/Anforderungen in zwei Gruppen unterteilt. Einmal allgemeine Anforderungen, die jedes Unternehmen der Wasserwirtschaft erfüllen sollte. Zudem Anforderungen für die kritische Infrastruktur, die darüber hinausgehen und für Betriebe der kritischen Infrastruktur angewendet werden müssen. Die Eignung des B3S WA wird durch das BSI festgestellt.

Auf dieser Grundlage wurden im Rahmen des Projektes subKRITIS - Bestandsaufnahme des Informationssicherheitsniveaus von kleinen und mittelgroßen Kläranlagen in NRW unterhalb des Schwellenwertes der KritisV - Kläranlagen innerhalb der Bezirksregierung Detmold und gefördert durch das Ministeriums für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz Nordrhein-Westfalen untersucht. In diesem Kurzbericht werden die wesentlichen Erkenntnisse aus dem Projekt dargestellt, für ausführlichere Informationen kann der Abschlussbericht herangezogen werden.

2. Bestandsaufnahme

Im Projekt subKRITIS wurden insgesamt 13 Kläranlagen in Ostwestfalen für die Bestandsaufnahme des Informationssicherheitsniveaus begutachtet. Zunächst wurde für das Prozessverständnis der einzelnen Kläranlagen Begehungen (bspw. Verlauf des Wasserweges) und Befragungen durchgeführt.

2.1. Vorgehen

Die Bestandsaufnahme erfolgt in den beiden zwei Teildisziplinen der wasserwirtschaftlichen Seite und der IT-technischen Seite. Beide Teildisziplinen werden zunächst unabhängig voneinander betrachtet und einzeln bewertet.

Auf der wasserwirtschaftlichen Seite werden die möglichen Folgen, die aus dem abwassertechnischen Aufbau der Kläranlagen entstehen können, betrachtet. Für die Begehungen werden drei verschiedene Schadensarten betrachtet, welche potenziell auf den Kläranlagen ausgelöst werden könnten:

- Monetärer Schaden für Betreiber durch Überschreitung der Ablaufwerte
- Umweltschaden durch Abwasserverunreinigungen
- Sachschäden durch beispielsweise Überflutungen

Auf der IT-technischen Seite wird die Erfüllung der anlagenspezifischen Anforderungen zur Informationssicherheit betrachtet, um ein Eindringen in das System zu verhindern. Im Wesentlichen werden drei Ausfallmöglichkeiten als relevant betrachtet: Physischer Angriff, Cyberangriff und ein Stromausfall. Für alle drei Angriffsarten muss auf verschiedene Punkte geachtet werden. Dabei wurden die folgenden Aspekte prioritär betrachtet und Fragen zu den folgenden vier Themen gestellt:

- Allgemeine (physische) Sicherheit: Steckende Schlüssel, Perimeterschutz, usw.
- Physische Eingriffsmöglichkeiten: Handschieber, ungesicherte Bedienelemente, …
- Cyberangriffe: Begutachtung der IT-Infrastruktur und von regulierbaren Aggregaten
- Stromausfall: Notstromaggregate, „Blackouttests“, Rückhalt von Kraftstoffen.

Für jeden dieser Aspekte wurde an den jeweils relevanten Verfahrensstufen eine Bewertung durchgeführt. Im Anschluss der jeweiligen Anlagenbegehung erfolgte ein Interview zur Bestandsaufnahme des Informationssicherheitsniveaus auf Grundlage des B3S WA mit dem Betreiber, zuständigen Mitarbeitern oder externen Dienstleistern. Der B3S WA besteht aus dem DVGW-Merkblatt W 1060 bzw. DWA-M 1060 und dem Informationssicherheitsleitfaden in Excel- oder PDF-Form. Der Leitfaden wird durch ein Handbuch erläutert und bringt die wesentlichen Komponenten eines jeden Managementsystems für die Informationssicherheit mit:

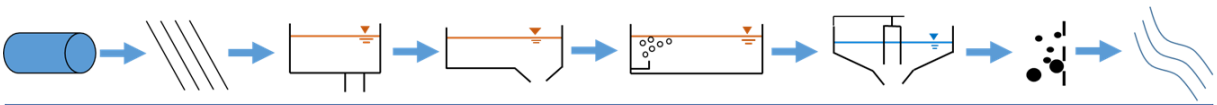
Aufnahme der Anforderungen, Bewertung der Risiken, entgegenwirkende Maßnahmen, Neubewertung des Risikos nach Maßnahmen und regelmäßige Wiederholung des Vorgehens. Das Merkblatt hilft zunächst die Begriffe zu verstehen, bspw. was ist eine Abwasserentsorgungsanlage aus Sicht der Informationstechnik. Der Informationssicherheitsleitfaden ist eine Excel-Liste, die von einer Website des DVGW heruntergeladen werden kann (Informationssicherheitsleitfaden (b3s-wa.de)). In der angewendeten Version 2 des Leitfadens kann dieser noch auf dem klassischen BSI-Grundschutz fußen, oder er verwendet bereits das BSI-Grundschutzkompendium. Im Falle subKRITIS wurde das Grundschutzkompendium aus dem Jahr 2019 angewendet, weil es dem B3S WA zu Grunde liegt. Das Handbuch zum Informationssicherheitsleitfaden beschreibt, wie dieser angewendet werden soll. Wegen seines normativen Charakters und seiner ubiquitären Einsatzmöglichkeit in der Wasserwirtschaft wurde der B3S WA als Analysewerkzeug für das Projekt subKRITIS gewählt.

2.2. Wasserwirtschaftliche Auswirkungen

Zur Einschätzung der abwasserwirtschaftlichen Auswirkungen ist zunächst eine Einordnung entscheidend, wann Informations-Sicherheitsmängel eine Relevanz für den Betrieb einer Kläranlage haben. Die Relevanz der Gefährdungen für den wasserwirtschaftlichen Bereich ist im Wesentlichen davon abhängig, ob durch die informationstechnischen Mängel ein steuernder Effekt direkt auf Anlagensteuerungen oder die Leitstellensoftware ausgelöst werden kann. Ist es möglich “schreibenden” Zugriff auf eine Kläranlage zu gewinnen, kann auf alle Systeme, Komponenten, Bauteile o.ä. zugegriffen werden, welche sonst nur über die Leitstelle steuerbar sind.

Ob einzelne Anlagen-Prozesse veränderbar sind, ist individuell unterschiedlich. So werden an einigen Kläranlagen noch viele Schieber rein händisch eingestellt oder Dosierungen über konstante Volumenströme gesteuert. Auf anderen Kläranlagen wiederherum, werden alle Prozesse über die Leitstellensoftware geregelt und können somit beeinflusst werden.

Bei den Begehungen wurden Angriffspunkte identifiziert, welche eine große Auswirkung auf die Abwasserreinigung oder möglicherweise Abschläge haben. Beispielhafte Angriffsmöglichkeiten sind in Abbildung 1 zu sehen.



Zulauf	Rechen	Sand-/ Fettfang	Vorklärung	Belebung	Nachklärung	Filtration
Schieber	Schieber	Ausfall Räumer	Ausfall Räumer	Ausfall Belüftung	Ausfall Räumer	Ausfall Fällmittel Dosierung
Manipulation Messsonde	Manipulation Messsonde	Aktivierung Notumlauf	Aktivierung Notumlauf	Manipulation Regelung der Belüftung	Veränderung Rücklaufschlammstrom	Veränderung der Rückspülintervalle

Abbildung 1: Beispielhafte Angriffsszenarien auf eine Kläranlage.

Wie lange ein Angriff unerkannt von statten gehen kann, ist insbesondere davon abhängig, ob das Alarmsystem kompromittiert wird und ob der Angriff bei einer Besichtigung auffällt. Daher lassen sich drei verschiedene Angriffsszenarien bezüglich der Dauer unterscheiden:

- Bereitschaftsstörung: Dauer 4 h
- Wochenendangriff: Dauer 24 h
- Versteckter Eingriff: Dauer ist unbekannt (Annahme 7 d)

Da alle Kläranlagen sowohl über eine Leitstellensoftware als auch über “schreibende” Informationssicherheitsmängel verfügen, kann jede Kläranlage als wasserwirtschaftlich vulnerabel eingestuft werden.

Um die Auswirkungen von möglichen Angriffen auf die Kläranlagen zu bewerten, wurden Kläranlagenmodelle zur Simulation der Angriffe aufgebaut. Dafür wurden alle 13 Kläranlagen mit Hilfe der Software SIMBA#WATER 4.3 vom Entwickler ifak - Institut für Automation und Kommunikation e. V. modelliert. Dabei besteht das Ziel der Simulation in dem Vergleichen und Identifizieren der kritischen Vulnerabilitäten unter Berücksichtigung unterschiedlicher Angriffsziele und Szenarien. Darauf aufbauend können Aussagen getroffen werden, auf welche Bereiche mit Sicherheitsmaßnahmen besonders geachtet werden muss.

Zur Ermittlung der Gefährdung, welche durch ein Teil- oder Vollversagen der Kläranlagen für die im Anschluss immer vorhandenen Vorfluter/Fließgewässer, Naturräume und wasserwirtschaftlichen Infrastruktur resultieren kann, wurde ein Stoffstrommodell aufgebaut. Dazu wurde ein GIS-Modell im Open Data Ansatz in Verbindung mit dem Modellsystem GREAT-ER (Geography-Referenced Regional Exposure Assessment Tool for European Rivers) aufgebaut. In diesem Modell wurden die Umweltkonzentration von Stickstoff und Phosphor modelliert, welche sich in den Fließgewässern bei verminderter Reinigungsleistung der Kläranlagen im Untersuchungsgebiet bei den Abflüssen MQ und MNQ einstellt. Auf Basis dieser Erkenntnisse wurden Empfehlungen zur Priorisierung von Kläranlagen getroffen.

2.3. Aufnahme des Informationssicherheitsniveaus

Das Schaubild in Abbildung 2 zeigt den Prozessablauf des B3S WA in einer vereinfachten Darstellung. Zu Beginn der Anwendung des B3S WA werden die **Assets** bzw. **Werte** der Anlage(n), bspw. Pumpen, Anlagenkomponenten der Filtrationsanlage, Rechen, usw. identifiziert und aufgelistet bzw. dokumentiert. Die Hauptfrage, die es anschließend zu beantworten gilt, ist „*was muss gesichert werden?*“. Dementsprechend werden die **Anlagen**, die es abzusichern gilt, definiert. Für Kläranlagen ist die Bündelung der Assets zu einer Anlage einfach zu leisten. Die Anlage besteht in aller Regel aus allen Werten innerhalb des Schutzzaunes. Davon ist beispielsweise das Kanalnetz mit eigenen Pumpstationen zu trennen, soweit sie nicht von der

Leitstelle gesteuert werden. Im nächsten Schritt erfolgt die Bestimmung der **Anwendungsfälle**, indem angeschaut wird, wie mit den jeweiligen Anlagen gearbeitet wird. Aus dem B3S WA ergeben sich bspw. Fragen wie „*Gibt es einen Server?*“, „*Wird nur lokal oder auch remote auf anlagenrelevante Baugruppen zugegriffen?*“ oder „*Wie werden die SPS-Steuerungen programmiert (lokal oder remote)?“* Der B3S WA v2 umfasst 23 Anwendungsfälle, aus denen sich unmittelbar vordefinierte Gefährdungen bzw. Risiken und ihnen entgegenwirkende Maßnahmen ergeben. Die **Risiken** lassen sich allerdings nicht mit geschlossenen Fragen, die mit ja oder nein zu beantworten wären, **bewerten**. Dementsprechend müssen in die Beurteilung der Fragen immer die genauen örtlichen Gegebenheiten einfließen.

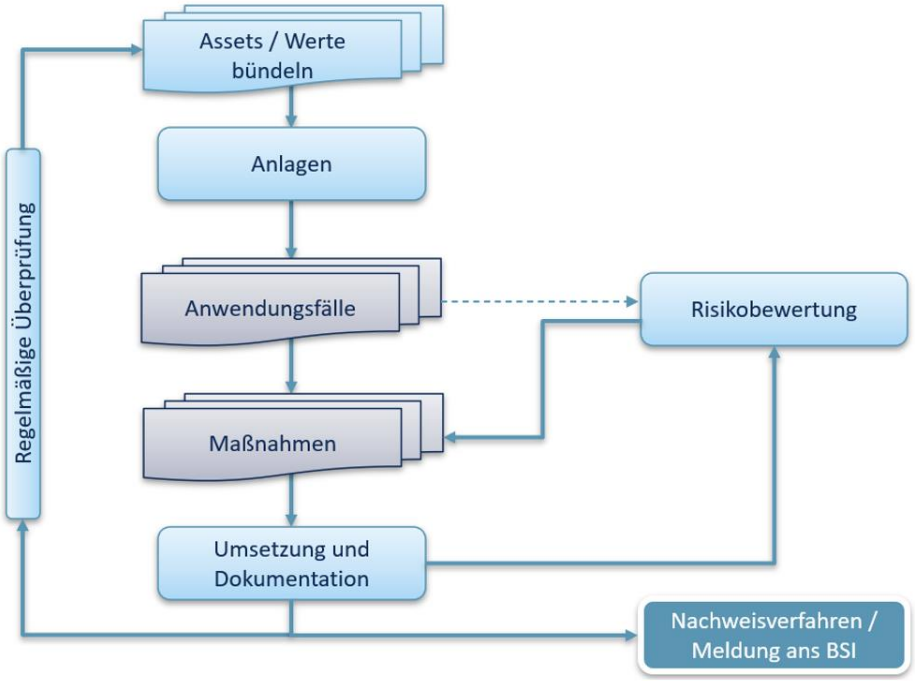


Abbildung 2: Vereinfachte Prozessdarstellung des Branchenspezifischen Sicherheitsstandards.

Gefährdungen können für verschiedene Anwendungsfälle gleichartig vorhanden sein. Um die Arbeitsbelastung für die Befragten deutlich geringer zu halten, wurde jede Gefährdung mit den dazugehörigen Maßnahmen aber nur einmal diskutiert. Für die vollständige Umsetzung des B3S WA wäre das nicht korrekt, weil mit den verschiedenen Anwendungsfällen verschiedene Assets verbunden sein können, deren Risiko natürlich getrennt betrachtet werden müsste. Für den Befragungszweck wurde jede Gefährdung aber nur einmal betrachtet und bei der Antwort versucht, die jeweilig unterschiedlichen möglichen Asset-Risiken zu berücksichtigen. Daraus ergibt sich, dass innerhalb der durchgeführten Interviews mit den verantwortlichen Personen der Kläranlagen insgesamt 949 Fragen bearbeitet und beantwortet wurden. Dahinter stehen

allerdings fast 6000 Gefährdungen. Da der B3S WA dem BSI Grundschutzkompendium[1] unterliegt, soll an dieser Stelle erwähnt werden, dass das Grundschutzkompendium Maßnahmen in sogenannten Bausteinen[2] bzw. Schichten zusammenfasst. Die Antworten aus den gestellten Fragen und ausgewerteten Tabellen ergeben, dass die meisten Fragen aus dem B3S WA im Rahmen dieser Untersuchung aus den vier Schichten *Netze und Kommunikation*, *Organisation und Personal*, *Betrieb* und *IT-Systeme* kommen. Das ist nachvollziehbar, denn Angriffe werden über Netzverbindungen ausgeführt und können nur durch korrekte Konfigurationen und unter der Aufsicht qualifizierten Personals verhindert werden.

3. Ergebnisse

3.1. Auswertung des Informationssicherheitsniveaus

Insgesamt kann festgehalten werden, dass das Interesse an Informationssicherheit bei den Verantwortlichen und Beschäftigten der Kläranlagen gegeben, und Wille zur stetigen Verbesserung vorhanden ist und bereits viele Maßnahmen zur Verbesserung der Informationssicherheit ergriffen wurden. Das Wissen bzw. die Kompetenzen in Punkto Informationssicherheit bzw. Informationstechnik hält allerdings in der Regel nicht mit der Einsicht in die Notwendigkeit Schritt.

Eine normierte Auswertung der Antworten des B3S WA nach Schichten ist der Abbildung 3 zu entnehmen. Diese zeigt auf, wo die Stärken und Schwächen im Bereich der Kläranlagen liegen. Spezifische Auswertungen für die drei untersuchten Größenklassen erscheinen nicht sinnvoll, weil die jeweilige Gesamtzahl zu gering ist.

Abbildung 3 zeigt, dass vor allem in den Schichten „*Konzeption und Vorgehensweise*“ sowie „*Infrastruktur*“ bereits über 60 % der Antworten „*sehr positiv“* oder „*gut*“ ausgefallen sind. Die Schichten „*Anwendungen*“ und „*Sicherheitsmanagement“* fallen dem gegenüber ab.

[1] Informationssicherheit mit System Der IT-Grundschutz des BSI (bund.de)

[2] BSI - IT-Grundschutz-Bausteine (Edition 2022) (bund.de)

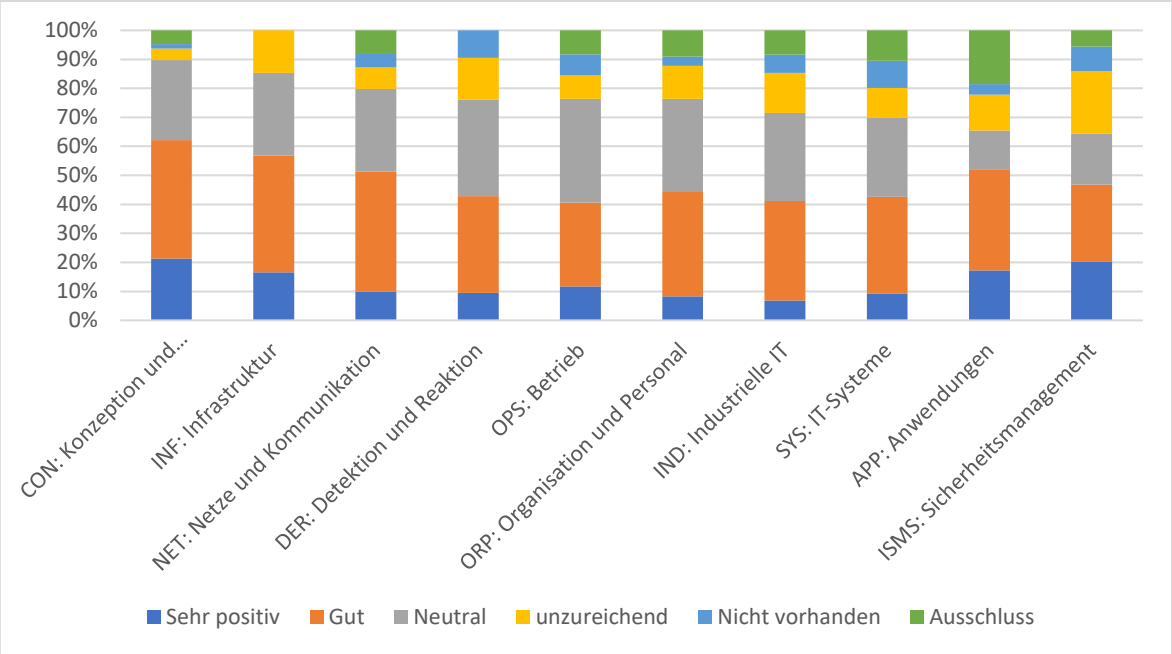


Abbildung 3: Antworten nach Schichten normiert – abnehmende Zahl positiver Antworten/Schicht.

Die technische Auswertung der Simulationsergebnisse einerseits und der Befragungsergebnisse nach dem B3S WA finden in Excel statt. Die Datenstrukturen unterscheiden sich in beiden Fällen stark. Deshalb werden zwei Tabellen verwendet. Eine Tabelle erlaubt die Auswirkung (engl. Impact) auszuwerten. Die andere Tabelle wird dazu genutzt, aus den wasserwirtschaftlichen Folgen, die für eine Anlage betrachtet werden, zu ermitteln, bezüglich welcher Informationssicherheits-Anforderungen etwas verbessert werden muss, damit diese Folgen gar nicht erst eintreten. Dazu zeigt Abbildung 4 für die virtuelle Anlage *Schlingensiepen* (Zusammengesetzt aus verschiedenen Untersuchungsteilen der realen Anlagen zum Zweck der Anonymisierung) auf der linken Seite die Anlagenteile, die bei Manipulation übers Netz zu einem Schaden (Überschreitung der erklärten Werte / Abschlag von Abwasser) führen würden. Zudem ist angegeben, welcher Fehler für den jeweiligen Anlagenteil eintreten würde.

Kläranlage-Impact	Schlingensiepen
Kläranlage	Schlingensiepen
IT-Relevanz	Schreibend
Beispielhafte Folgen	All
Betrachteter Zeitraum	168

Was ist betroffen?	Erklärte Werte überschritten /
Pumpwerke	
Ausfall	
Manipulation Messonden	
Rechen	
Räumer	
Räumer Intervall	
Veränderung Regelgrößen	
Zulaufschieber	
Zwischenpumpwerk	
Ausfall	
Gesamtergebnis	

Kläranlage-Impact	Schlingensiepen
Kläranlage	Schlingensiepen
Aktiv	ja
IT-Relevanz	Schreibend
Betrachteter Zeitraum	168

Maßnahmen	Bezeichnung der Maßnahme
CON.3.M4	Erstellung eines Minimaldatensicherungskonzeptes
CON.3.M5	Regelmäßige Datensicherung [IT-Betrieb]
CON.5.M10	Notfallvorsorge für Anwendungen [Leiter IT]
IND.1.M3	Schutz vor Schadprogrammen
IND.1.M7	Etablieren einer Berechtigungsverwaltung
IND.1.M9	Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten
IND.2.1.A1	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen [ICS-Administrator]
IND.2.1.A11	Wartung der ICS-Komponenten
IND.2.1.A4	Deaktivierung nicht genutzter Dienste, Funktionen und Schnittstellen
IND.2.2.A2	Einschränkung des Zugriffs für Konfigurations- und Wartungsschnittstellen
INF.1.M1	Planung der Gebäudeabsicherung
INF.2.A11	Automatisierte Überwachung der Infrastruktur
NET.1.1.A2	Dokumentation des Netzes
:::::::::::::::	::::::::::::::::::::

Abbildung 4: Verknüpfung Wasserwirtschaft ←→ Informationstechnik

Beispielhaft seien hier die Pumpwerke genannt, die entweder ausfallen können oder deren Messsonden manipuliert werden. Betrachteter Zeitraum ist im Beispiel 7 Tage. Die rechte Seite in Abbildung 4 zeigt, mit welchen Maßnahmen durch vollständige Umsetzung dem entgegenwirkt werden kann. Hierbei geht es um Datensicherung, Virenschutz, Berechtigungsverwaltung, Wartung, Systemhärtung und weiteres. Wohl gemerkt bedeutet dies nicht, dass bei Umsetzung aller Maßnahmen die Folgen nicht mehr eintreten können. Es bedeutet, dass es einem Angreifer sehr viel schwerer gemacht wird, den Schaden zu verursachen. Und je nach Maßnahme auch, dass der unerwünschte Zustand der Anlage schneller wieder verlassen kann, z.B. durch das Rückspielen von Backups. Da diese Auswertung auch für 4 h bzw. 24 h vorgenommen werden kann, lassen sich die wichtigsten Maßnahmen für jede Anlage schnell ermitteln. Dies stellt dann die im Projekt genannten „Quick Wins“ dar.

3.2. Auswertung der Wasserwirtschaftlichen Auswirkungen

Die wasserwirtschaftliche Auswertung und Aufbereitung der Begehungen und der Simulation haben gezeigt, dass es einige Stellen auf den Kläranlagen gibt, an denen kurzfriste Änderungen für eine Steigerung der Sicherheit möglich sind. Dazu gehört beispielsweise, dass Schlüssel nicht mehr in Aggregaten stecken, Tore und Türen verschlossen werden und offenes Messequipment geschützt wird. Dazu sollte besondere Acht auf das Alarmsystem gelegt werden. Dieses sollte für die wichtigsten Parameter redundant ausgelegt sein, damit es auch bei kompromittierter Leitstelle warnt. An den kritischen Stellen (beispielsweise Überwachung Schieberstellungen durch Wasserstandsmessungen) sollte also ein separates, unabhängiges Alarmsystem ergänzt werden.

Die Ausführung und Kontrolle der Notstromversorgung ist auf einigen Kläranlagen verbesserungswürdig. Die Notstromversorgung ist auch für physische oder Cyberangriffe von großer Bedeutung und sollte deshalb kombiniert betrachtet werden. Aggregate waren auf den meisten Anlagen vorhanden. Die Durchführung von „Blackouttests” sind zur Kontrolle der Aggregate dringend zu empfehlen. Kontakt zum THW und bereits eingebaute Anschlussmöglichkeiten für externe Stromversorgung sind zu herzustellen.

Weiterhin bietet die Handsteuerung von Aggregaten physische Angriffspunkte, aber gleichzeitig auch die Möglichkeit auf Angriffe zu reagieren. Hier muss versucht werden ein Mittelweg zu finden. Es sollte sichergestellt werden, dass Aggregate auch per Hand im Falle eines Cyberangriffes bedienbar sind, gleichzeitig muss darauf geachtet werden, dass diese durch Schlüssel oder Schlösser gesichert werden können. Ebenso sollte eine Veränderung der Stellung (Umschaltung in Handmodus) an kritischen Stellen zu einem Alarm führen.

Auf Grund der geringen Zeiten, ab denen es zu Schäden auf den Kläranlagen kommen kann, sind funktionierende (separate) Alarmsysteme zur Reaktion auf Angriffe das wichtigste Instrument. Die Begehungen an Wochenenden und Feiertagen können diese nur teilweise ersetzen. Diese personellen Sichtprüfungen sind allerdings unerlässlich, wenn es zu einem Ausfall der Alarmsysteme kommen sollte. Bei der individuellen Betrachtung sind dabei immer die Anlagenteile zu priorisieren, durch die ein unkontrollierter Austritt entstehen kann (z.B. Zulauf), die einen Prozess in der Kläranlage gefährden (z.B. die Bakterien in der Biologie) und die, die die höchste Schadstofffracht emittieren können (z.B. Schlammabtrieb Nachklärbecken).

3.3. Übertragbarkeit der Ergebnisse

Die Ergebnisse des subKRITIS Projekt sollen laut Zielstellung möglichst auf alle Kläranlagen in NRW übertragen werden, um eine Einordnung des allgemeinen Informationssicherheitsniveaus von Kläranlagen unterhalb der KritisV darzustellen. Hierzu sollte in Zukunft auch eine bundesweite Betrachtung durchgeführt werden. Dies ersetzt allerdings nicht die individuelle Untersuchung einer einzelnen Kläranlage auf ihre spezifischen Sicherheitslücken und Anfälligkeiten für Angriffe.

Im Projekt wurden 13 Kläranlagen untersucht. Insgesamt gibt es in NRW 599 Kläranlagen (Stand 31.12.2018) (IT.NRW, 2021). Somit wurde nur ein geringer (< 2 %) Teil betrachtet. Die Kläranlagen decken im Ausbau die Größenklassen 3 bis 5 ab. Die angeschlossenen Einwohnerwerte liegen zwischen 2.300 und 115.000 EW. Diese Anlagen gehören nicht zu den sondergesetzlichen Abwasserverbänden in NRW, sondern werden vornehmlich von den Kommunen betrieben. In der Verfahrenstechnik zeigten die Kläranlagen deutliche Unterschiede auf. Als Reinigungsverfahren wurden auf den Anlagen Kaskaden, intermittierende, simultane und vorgeschaltete Denitrifikationen eingesetzt als auch ein SBR Verfahren. Zudem wurden einzelne Anlagen mit einer dritten und vierten Reinigungsstufe betrachtet.

Im Projekt wurden somit sehr kleine Kläranlagen, Membranbelebungsanlagen, Kläranlagen mit einem sehr hohen industriellen Anteil und sehr hoch ausgelastete kommunale Kläranlagen nicht betrachtet. Weiterhin wurden Kleinkläranlagen bisher nicht betrachtet, allerdings sind diese zu vernachlässigen, da diese zumeist keine IT aufweisen und auch der Ausfall geringere Folgen hätte als der von kommunalen Anlagen. Da industrielle Kläranlagen mit 15,9 % einen wesentlichen Anteil am eingeleiteten Abwasser in Gewässer haben (MULNV NRW, 2022), müssten auch diese auf ihre Sicherheit untersucht werden, um die Umwelt vor Schäden durch Angriffe auf Kläranlagen zu schützen. Dies ist auf Grund der Vielfalt und der privaten Betreiber schwierig zu untersuchen. Als letzter Punkt sollte auch eine separate Untersuchung mit Fokus auf die Kanalisation erfolgen. Dieses wurde bisher in diesem Vorhaben nicht untersucht, stellt aber unterhalb der KritisV ein Ziel dar, über welches erhebliche Schäden verursacht werden können.

Insgesamt gibt die Untersuchung im subKRITIS-Projekt eine erste Stichprobenanalyse mit gutem Einblick in kommunale Kläranlagen unterschiedlicher Größe. Auf Grund der Vielfalt der kommunalen Kläranlagen ist dieses Vorhaben aber nicht als repräsentativ für ganz NRW anzusehen. Für eine repräsentative Aussage für alle Kläranlagen sollte die Stichprobenanzahl erhöht werden. Weiterhin sollten Kläranlagen mit den genannten - nicht untersuchten – Eigenschaften mit aufgenommen werden. Zudem wäre auch ein regionaler Vergleich und ein Vergleich der Organisation (durch beispielsweise Wasserverbände) relevant, um regionale/ organisatorische Strukturen und Muster zu unterscheiden.

3.4. Ableitung von Prioritäten

Zur Priorisierung des Schutzbedarfes wird dieser in zwei Punkte unterteilt. Zunächst wird untersucht, welche Anlagenteile auf Kläranlagen die höchste Vulnerabilität für den Abwasserreinigungsprozess aufzeigen. Im nächsten Schritt wird abgeleitet, ob es Kläranlagengruppen gibt, welche prioritär geschützt werden sollten, um bei einem einzelnen oder kollektiven Ausfall die entstehenden Schäden zu minimieren.

3.4.1. Priorisierung von Anlagenteilen

Auf abwasserwirtschaftlicher Seite gibt es auf den Kläranlagen Prozesse die immer prioritär geschützt werden sollten. Dazu gehören beispielsweise die Belüftung, der Schlammabzug oder vorhandene Abwasserpumpwerke. Auch gehört dazu die Kanalnetzsteuerung, die in diesem Projekt aber nicht näher behandelt wurde. Durch die individuellen Aufbauten der Kläranlagen gibt es auf jeder Kläranlage weitere kritische Punkte, die nur durch eine Begehung festgestellt werden können und auch zu schützen sind. Der abwasserwirtschaftliche Schutz kann ergänzend zur Informationssicherheit durch Alarmsysteme oder durch *physische Sicherheit* geschaffen werden.

Auf Basis der Erkenntnisse auf den einzelnen Kläranlagen kann keine Priorisierung erfolgen, welche Kläranlage schützenswerter sind als andere. Auch die Größe der Kläranlagen spielt keine übergeordnete Rolle, sondern der individuelle Aufbau ist der maßgebende Faktor für die Anfälligkeit einer Anlage.

3.4.2. Priorisierung einzelner Anlagen

Auf Basis der Betrachtung der SIMBA Simulation zeigt sich, dass aus den bisherigen limitierten Daten aus abwasserwirtschaftlicher Sicht keine Priorisierung der Kläranlagen erfolgen kann, da die Anfälligkeit der Abwasserreinigung gegenüber Angriffen maßgeblich von den individuellen Charakteristika (hydraulische Verweilzeit, Auslastung) und Aufbau der Kläranlagen abhängig ist. Weitere Zusammenhänge könnten gegebenenfalls aber mit einer größeren Datenbasis erkannt werden.

Anhand der GIS-Modellierungsergebnisse erweist sich auf wasserwirtschaftlicher Seite die Priorisierung von großen Anlagen oder Anlagen mit hohem Abwasseranteil am Gewässer als sinnvoll. Die erheblichen Unterschiede bei den Emissionen der Anlagen des Arbeitsgebietes führen dazu, dass besonders die Abschnitte hinter großen Kläranlagen Grenzwertüberschreitungen aufweisen. Analog dazu gibt es große Anlagen, die in keinem der simulierten Szenarien Grenzwertüberschreitungen in den anschließenden Gewässern verursachen.

Aus diesen Gründen ist eine Ableitung der schützenswerten Anlagen nur auf Grund der Basis der Größe der Kläranlagen nicht zielführend für einen Schutz von Gewässern, Umwelt und Trinkwassergewinnung. Bei weiträumigerer Betrachtung sollte in der Priorisierung mehr Wert auf den Anteil des Kläranlagenabflusses am Gewässer und auf relevante Nutzungsarten im Gewässer - wie die Trinkwasserversorgung - gelegt werden. Hier könnte eine Vorgehensweise analog zur Mikroschadstoffstrategie von NRW angestrebt werden.

4. Ableitung von fachpolitischen Ansätzen

Im Rahmen der Bestandsaufnahme wurde kurz-, mittel- und langfristiger Handlungsbedarf zur Herstellung einer sicheren IT-Infrastruktur identifiziert. Daraus wird eine erste fachpolitische Agenda formuliert, die zu einer Verbesserung des Schutzniveaus von Kläranlagen beiträgt. In Abbildung 5 sind im Zeitstrahl kurz- und langfristige Maßnahmen dargestellt, welche zur Erhöhung des Schutzniveaus beitragen.

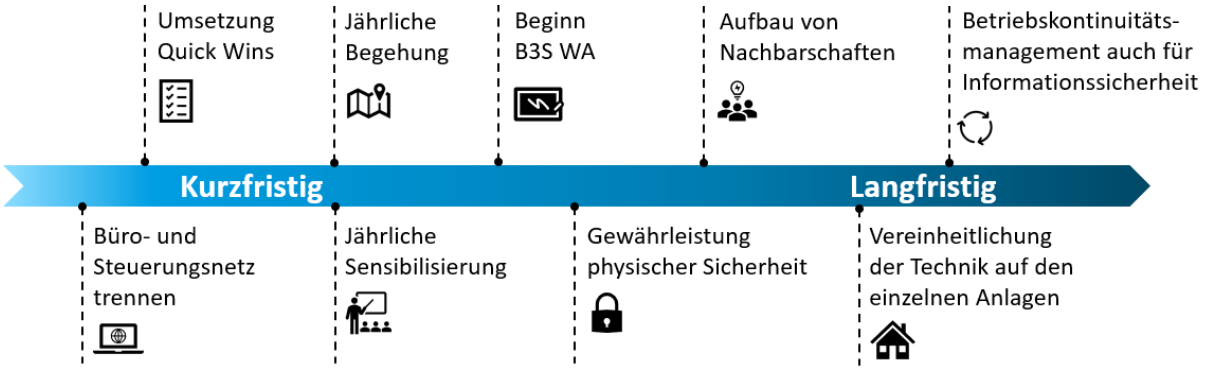


Abbildung 5: Empfohlener Zeitplan für die kurz- und langfristige Maßnahmen-Umsetzung.

Mittelfristig sollte der vorhandene Standard (B3S WA) von den Betreibern umgesetzt werden. Zusammenschlüsse und Spezialisierung einiger Mitarbeiter, z.B. auf Kreisebene, würden das erleichtern. Bei Anwendung des B3S WA muss ein *Informationssicherheitsmanagementsystem* (ISMS) implementiert werden, in dem u.a. die in Abbildung 6 genannten Maßnahmen umgesetzt werden. Dabei ist in einem regelmäßigen Zyklus, die Überprüfung und (Risiko-) Bewertung durchzuführen, um ein entsprechendes Sicherheitsniveau zu erstreben. Grundsätzlich ist für jede Anlage eine individuelle Priorisierung von Schutzmaßnahmen auf Grundlage

einer Risikoabschätzung notwendig. Um das Risiko am Puls der Zeit abschätzen zu können, sollten bspw. Schulungen strukturiert und regelmäßig erfolgen und in einen periodischen Rahmen implementiert werden. Auf Grundlage einer zu erstellenden Gefährdungsabschätzung sind an dieser Stelle die Erstellung von Backups, eine segmentierte Trennung der Netze sowie die Durchführung von Updates zu nennen. Zusätzlich stehen das Trennen der Netze von Steuerungstechnik und IT, Absichern von bestehenden externen Zugriffen, ein Zugriffs- und Kontenmanagement und die Vergabe von sicheren Passwörtern im Zentrum der Empfehlungen. In diesem Zusammenhang sollte auch ein regelgeleitetes und systematisches Monitoring der Datenflüsse erfolgen.

5. Empfehlungen zur Informationssicherheit (Quick-Wins)

Im Datenschutz ist der Begriff der Technisch-Organisatorischen Maßnahmen (TOMs) bekannt. Der Begriff beschreibt gut, wie Informationssicherheit zu erreichen ist. Zu 100 % ist das nicht zu schaffen und sollte somit als Disziplin des stetigen Strebens eines hohen Sicherheitsgrades in der Informationssicherheit verstanden werden. Allerdings ist es bereits mit vergleichsweise geringem Aufwand möglich den potenziellen Angreifern unattraktiv zu machen. Monetär motivierte Angreifer können so sehr gut von den Anlagen ferngehalten werden. Technisch ist dies durch sauberes Aufsetzen segmentierter Netze und guten Schutz gegen ungewollten äußeren Zugriff erreichbar, organisatorisch hauptsächlich durch Verbessern des Wissens der Mitarbeiter. Organisatorisch auch dadurch, dass sich auf den Fall einer Kompromittierung gut vorbereitet und überlegt wird, wie der ordnungsgemäße Zustand der Steuerung der Kläranlage schnell wiederhergestellt werden kann und diese Prozesse dokumentiert.

Natürlich müssen Steuerungen parametriert und hier und da auch Anpassungen an der Leitstellensoftware vorgenommen werden. Allerdings können grundsätzlich Steuerungen, die nicht aus dem Internet erreichbar sind, auch nicht von dort kompromittiert werden. Was sich so trivial anhört, ist die beste Methode zum Schutz kritischer Infrastrukturen. Und in der Tat gehen viele Unternehmen der kritischen Infrastruktur so vor, zu der ebenfalls Energieversorger zählen. Die Vorteile liegen auf der Hand, Angriffe übers Internet sind somit unmöglich, Updates aller Geräte sind nur aus funktionalen, nicht aber aus Sicherheitsgründen notwendig und mittels Intrusion Detection Systemen (IDS, Angriffserkennungssysteme) lassen sich nicht zulässige Netzteilnehmer sehr einfach sichtbar machen.

Zusammengefasst lassen sich allgemein folgende Maßnahmen umsetzen, die schnell das Sicherheitsniveau auf den Kläranlagen anheben.

1. *Trennung von IT und Prozess- bzw. Steuerungstechnik. Das ist auf den meisten Anlagen umgesetzt. Eine gelegentliche Überprüfung, ob die Trennung wirklich besteht, ist*

zu empfehlen. Dies kann mit einem Intrusion Detection System (Angriffserkennungssystem) geschehen oder vom IT-Dienstleister mit Programmen wie Wireshark geprüft werden.

2. *Der Internetzugang zur Anlage wird auf getrenntem Weg per Telefoneinwahl (Außenverbindung) oder auf Anforderung von intern freigeschaltet. Der externe Zugriff kann also nur durch zwei unabhängige Handlungen hergestellt werden.*
3. *Regelmäßige Schulungen des Personals führen zum Anwachsen des Informationssicherheitsbewusstseins. Im IT-Bereich der Städte und Gemeinden, häufig in Zusammenarbeit mit kommunalen Rechenzentren und/oder Dienstleistern, werden solche Schulungen angeboten. Auch wenn sie nicht spezifisch auf Steuerungen ausgelegt sind, ist die jährliche Teilnahme an diesen Schulungen zu empfehlen.*
4. *Regelmäßige Prüfung von Zugriffs- und Benutzermanagement aus den aufgezeichneten Logs. Überprüft werden sollten die Logs der Firewalls und der eingesetzten PCs.*
5. *Regelmäßige Prüfung auf Updates der Softwarekomponenten, die dauerhaft oder gelegentlich Verbindung zum Internet haben. Updates müssen immer zeitnah eingespielt werden. So sollten nach einem Patch-Tuesday von Microsoft (2.ter Dienstag im Monat) nicht mehr als drei Tage verstreichen, bis die Systeme mit den Patches versehen sind. Updates der Virenschutzlösungen müssen täglich vorgenommen werden, weil es im Moment mehr als 300.000 neue Schadprogramme täglich gibt. Die kann jeder Virenschutz nur finden, wenn er sehr aktuell gehalten wird.*
6. *Regelmäßiges Erstellen von verlässlichen (Offline-)Backups von Systemen und Daten. Auch Systeme können so auf externe Datenträger übertragen werden, dass nach Datenträgerwechsel die Rechner mit dem externen Sicherungssystem sofort wieder mit voller Funktionalität starten. Werden dann die Daten des letzten Backups wieder zurückgespielt, werden bestenfalls einige Stunden in denen die Daten nicht aktuell sind verloren.*
7. *Wer auch das vermeiden möchte, muss sich mit der Etablierung von redundanten Systemen befassen, die während des Betriebs auf ein Sekundärsystem spiegeln. Dieses einzurichten verlangt allerdings viel Erfahrung, damit nicht versehentlich ein kompromittiertes System automatisch auf die redundante Maschine übertragen wird.*
8. *Planung und Organisation der Business Recovery (für alle Fälle), insbesondere müssen eine aktuelle Dokumentation und aktuelle Backups vorhanden sein. Es ist zu überlegen, wie lange es dauern darf, bis das Steuerungssystem komplett neu aufgesetzt ist. Dazu wird sich also am schlimmsten anzunehmenden Fall orientiert. Es sollte nicht nur ein Konzept aufgestellt werden, sondern es sollte regelmäßig mindestens jährlich getestet werden.*

9. *Wenn ein Prozessleitsystem kompromittiert ist, wird es auch keine Alarme mehr korrekt weiterleiten. Für die wichtigsten Parameter, die zum Überschreiten erklärter Werte führen, sollte deshalb ein zweites Alarmsystem aufgebaut sein, das nur meldet und nicht von außen erreichbar ist.*
10. *Wenn die Verbindung des Prozessleitnetzes zum Internet dauerhaft besteht, sollte regelmäßig ein Penetrationstest durch einen unabhängigen, externen Tester vorgenommen werden. Dieser Tester braucht viel Erfahrung, damit nicht durch Unachtsamkeit Steuerungen betätigt werden und so der eigentlich zu verhindernde Schaden durch den Test erzeugt wird. Solche Tests werden üblicherweise als „White Hat"-Test ausgeführt, d.h. der Anlagenbetreiber verabredet mit dem Tester, wann der simulierte Angriff durchgeführt wird oder ist sogar während des Tests mit dem Angreifer verbunden.*
11. *Informationssicherheit muss als Managementsystem betrieben werden, d.h. die entsprechenden Untersuchungen müssen jährlich wiederholt werden, die Ergebnisse dokumentiert und die Fortschritte gegenüber dem Vorjahr vom Anlagenverantwortlichen beurteilt werden.*
12. *Mit Blick auf die Notstromversorgung verweisen wir auf das Dokument des BBK* (BBK, 2019)*.*
13. *Die zuständigen Behörden sollten bei der Verbreitung der Verhaltensempfehlungen unterstützen. Ggfs. ist zu überlegen, Veranstaltungen zum Thema zu initiieren. Spezifische Schulungspläne, die die Besonderheiten für Kläranlagen beinhalten, sollten entwickelt werden.*
14. *Menschen, die sich aus Eigeninteresse mit Informationssicherheit befassen und sich weiterbilden, z.B. von der Meister:in zur Techniker:inebene, sollten unbedingt motiviert werden, im Unternehmen zu bleiben. Es ist zu überlegen, ob solche Positionen in Anlagenübergreifenden Stellenplänen oder einer Art Stabsfunktionalität eingerichtet werden können. Es ist auch sinnvoll, Weiterbildung in diesem Bereich proaktiv anzubieten und Bildungsurlaubsansprüche dafür einzusetzen. Gut ausgebildete Experten;innen für Informationssicherheit wecken immer externe Begehrlichkeiten. Die Wasserwirtschaft benötigt sie aber auch.*
15. *Der B3S WA sollte auf allen Anlagen umgesetzt werden.*

6. Ausblick

Zusammengefasst ist festzustellen, dass die verwendete und weiter entwickelte Methodik sowohl die Schwachstellen identifizieren, als auch auf der IT-Seite die Anforderungen und Maßnahmen benennen kann, die der leichten Ausnutzbarkeit entgegenwirken. Es hilft den Anlagenbetreibern zu priorisieren, was vorrangig umgesetzt werden muss und reduziert so den zwingend zu leistenden Aufwand. Dies ist sowohl für einzelne Anlagen als auch in Summe

möglich. Die Automatisierung dieser Auswertungen kann Gegenstand eines weiterführenden Projektes sein. Des Weiteren spielen die aktuellen Veränderungen bezüglich europäischer Richtlinien bzw. Verordnungen wie bspw. der NIS2-Richtlinie und der damit verbundenen Wandlung in nationales Recht eine wichtige Rolle und sorgen für weiteren Handlungsbedarf in Punkto Informationssicherheit. Im Januar 2022 sollen mit Beginn der französischen Ratspräsidentschaft die Triologverhandlung zur NIS-2-Richtlinie gestartet werden. Mitte dieses Jahres soll dann die NIS-2-Richtlinie in Kraft treten. Nach jetzigem Kenntnisstand will die EU-Kommission daran festhalten, einen einheitlichen europäischen Schwellenwert für KRITIS-Unternehmen auf Basis der KMU-Empfehlung der EU-Kommission (2003/361/EG) festzulegen. Demnach ist vorgesehen, dass nur Kleinst- und Kleinunternehmen mit weniger als 50 Beschäftigten und einen Jahresumsatz bzw. Jahresbilanz von maximal 10 Mio. €, die sogenannte *size-cap rule*, von der gesetzlichen Verpflichtung in Bezug auf ein Mindestniveau von Informationssicherheit ausgenommen werden. Auch Unternehmen mit einer Beteiligung der öffentlichen Hand von mehr als 25 % sollen unter die Regelung fallen. Nach erster Abschätzung des BMI würden durch die Einführung der size-cap rule statt bisher 1.500 Unternehmen zukünftig ca. 40.000 Unternehmen (alle Sektoren) in Deutschland als KRITIS-Unternehmen eingestuft werden.

Die Betrachtung der Übertragbarkeit zeigt, dass eine Erweiterung der Untersuchungen auf weitere Kläranlagen notwendig ist. Dabei sollten noch kleinere Kläranlagen und auch bisher nicht erfasste Strukturen und Verfahren betrachtet werden. Dazu gehört auch der Schlammweg der Kläranlagen der nicht Teil dieser Untersuchung war. Zudem wäre auch ein regionaler Vergleich und ein Vergleich der Organisation (durch beispielsweise Wasserverbände) relevant. Wird die Betrachtung um die genannten Punkte erweitert ist eine Übertragung auf alle Kläranlagen in NRW möglich.

Insgesamt spielt die industrielle Abwasserbehandlung in NRW (mit einem Anteil von 15,9 % am gesamten eingeleiteten Abwasser) und auch in Deutschland eine wesentliche Rolle in der Abwasserbehandlung (MULNV NRW, 2022). Es sind Angriffsszenarien möglich, in denen es sowohl zu direkten Einleitungen von Abwässern in Gewässern kommt oder nicht vorgereinigtes Abwasser in kommunale Kläranlagen gelangt. Aufgrund der möglicherweise höheren Belastung und Toxizität dieses Abwassers können so erhebliche Schäden in Gewässern resultieren oder Belebtschlämme auf kommunalen Kläranlagen langfristig Schaden nehmen. Hier sollte eine Überprüfung erfolgen, inwiefern eine Informationssicherheit auf diesen Kläranlagen existiert. Kontrollen und eine Ist-Aufnahme sind aufgrund der vielfältigen privaten Betreiber schwierig.

Die ersten Modellierungsergebnisse haben exemplarisch gezeigt, dass die reine Kläranlagengröße nicht der wichtigste Faktor für die Priorisierung von Schutzniveau vor Angriffen darstellt.

Insbesondere der Anteil der Kläranlage am Vorfluter und die Nutzungen des Gewässers im Unterstrom sind von großer Bedeutung. Für eine Einstufung eines Schadens wurden in dieser Arbeit Umweltqualitätsnormen verwendet. Hier sind weitere Untersuchungen notwendig, um zu zeigen, welche zeitlichen und gewässerspezifischen Faktoren letztendlich zum konkreten Eintritt von ökologischen Schäden und einer erheblichen Beeinflussung der Trinkwassergewinnung führen. Darauf aufbauend können Risikoanalysen für Kläranlagen erstellt werden du aus den Ergebnissen neue sinnvollere KRITIS Grenze für Kläranlagen bestimmt werden.

Weiterhin ist auch das Kanalnetz von großer Relevanz. Die Kanalisation wird auch in der KritisV aufgeführt und besitzt dieselben Schwellenwerte wie Kläranlagen von 500.000 EW zur Einstufung als kritische Infrastruktur. Von Kanalnetzen gehen große Schadenspotenziale aus, da ökologische Schäden durch Einleitung von ungeklärtem Abwasser entstehen können und monetäre Schäden und seuchenhygienische Gefahren durch eine forcierte Überflutung von Siedlungsflächen möglich sind. Hier sollte analog zum subKritis Projekt eine Bestandsaufnahme, der unter der KritisV fallenden Kanalisationen erfolgen.

7. Literaturverzeichnis

BBK. (2019). *Leitfaden für die Planung, die Einrichtung und den Betrieb einer Notstromversorgung in Unternehmen und Behörden.* Von https://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/PiB/PiB-13-notstromversorgung-unternehmen-behoerden.pdf?__blob=publicationFile&v=8 abgerufen

IT.NRW. (05. 07 2021). *ELWAS-WEB*. Abgerufen am 08 2021 von Landesbetrieb Information und Technik Nordrhein-Westfalen: https://www.elwasweb.nrw.de/elwas-web/index.jsf;jsessionid=984FCB12CBB06885C2F7BC84A747AA50

MULNV NRW. (2022). *Entwicklung und Stand in der Abwasserbeseitigung in Nordrhein-Westfalen.* Stichtag der Daten: 31.12.202, Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfale, Düsseldorf. Von https://www.lanuv.nrw.de/fileadmin/lanuv/wasser/abwasser/lagebericht/00_EStAb2020_Gesamtversion.pdf abgerufen

Glossar

Asset- und IP-Listen	Mit Assets sind alle Steuerungen und Netzwerkkomponenten gemeint, die in dem Steuerungsnetz einer Kläranlage vorkommen. Diese haben eine Hardware-Adresse, die so genannte MAC-Adresse (Media-Access-Control-Address) und eine IP-Adresse (Internet-Protokoll-Adresse). An Hand beider kann ein Gerät eindeutig identifiziert werden.
American Water Works Association	Die American Water Works Association ist eine internationale gemeinnützige wissenschaftliche und pädagogische Vereinigung, die gegründet wurde, um die Wasserqualität und -versorgung zu verbessern.
Branchenspezifischer Sicherheitsstandard Wasser/Abwasser	Branchenspezifischer Sicherheitsstandard Wasser/Abwasser, mittlerweile in der Version 3 verfügbar, ein Sicherheitsstandard, der ausgehend von einer Anlage und der Betriebsart nur die für diese spezifische Anwendungsumgebung erforderlichen Sicherheitsvorkehrungen verlangt. Er basiert auf dem Grundschutzkompendium des BSI jeweils aus dem Erscheinungsjahr des Standards und wird von der DWA und dem DVGW gemeinsam erarbeitet.
Intrusion Detection System	Angriffserkennungssystem ist ein System zur Erkennung von Angriffen, die gegen ein Computersystem oder Rechnernetz gerichtet sind. Ab dem 03. Mai 2023 ist der Betrieb für die kritische Infrastruktur vorgeschrieben (BSIG §8a Abs. 1a)
Intrusion Prevention System	Eine Software, um Angriffe unmittelbar ereignisgesteuert automatisch zu blockieren. In Büroumgebungen in der Regel problemlos einsetzbar, in Steuerungsumgebungen eher nicht.
Informationssicherheitsmanagementsystem	Ist die Aufstellung von Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
KRITIS	Kritische Infrastrukturen sind Anlagen, Systeme oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen hätte.
Steuerungstechnik (Operational Technology - OT)	Abgrenzung zur IT (Informationstechnik), die meisten der eingesetzten Techniken sind heute für beide Bereiche gleich.
Patch	Ein Patch (engl. to patch = flicken, ausbessern) ist eine Korrekturauslieferung für Software oder Daten aus Endanwendersicht, um Fehler zu beheben – meist um bekannt gewordene Sicherheitslücken zu schließen – oder bislang nicht vorhandene Funktionen nachzurüsten.
Perimeter (-los)	Grenze zwischen zwei Segmenten, z.B. innen und außen bei einem Netzwerk. Perimeterlos bedeutet also, dass innen und außen nicht mehr unterschieden wird.
Physische Sicherheit	Physische Sicherheit oder -management auch als Objektschutz bezeichnet, ist eine Kombination aus baulichen, technischen, organisatorischen und personellen Maßnahmen. Dazu gehören beispielsweise eine Zutrittskontrolle oder Einbruchsicherung.

Prozessleitsystem	Dient zum Führen einer verfahrenstechnischen Anlage, zum Beispiel einer Kläranlage. Es besteht typischerweise aus sogenannten prozessnahen Komponenten (PNK - zur direkten Steuerung von Pumpen und Schiebern) und Bedien- und Beobachtungsstationen (BUB, auch Anzeige und Bedienkomponente (ABK), zum Beispiel einem grafischen Bildschirm in der Leitstelle) und Engineering-Komponenten (EK, engl. engineering station ES - zur Programmierung und Parametrierung der Komponenten)
Size-cap rule	Es besteht in der Anwendung einer Größenobergrenze, der alle mittleren und großen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission unterliegen. Diese Größenobergrenze wird gesenkt, so dass mehr Unternehmen der kritischen Infrastruktur den Regeln unterliegen.
Social Engineering	Social Engineering werden zwischenmenschliche Beeinflussungen mit dem Ziel genannt, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen.
Speicherprogrammierbare Steuerung	Ein Gerät, das zur Steuerung oder Regelung einer Maschine oder Anlage eingesetzt und auf digitaler Basis programmiert wird.
Technisch-Organisatorische Maßnahmen	Technisch-Organisatorische Maßnahmen, nach Art. 32 Datenschutz-Grundverordnung (DS-GVO) vorgeschriebene Maßnahmen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten.