Bad Oeynhausen

DVGW S&C

FiW

Kennziffer: IT-01/20-BO

ABSCHLUSSBERICHT

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

gefördert vom

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

Bezirksregierung Detmold

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 IT-Sicherheitsniveaus 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)

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erläuterung
AbwV	Abwasserverordnung
AWWA	American Water Works Association
B3S WA	Branchenspezifischer Sicherheitsstandard Wasser/Abwasser
BKM	Betriebskontinuitätsmanagement
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
DMZ	Demilitarisierte Zone
DSGVO	Datenschutzgrundverordnung
DVGW	Der Deutsche Verein des Gas- und Wasserfaches e. V.
DWA	Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e.V.
E	Einwohner
EGW	Einwohnergleichwerte
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
MBR	Membran Bio Reaktor
MFA	Multi-Faktor-Authentisierung
MNQ	Mittlerer Niedrigwasserabfluss
MQ	Mittlerer Abfluss
NAICS-System	North American Industry Classification System
OT	Steuerungstechnik (Operational Technology)
PLS	Prozessleitsystem
SBR	Sequencing Batch Reaktor
SCADA	Supervisory Control and Data Acquisition (zu Deutsch: Überwachung, Steuerung und Datenerfassung)
SPS	Speicherprogrammierbare Steuerung
SüwV-kom	Selbstüberwachungsverordnung kommunal
TOM	Technisch-Organisatorische Maßnahmen (z.B. DSGVO)

VPN	Virtual Private Network

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.
B3S WA - Architecture 1 - Dediziertes Netzwerk	Alle Netzwerk-und Kommunikations-Infrastruktur ist ausschließlich dem SCADA-System zugeordnet. (Maßnahmen: Netzwerksegmentierung).
B3S WA - Architecture 2 - Gemeinsame Nutzung des WAN mit anderen IT-Systemen	WAN-Kommunikationsinfrastruktur wird geteilt (mittels physischer (Medien) Trennung, VPN, VLAN, Firewall)
B3S WA - Architecture 3 - Gemeinsame Nutzung des LAN mit anderen IT-Systemen	LAN-Kommunikation (innerhalb der Anlage) wird geteilt (mittels VLAN, Firewall)
B3S WA - Architecture 4 - Servereinsatz	Für den Betrieb der Anlagen werden Client-Server- oder Web-Anwendungen eingesetzt, ebenfalls für die Desktop-Virtualisierung. Insbesondere bei der Client-Server-Anbindung sind auch die Clients in die Sicherheitsbetrachtungen einzubeziehen.
B3S WA - Infrastructure 1 - Infrastructurerastruktur	Gebäude, Serverräume und Schutzschränke müssen physisch geschützt werden
B3S WA - Network Management 1 - Lokales Netzwerkmanagement	Zugriff auf die Konfiguration der Netzwerk-Infrastruktur aus der unmittelbaren Umgebung des Benutzers (seriell oder Netzwerk).
B3S WA - Network Management 2 - Anlagenweites Netzwerkmanagement	Zugriff auf die Konfiguration der Netzwerkinfrastruktur am jeweiligen Standort (LAN Access)
B3S WA - Network Management 3 - Netzwerkmanagement über Remotezugriff (von anderem Standort aus)	Zugriff auf die Konfiguration der Netzwerk-Infrastruktur von einem anderen Standort aus.
B3S WA - Organizational Measures 1 - Interne Verantwortung für IT-Sicherheit	Das Unternehmen verantwortet den Einsatz und die Nutzung der IT-Systeme.

B3S WA - Program Access 1 - Automatisiertes Senden von Nachrichten	Automatisiertes, nicht-interaktives Versenden von SMTP, SMS oder anderen ausgehenden Alarmen und Meldungen durch das System.
B3S WA - Program Access 2 - Interaktives Senden von Dateien	Interaktives Versenden von Dateien aus dem System heraus an andere Standorte.
B3S WA - Program Access 3 - Interaktives Empfangen von Dateien	Interaktiver Empfang von Dateien von anderen Standorten in Richtung System.
B3S WA - Program Access 4 - Automatische Software-Updates	Automatisierter, nicht-interaktiver Abruf von Lizenzen, Betriebssystem-Updates, Anti-Virus-Signaturen und anderen Systemdaten von anderen Standorten in Richtung System.
B3S WA - Program Access 5 - Automatisierter Datenaustausch	Automatisierter, nicht-interaktiver Austausch von Daten (z.B. DB-zu-DB-Austausch, NTP oder andere externe Daten) mit Systemen von anderen Standorten aus. (Implizite Online/Vollzeit Verbindung.)
B3S WA - Program Access 6 - Automatisierte Netzwerk-Authentifizierung	Automatisierter, nicht interaktiver Austausch von Netzwerkverwaltungsdaten (z.B. syslog, SNMP-Traps, SNMP Polling) mit System(en) außerhalb des Systems. (Impliziert Vollzeit-Verbindung.)
B3S WA - Programming and Maintenance 1 - Lokale SPS Programmierung und Wartung	Zugang zur SPS-Programmierung aus der unmittelbaren Umgebung des Benutzers (seriell oder Netzwerk).
B3S WA - Programming and Maintenance 2 - SPS Programmierung und Wartung von zentraler Stelle auf der Anlage	Zugriff auf die SPS Programmierung auf derselben Anlage von zentraler Stelle (LAN Access)
B3S WA - Programming and Maintenance 3 - SPS Programmierung und Wartung über Fernzugriff (von anderem Standort aus)	Zugang zur SPS Programmierung von einem anderen Standort aus.
B3S WA - User Access 1 - Systemzugang (steuernd) im gesicherten Kontrollraum	Zugang zum System mit vollen Lese- und Schreibmöglichkeiten von der Warte aus (auf der Anlage, physisch gesichert).
B3S WA - User Access 2 - Systemzugang (steuernd) innerhalb der Anlage	Zugang zum System mit vollen Lese- und Schreibmöglichkeiten am Anlagenstandort, nicht physisch gesichert (z.B. in der Werkstatt).
B3S WA - User Access 3 - Remotesystemzugang (steuernd, von anderem Standort aus)	Zugang zum System [mit vollen Lese- und Schreibmöglichkeiten] von einem Standort außerhalb des Wartenbereichs und außerhalb des Anlagenstandortes aus.
B3S WA - User Access 4 - Remotezugang (lesend, von anderem Standort aus)	Zugang zum System mit begrenzten „Nur-Lese"-Möglichkeiten von einem Standort außerhalb des Wartenbereichs und außerhalb des Anlagenstandortes aus.
B3S WA - User Access 5 - Webzugang (lesend)	Zugriff auf Web-Anzeigen von Systemdaten mit begrenzten „Nur-Lese"-Möglichkeiten von einem Standort außerhalb des Wartenbereichs und außerhalb des Anlagenstandortes aus.
B3S WA Anlagentypen	Kanalisation, Kläranlage, Leitzentrale, Trinkwassergewinnungsanlage, Wasserwerk Trinkwasseraufbereitungsanlage, Wasserverteilsysteme
BIA - Business Impact Analysis	Business-Impact-Analyse (BIA) ist eine Methode zur Sammlung und Identifizierung von Prozessen und Funktionen innerhalb einer Organisation, um

	die den Prozessen zugrundeliegenden Ressourcen zu erfassen.
Betriebskontinuitätsmanagement (Business Continuity Management)	Bezeichnet in der Betriebswirtschaftslehre die Entwicklung von Strategien, Plänen und Handlungen, um Tätigkeiten oder Prozesse – deren Unterbrechung der Organisation oder dem Gemeinwesen ernsthafte Schäden oder vernichtende Verluste zufügen würden (etwa Betriebsstörungen) – zu schützen bzw. alternative Abläufe zu ermöglichen.
Demilitarisierte Zone	Bezeichnet ein Computernetz mit sicherheitstechnisch kontrollierten Zugriffsmöglichkeiten auf die daran angeschlossenen Server. Die in der DMZ aufgestellten Systeme werden durch eine oder mehrere Firewalls gegen andere Netze (z. B. Internet, LAN) abgeschirmt. Durch diese Trennung kann der Zugriff auf öffentlich erreichbare Dienste (mit z. B. E-Mail, WWW o. ä.) gestattet und gleichzeitig das interne Netz (LAN) vor unberechtigten Zugriffen von außen geschützt werden. Der Sinn besteht darin, auf möglichst sicherer Basis Dienste des Rechnerverbundes sowohl dem WAN (Internet) als auch dem LAN (Intranet) zur Verfügung zu stellen.
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.
North American Industry Classification System	Klassifikationssystem zur Klassifizierung von Unternehmen nach der Art ihrer ökonomischen Aktivitäten bzw. ihres Produktionsprozesses. In der EU wird NACE Revision 2 – Statistische Systematik der Wirtschaftszweige, verwendet.

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.
SNORT	Snort ist ein freies Network Intrusion Detection System (NIDS) und ein Network Intrusion Prevention System (NIPS). Es kann zum Protokollieren von IP-Paketen genauso wie zur Analyse von Datenverkehr in IP-Netzwerken in Echtzeit eingesetzt werden. Die Software wird überwiegend als Intrusion-Prevention-Lösung eingesetzt, um Angriffe unmittelbar ereignisgesteuert automatisch zu blockieren.
Social Engineering	Social Engineering werden zwischenmenschliche Beeinflussungen genannt, mit dem Ziel, 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.
Virtualisierung	Virtualisierung bezeichnet in der Informatik die Nachbildung physischer Objekte als virtuelle (d. h. nicht-physische) Geräte oder Dienste wie emulierte Hardware, Betriebssysteme, Datenspeicher oder Netzwerk-ressourcen.
Virtual Private Network	Auf einer öffentlichen technischen Infrastruktur wird durch Verschlüsselung ein „privates" logisches Netzwerk abgebildet, das nicht abhörbar ist.
Zero Trust Sicherheitsmodell	Das Zero-Trust-Sicherheitsmodell (auch Zero-Trust-Architektur, Zero-Trust-Netzwerkarchitektur, ZTA, ZTNA), manchmal auch als perimeterlose Sicherheit bezeichnet, beschreibt einen Ansatz für das Design und die Implementierung von IT-Systemen. Das Hauptkonzept hinter Zero Trust ist „niemals vertrauen, immer überprüfen“, was bedeutet, dass Geräten standardmäßig nicht vertraut werden sollte, selbst wenn sie mit einem verwalteten Unternehmensnetzwerk wie dem Unternehmens-LAN verbunden sind.

1. Einleitung

Das IT-Sicherheitsgesetz 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. Es rückte ins allgemeine Bewusstsein, dass diese Technik aus dem Internet angreifbar ist, zu leicht angreifbar ist. Viele Anlagenverantwortliche hatten zur Zeit der Verabschiedung des Gesetzes offenbar keine hinreichenden Maßnahmen ergriffen, um solchen Angriffsmöglichkeiten entgegenzuwirken.

Die Einführung neuer staatlicher Regeln sollte immer mit Blick auf die Auswirkungen für die Betroffenen und die Aufsichtsbehörden geschehen. Beide müssen in der Lage sein, die Anforderungen an die Ziele in den geforderten Zeiten umzusetzen. Deshalb hat 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) Schwellenwerte aufgenommen, die aus dem Katastrophen- und Bevölkerungsschutz kommen. Kritisch ist, was mindestens 500.000 Einwohner betrifft. Wenn es um die Festlegung von Schwellenwerten geht, kann aus der Einwohnerzahl abgeleitet werden, wieviel Trinkwasser 500.000 Menschen benötigen, wieviel Abwasser sie erzeugen, wieviel Energie sie benötigen, welche Bankinfrastruktur notwendig ist, wie ihre Lebensmittelversorgung sichergestellt werden kann oder welche Krankenhauskapazitäten vorhanden sein müssen. Alle Infrastruktur, die oberhalb der abgeleiteten Schwellwerte lag, wurde zu Maßnahmen zur Steigerung der Informationssicherheit verpflichtet.

Auch wenn das Gesetz es vermieden hat, die Maßnahmen selbst festzulegen oder zu detailreich zu beschreiben, so wurde den betroffenen Branchen die Möglichkeit eröffnet, sich selbst Regelwerke für Informationssicherheit zu geben und in Abstimmung mit dem BSI anzuwenden. Die Idee dahinter ist, dass die Betroffenen selbst am besten wissen, welche Maßnahmen wie umgesetzt werden müssen, ohne durch den Zwang zu weitreichenden Maßnahmen über das Ziel hinauszuschießen. Mit dem Blick in andere Länder hat eine gemeinsame Arbeitsgruppe der DWA und des DVGW eine Lösung auf Basis einer Grundlage der American Water Works Association (AWWA) erarbeitet.

Dieser basiert auf dem BSI-Grundschutz, dem IT-Sicherheitsregelwerk des Bundes. Der Grundschutz wurde bereits 1994 erstmals unter diesem Namen veröffentlicht und seither immer weiterentwickelt. Das Regelwerk für die Deutsche Wasserwirtschaft ist der

Branchen**S**pezifische **S**icherheits**S**tandard Wasser/Abwasser (B3S WA). Seine Eignung für den Anwendungszweck wurde vom BSI nach §8a Abs. 2 BSIG erstmals am 26. Juni 2017 festgestellt (Die aktuelle Version B3S WA v.3 ist mit Datum vom 21.01.2022 eignungsfestgestellt). 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. Zu unterscheiden sind die allgemeinen Anforderungen, die jedes Unternehmen der Wasserwirtschaft erfüllen sollte und Anforderungen für die kritische Infrastruktur, die darüber hinausgehen und für Betriebe der kritischen Infrastruktur angewendet werden müssen, um den Stand der Technik vollständig implementiert zu haben.

Auf Grundlage des im Untersuchungszeitraum gültigen B3S WA v.2 wurden im Rahmen des Projektes subKRITIS - Bestandsaufnahme des IT-Sicherheitsniveaus 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.

2. Hintergrund / Stand des Wissens

Allgemeine Aussagen zur **Häufigkeit und der Art von Angriffen auf Kläranlagen** sind aus öffentlich zugänglichen Daten nicht zu treffen, weil schlichtweg zu wenige Daten öffentlich werden. Grundsätzliche Aussagen finden sich z.B. in Verizons Data Breach Investigations Report 2021 (Verizon, 2021). Dies ist eine Untersuchung basierend auf Daten von 78 Institutionen, darunter Virenschutzhersteller, Suchmaschinen für Industriesteuerungen, Polizeieinheiten, Universitären Einrichtungen und CERTs[1]. Untersucht wurden fast 80.000 Vorfälle aus dem Jahr 2020. Die Vorfälle wurden dann nach dem NAICS-System (North American Industry Classification System) klassifiziert. Die Auswertungen fassen die Gewinnung von Bodenschätzen, die Energiegewinnung sowie Abwasser/ Wasser zusammen. Das ist zwar nicht sehr spezifisch für den Abwasserbereich, trotzdem sind die Ableitungen interessant. Untersucht wurden 546 Vorfälle, in 355 Fällen wurden tatsächlich Daten von den Anlagen abgeleitet. Die Angriffe wurden zu 98 % per Social Engineering, direktes Eindringen in die Systeme sowie das Knacken von Websites vorgenommen. Die Angreifer waren in 98 % der Fälle Externe, bei 2 % Interne. Die Motivation der Angreifer war überwiegend finanzieller Natur (>78 %), teils ging es aber auch um Spionage. Für die Angriffe wurden zu 94 % Zugriffsdaten von Mitarbeitern benutzt, die also ganz offensichtlich zu schwach gewählt oder öffentlich bekannt waren, ggfs. auch durch Phishing. Es wurde nicht unterschieden, ob die Office-IT der Anlagen oder die Steuerungstechnik kompromittiert wurde.

Tabelle *2*-1: Bericht über die Untersuchung von Datenverletzungen *(Verizon, 2021)*

Häufigkeiten	546 Vorfälle, davon 355 mit bestätigten Datenlecks
Verbreitete Angriffs- und Vorfallsmuster	98 % der erfassten Sicherheitsverletzungen entfallen auf die Kategorien „Social Engineering“, „Systeminfiltration“ und „Einfache Angriffe auf Web-Anwendungen“.
Urheber der Bedrohungen	Extern (98 %), intern (2 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Motive der Angreifer	Habgier (78-100 %), Spionage (0-33 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Betroffene Daten	Anmeldedaten (94 %), Personenbezogene Daten (7 %), Interna (3 %), Sonstige (3 %) – gemessen an der Gesamtzahl der Sicherheitsverletzungen
Empfohlene Abwehr-maßnahmen	Schulungen zur Steigerung des Sicherheitsbewusstseins (14 %), Zugangskontrolle (6 %), Management von Nutzerkonten (5 %)

[1] Computer Emergency Response Team

Die allgemeinen Empfehlungen des Verizon Berichtes sind:

- Das Sicherheitsbewusstsein der Mitarbeiter der Anlagen muss verbessert werden (Sicherheit hängt von jedem Einzelnen ab)
- Die Mitarbeiter müssen besser unterwiesen werden
- Das Zugriffsmanagement muss verbessert werden (z.B. Zugriff nur während der Dienstzeit, Zugriff von außen nur mit Multi-Faktor-Authentisierung, mit unzulässigen Geräten etc.)
- Die Kontenverwaltung ist zu verbessern (Eintritt ins Unternehmen, Kündigung, Externe).

2.1. Stand der IT-Technik allgemein

Um eine sichere Basis zur Beurteilung zu bekommen, ob die eigene IT und Steuerungstechnik dem Stand der Technik entspricht, können von Betreibern oder Verbänden nach BSIG § 8 Abs. 2 B3S verfasst und dem BSI zur Feststellung der Eignung vorgelegt werden. Wenn ein Standard wie der B3S Wasser/Abwasser (WA) zusätzlich auf dem IT-Grundschutz-Kompendium aufsetzt, wird auch durch die Anforderungen in dessen Bausteinen die Einhaltung des Standes der Technik sichergestellt. Das Grundschutz-Kompendium wird jährlich im Februar in einer neuen Edition veröffentlicht, der B3S WA zweijährlich überarbeitet (Basis ist BSIG § 8 Abs. 3). Der schnellen technischen Entwicklung im IT-Bereich wird dadurch Rechnung getragen. Der B3S WA wird von einem Projektkreis im Gemeinsamen Technischen Komitee „IT-Sicherheit“ des DVGW in Zusammenarbeit mit der DWA-Arbeitsgruppe „Cyber-Sicherheit“ erarbeitet und in Abstimmung mit dem BSI erstellt.

Als Grundlage der Untersuchungen im Rahmen des subKRITIS-Projekts diente der im Jahr 2021 gültige B3S WA in der Version 2. Unter Verwendung dieses Standards kann sichergestellt werden, dass die Untersuchungen nach dem aktuellen Stand der Technik vorgenommen wurden.

2.2. Stand der IT-Technik auf Kläranlagen

Die Projektbeteiligten verfügen über Erfahrungen aus der Betreuung, Besichtigung und Bewertung anderer Anlagen der kritischen Infrastruktur, wie bspw. der Wasserversorgung. Die auf anderen Anlagen der kritischen Infrastruktur außerhalb der hier im Projekt betrachteten Anlagen verwendete Operational Technology (OT/Steuerungstechnik), z.B. der Hersteller SIEMENS AG, WAGO GmbH & Co. KG, Phoenix Contact GmbH & Co. KG, ist ebenfalls vielfach älter, die Installations- und Nutzungszeiträume erstrecken sich über mindestens 20 Jahre. Der Begriff alt ist bei Industriesteuerungen relativ, weil der Nutzungszeitraum der Technik sich durchaus über 30 Jahre erstrecken kann. Beispielsweise wurde die Siemens S7 Steuerung 1994 auf den Markt gebracht und seither ständig weiterentwickelt. Insofern repräsentiert die vorgefundene Steuerungstechnik einen erwartbaren Stand

unterschiedlichster Technikgenerationen. Allerdings ist darauf hinzuweisen, dass diese Steuerungen, auch nicht indirekt über eine Leitstelle, mit dem Internet verbunden sein dürfen, wenn sie nicht generell oder mit aktuellen Patches angriffssicher gemacht werden können. Die auf den besichtigen Kläranlagen verwendete Informationstechnik (IT), z.B. Fritzboxen, PCs und Laptops, wies einen in Bezug auf diese IT altersgerechten Zustand auf, der üblicherweise einen Nutzungszeitraum von 5 Jahren umfasst. Die vorgefundene Netztechnik, Router/ Switches waren ebenfalls auf dem Stand der Technik. Teilweise wurden auf den Anlagen bereits Glasfaserringe vorgefunden. Jedoch wurde schon zu Beginn festgestellt, dass die Notstromversorgung teilweise unzulänglich, nur sehr eingeschränkt funktionstüchtig oder gar nicht vorhanden ist. Auch die Versorgung mit Kraftstoff für die Generatoren ist häufig nur für einen kurzen Zeitraum sicher. Es ist sinnvoll dazu die beiden folgenden Publikationen des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe zu berücksichtigen:

1. PiB-13-notstromversorgung-unternehmen-behoerden.pdf (bund.de)

2. Treibstoffversorgung bei Stromausfall (bund.de)

Eine ausführliche Darstellung der technischen Ausstattungen sowie IT-Ausrüstungen und aktuellen Entwicklungen in der auf Kläranlagen eingesetzten IT wurde in den Einzelberichten an die jeweiligen Anlagenbetreiber gegeben.

2.3. Verwendete Technik auf den untersuchten Kläranlagen

Um die Auswirkungen der IT-Technik auf die Abwasserreinigung zu bestimmen, muss untersucht werden, welche Aggregate verwendet werden und eine Angriffsoberfläche bieten. Generell können alle Aggregate durch einen Cyberangriff betätigt werden, die an von außen erreichbare IT-Netze bzw. das Prozessleitsystem angeschlossen sind. Dazu gehören: Schieber, Pumpen, Schnecken, Messequipment, Belüfter und Räumer. Diese Aggregate können teilweise nur elektrisch, nur händisch (in diesem Fall kein Anschluss an das Prozessleitsystem und keine Angriffsmöglichkeit über das Internet) oder auf beiden Wegen betrieben werden. Zusätzlich werden auch einige Aggregate halbautomatisch betrieben. In diesem Fall sind die Aggregate zwar vom Strom abhängig, werden aber nicht über das Prozessleitsystem (PLS) geregelt, sondern vom Kläranlagenpersonal in und außer Betrieb genommen. Wie welches Aggregat in welcher Verfahrensstufe auf welcher Kläranlage betrieben wird, kann für die meisten Fälle nicht allgemein bestimmt werden. In Tabelle 2-2 ist dazu die verbaute elektrische Technik sortiert nach Verfahrensstufen gelistet.

Tabelle 2-2: Verfahrensstufen differenziert nach der verbauten Technik auf den untersuchten 13 Kläranlagen, die eine elektrische Stromversorgung haben.

Verfahrensstufe	Verbaute Technik	Anzahl Aggregate mit Stromversorgung
Zulauf	Pumpwerk	12
	Messsonde	11
Rechen	Räumer	13
	Messsonde	13
Sand- und Fettfang	Belüftung	13
	Sandabzug	13
Vorklärung	Räumer	7
	Schlammabzug	7
Zwischenpumpwerk	Pumpwerk	9
Belebung	Belüfter	13
	C-Dosierung	4
	Messsonden	12
	Rezirkulation	5
	Rührwerk	13
Phosphor-Elimination	Messonden	11
	Dosierpumpe	13
Nachklärung	Räumer	12
	Schlammabzug	13
	Schlammrückführpumpwerk	12
	Dekanter	1
Erweiterte Reinigung	Pumpwerke	5
	Rückspülung	5
	C-Dosierung	1
	Elektrische Schieber	3

In der Tabelle ist zu sehen, dass es einige wenige Aggregate mit Stromversorgung gibt, die auf allen 13 Kläranlagen vorhanden sind. Dazu gehören Rechen, Sandfang, Belüftung, Rührwerke, Schlammabzüge und Fällmittel-Dosierpumpen. Aber auch bei diesen Aggregaten fallen die Steuerungen unterschiedlich aus und haben nicht immer eine IT-Anbindung. Insbesondere Rechen und Sandfänge werden teilweise halbautomatisch gesteuert. Ebenso werden einige Phosphor-Eliminationen über fest eingestellte Werte lokal betrieben und sind nicht über die IT beeinflussbar. Dies zeigt, dass über einen Cyberangriff nicht überall derselbe Einfluss gewonnen werden kann und somit die Konsequenzen für jede Kläranlage einzeln bewertet werden müssen.

Die größte Vielfalt existiert bei Schiebern. Schieber sind auf jeder Anlage zumeist vor und hinter Aggregaten zu finden. Dabei existieren Handschieber, elektrische Schieber ohne

Handsteuerung und elektrische Schieber mit Handsteuerung. Zudem sind einige Handschieber nicht fest verbaut, sondern werden eingeschoben. Auf Grund dieser großen Vielfalt wurden die Schieber nicht mit in die Liste aufgenommen. Auf jeder Kläranlage sind aber Schieber mit IT-Anbindung vorhanden.

Allgemeingültige Aussagen zu Schutzmaßnahmen an vorwiegend eingesetzten Prozessleitsystemen sind wegen der Heterogenität der verwendeten Systeme nicht zu treffen. Üblicherweise sind solche Systeme basierend auf Datenbanksystemen, Logik- und Anzeigeschichten aufgebaut, die gemeinsam oder einzeln virtualisiert und gesichert sein können. In aller Regel ist für diese Systeme und die damit verarbeiteten Daten ein regelmäßig erstelltes Backup und dessen Rückspielen zur Funktionsprüfung die wichtigste Sicherheitsmaßnahme. Die Sicherheit des Netzsegmentes, in dem die Leitstellensoftware betrieben wird, wird durch Firewalls gewährleistet. Diese sind üblicherweise zweistufig mit dazwischen liegender Demilitarisierter Zone (DMZ) vorzusehen, also mit außenliegender Firewall, dann der demilitarisierten Zone und innenliegender Firewall. Auf den untersuchten Kläranlagen war der Absicherungsaufwand auf eine Firewall ohne DMZ und zweite Firewall beschränkt.

Zu erwarten ist für die auf den Anlagen verwendeten IT-Komponenten wie Router und PCs als Arbeitsplatzrechner oder Server, dass sie maximal 5 Jahre alt sind. Danach werden solche Komponenten ersetzt. Zu erwarten ist weiter, dass die Steuerungen der Anlagen bis über 30 Jahre alt sein können. Steuerungen sind für einen solchen Langzeit- und Dauerbetrieb ausgelegt. Sie sind zudem zwischen verschiedenen Generationen kompatibel. Die Anlagen können zwar im Kern einige Jahrzehnte alt sein, werden aber bei Bedarf überarbeitet oder ergänzt und die neu hinzugekommen Anlagenteile mit neuen Steuerungen versehen. Das kann auch Steuerungen unterschiedlicher Hersteller einschließen. Diese pragmatischen Erwartungen zeigten sich überall erfüllt.

Potentielle Schwachstellen der Informationssicherheit zeigen sich, wenn der Zutritt zu den Geräten nicht gesichert ist oder der Zugang zum Steuerungsnetz aus dem Internet offensteht. Im ersten Fall ist der Zutritt zu unterbinden, indem Anlagenteile verschlossen sind bzw. vollständig in geschlossenen Räumen betrieben werden. Dies ist nicht immer vollumfänglich möglich, weil beispielsweise Not-Aus Schalter zur Personensicherung an vielen Stellen vorgeschrieben sind und nicht verschlossen sein können, wenn sie ihren Zweck erfüllen sollen. Ein ungehinderter Zugang aus dem Internet würde die Steuerungsnetze Angriffen aussetzen. Da viele Steuerungen gar keine Sicherheitsfunktionen enthalten, wäre dies fatal, selbst dann, wenn die Anlagen stets durch Patches auf neuestem Softwarestand gehalten würden. Der Zugang muss also durch Netztrennung, Firewalls und/oder Zeitsteuerungskonzepte für Zugänge aus dem Internet gesichert sein.

3. Bestandsaufnahme

Die Bestandsaufnahme wird in zwei Teile aufgeteilt. Dabei wird zwischen Erkenntnissen auf der wasserwirtschaftlichen Seite und auf der IT-technischen Seite unterschieden. Beide Teile werden dazu zunächst unabhängig betrachtet und einzeln bewertet. Auf der wasserwirtschaftlichen Seite wird betrachtet, welche Folgen aus dem abwassertechnischen Aufbau der Kläranlagen entstehen können. Auf der IT-technischen Seite wird betrachtet, welche Schwachstellen auf den Kläranlagen vorhanden sind, welche eine Intrusion ins System ermöglichen könnten. Auf Basis der Erkenntnisse aus beiden Bereichen können die Ergebnisse verbunden werden, um zu ermitteln, welche Folgen aus den Schwachstellen resultieren können.

3.1. Prozessverständnis der wasserwirtschaftlichen Komponenten der Kläranlagen

Für das Prozessverständnis der einzelnen Kläranlagen wurden Begehungen und Befragungen durchgeführt. Das Vorgehen dabei wird im nachfolgenden Unterkapitel erläutert. Anschließend ist eine Betrachtung der Repräsentativität für die Einordnung der Kläranlagen in den Kontext aller Kläranlagen in NRW dargestellt.

3.1.1. Vorgehen

Bereits vor der Besichtigung der Kläranlagen wurden Datenabfragen an die Betreiber gestellt und - wenn vorhanden - das auf Webseiten von Kläranlagen zur Verfügung gestellte Informationsmaterial genutzt, um die Befragenden mit Fragestellungen auf die jeweils aufgebauten Verfahrensarten vorzubereiten. Auf den Kläranlagen wurde anschließend zunächst eine Begehung des Wasserweges durchgeführt. Für die Begehungen werden drei verschiedene Schadensarten betrachtet, welche potenziell auf den Kläranlagen ausgelöst werden könnten:

- Monetärer Schaden für Betreiber
    - Was muss verändert werden, damit es zu einer Überschreitung der Ablaufwerte kommt?
    - Beispiel einer Kläranlage: Räumer des Nachklärbeckens fällt im Winter aus, wodurch Schlammabtriebe folgen. Daraus resultierend wird eine Abwasserabgabenerhöhung von 1.5 Mio. € fällig.
- Umweltschaden
    - Eine Abwasserverunreinigung kann als Strafbestand nach StGB §324 gewertet werden.
    - Ökologische Schäden in Fließ- und Standgewässern erzeugbar.

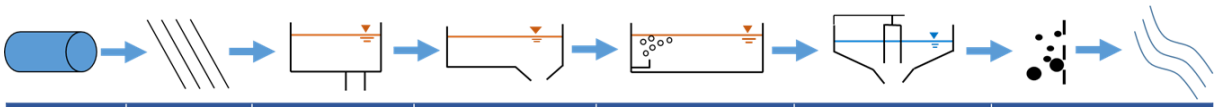
    - Möglicherweise können flussabwärts gelegene Wassernutzungen beeinträchtigt werden.
- Sachschäden
    - Überflutungen angrenzender (vor- und nachgeschalter) Infrastruktur, Siedlungen oder auf der Anlage.
    - Eine mutwillige Zerstörung von Anlagenteilen wurde vernachlässigt.

Im Wesentlichen werden drei Angriffsmöglichkeiten als relevant betrachtet: Physischer Angriff, Cyberangriff und ein Stromausfall. Für alle drei Angriffsarten muss auf verschiedene Punkte geachtet werden. Dabei wurde auf die folgenden Aspekte geachtet und Fragen zu den folgenden Themen gestellt:

- Allgemeine Sicherheit:
    - Abgeschlossene Türen, steckende Schlüssel, Zeiten ohne Personal und Begehung der Kläranlage (unbesetzte Kläranlage), Alarmsysteme, Videoüberwachung, …
- Physische Eingriffsmöglichkeiten:
    - Handschieber, Knöpfe, ungesicherte Bedienelemente, …
- Cyberangriff:
    - Begutachtung der Leitstelle und Leitstellensoftware, von regulierbaren Aggregaten: Belüfter, Messequipment, Rührwerke, Pumpen, …
- Stromausfall:
    - Notstromaggregate, „Blackouttests“, Rückhalt von Kraftstoffen.

Für jeden dieser Aspekte wurde an den jeweils relevanten Verfahrensstufen eine Bewertung durchgeführt. Durch das Personal konnten dabei ausführliche Informationen zu den jeweiligen Steuerungen/ Regelungen und dem Alarmsystem gegeben werden.

Durch den individuellen Aufbau jeder Kläranlage unterscheiden sich die betrachteten Stellen deutlich, wobei es einige Aspekte gibt, die auf jeder Kläranlage gleich untersucht werden konnten. Eine Betrachtung des Schlammweges wurde im Rahmen dieses Projektes zunächst vernachlässigt. Hier wären in Zukunft weitere Betrachtungen sinnvoll, da beispielswese durch die Störung der anaeroben Biozönose im Fermenter langfristige Auswirkungen auf Kläranlagen möglich sind. Beispielhafte Angriffsmöglichkeiten sind in Abbildung 3-1 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 3-1: Beispielhafte Angriffsszenarien auf eine Kläranlage. (eigene Darstellung)

Im Anschluss der örtlichen Begehung wurde die Besichtigung mit einem Interview fortgeführt. Ziel war es, weitere Informationen zu möglicherweise nicht vorhandenen Daten zu erhalten, welche im Rahmen der Kläranlagen-Angriffssimulation notwendig sind. Dies umfasst unter anderem Volumina und Tiefen von Becken, Zu- und Ablaufwerte, Überwachungswerte oder die Regelung von einzelnen Aggregaten. Weiterhin wurden Informationen zu vergangenen Problemen auf der Anlage abgefragt, analysiert und für die weitere Auswertung verwendet. Dies beinhaltet bereits beobachtete Angriffe, Stromausfälle oder sonstige Störungen, die auf den Anlagen aufgefallen sind und was daraus resultierend auf der Anlage unternommen wird, beispielsweise durch eine Anpassung der Kontrolluntersuchungen an Wochenenden.

3.1.2. Repräsentativität

Im Projekt subKRITIS wurden insgesamt 13 kommunale Kläranlagen untersucht. Mit diesem Status-Quo (Stand 31.12.2018) wurde ein erster Überblick der Situation auf den insgesamt 599 Kläranlagen in ganz Nordrhein-Westfalen (NRW) erarbeitet. Daher müssen die Kläranlagen auf verschiedene Eigenschaften verglichen werden, um einen Kontext und eine Übertragbarkeit zu den restlichen Anlagen in NRW herzustellen. Die abgeglichenen Eigenschaften/ Informationen sind die Größenklassen (GK) nach Abwasserverordnung (AbwV), die Anschlussgrößenbereiche, die Einwohnergleichwerte (EGW), die Auslastung der Kläranlagen und die Art der Belebung (IT.NRW, 2021).

Kommunale Kläranlagen

Die Größenklassen nach der Abwasserverordnung (AbwV) richten sich nach der Ausbaugröße und sind in 5 Größenklassen geteilt. Die erste Klasse umfasst die Ausbaugröße < 1.000 Einwohnerwerte (EW), Klasse zwei umfasst 1.000 EW bis 5.000 EW, Klasse drei von 5.001 EW bis 10.000 EW, die vierte Klasse beinhaltet alle Kläranlagen von 10.001 EW bis 100.000 EW und die letzte Klasse 5 umfasst alle Kläranlagen > 100.000 EW. In der nachfolgenden Abbildung 3-2 ist die Verteilung der Größenklasse der Kläranlagen in NRW (blau) und die der untersuchten Kläranlagen (orange) dargestellt.

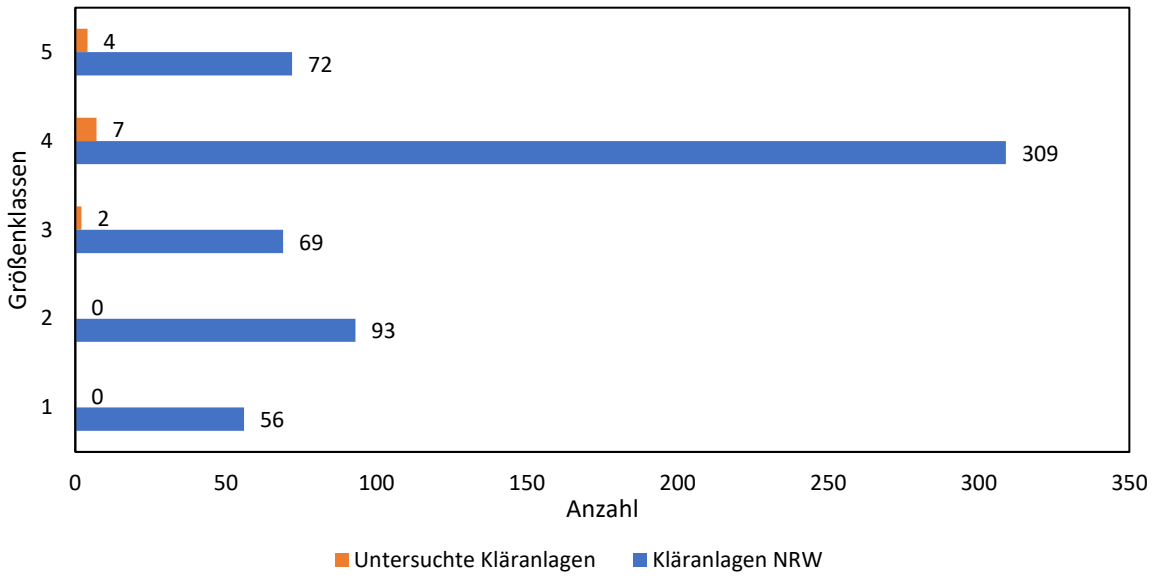


Abbildung 3-2: Vergleich der Größenklassen basierend auf *ELWAS-Web*.

Da die Größenklassen 1 und 2, bei den 13 von insgesamt 599 betrachteten Kläranlagen, nicht berücksichtigt werden und damit einhergehend die Größenklasse 5 stärker repräsentiert wird, sind Aussagen zu allen Kläranlagen nur mit den untersuchten Kläranlagen bedingt repräsentativ. Von den Kläranlagen der GK 5 fallen 10 Kläranlagen nach der Ausbaugröße unter die KritisV. Somit sind 62 Kläranlagen für die Auswertung unterhalb der Kritis in GK 5 relevant. Eine weitere Größenklasse an Kläranlagen, die Kleinkläranlagen, wird ebenfalls nicht berücksichtigt. Darauf wird im weiteren Verlauf des Berichtes genauer eingegangen.

Abbildung 3-3 zeigt den Vergleich der Kläranlagen bezüglich des Anschlussgrößenbereichs. Dieser ist ein Vergleichswert, für die in den Abwässern enthaltenden Schmutzfrachten. Es kann entnommen werden, dass bis auf den Anschlussbereich < 1.000 EW alle Bereiche bei den untersuchten Kläranlagen berücksichtigt werden.

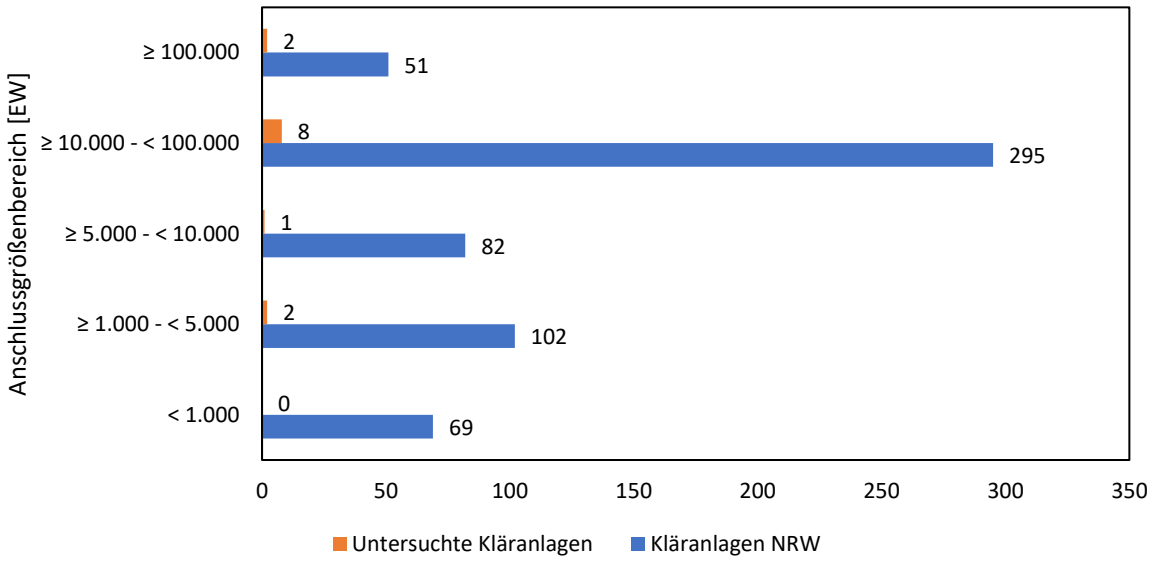


Abbildung 3-3: Vergleich der Anschlussgrößen basierend auf *ELWAS-Web*.

In Abbildung 3-4 können der Anteil der Einwohnergleichwerte (EGW, industrielle Abwasseranteile) an der Anschlussgröße für alle Kläranlagen in NRW und für die untersuchten Kläranlagen entnommen werden. Industrielles Abwasser kann potentiell höhere Frachten an umweltgefährdenden Stoffen beinhalten. Somit könnten. Der Anteil stellt dar wie hoch der industrielle Abwasseranteil an einer Kläranlage ist. Je höher der prozentuale Anteil ist, desto höher ist - in Abhängigkeit von der Art der relevanten Einleitungen - das Risiko, einer relevanten Gewässerverschmutzung im Falle eines Anlagenausfalls.

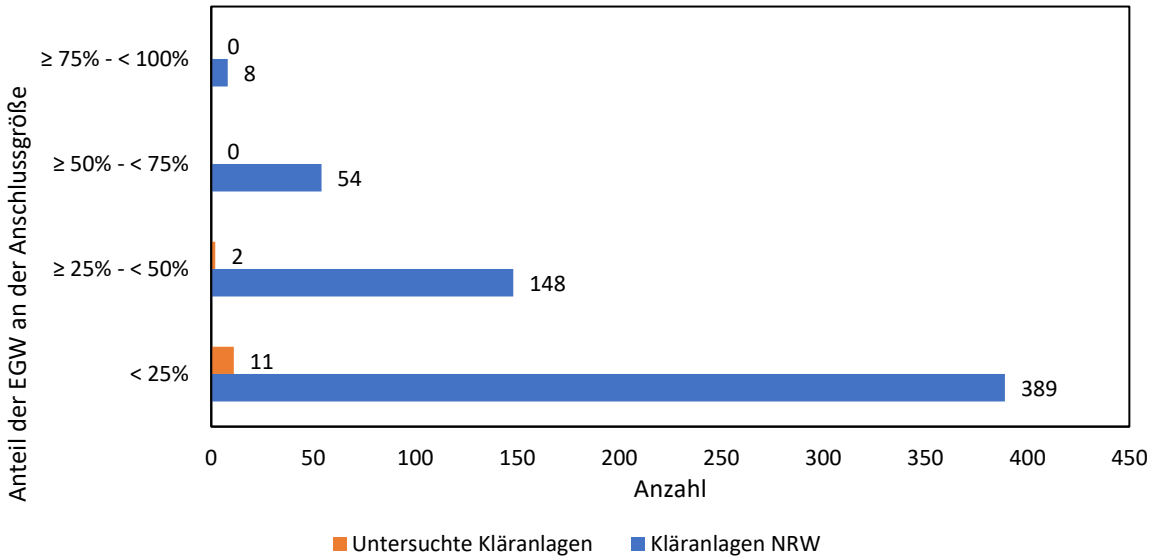


Abbildung 3-4: Vergleich des Anteiles der Einwohnergleichwerte an der Anschlussgröße basierend auf *ELWAS-Web*.

Wie in der Grafik zu sehen ist, werden Kläranlagen mit Anteilen von ≥ 50 % bisher nicht untersucht. Für die Meisten Kläranlagen liegen wie für die untersuchten geringere Anteile vor.

Die Auslastung [%] aller Kläranlagen (Quotient aus Anschlussgröße und Ausbaugröße) in NRW ist in Abbildung 3-5 in blau dargestellt, wohingegen die Auslastung der untersuchten Kläranlagen in orange dargestellt ist.

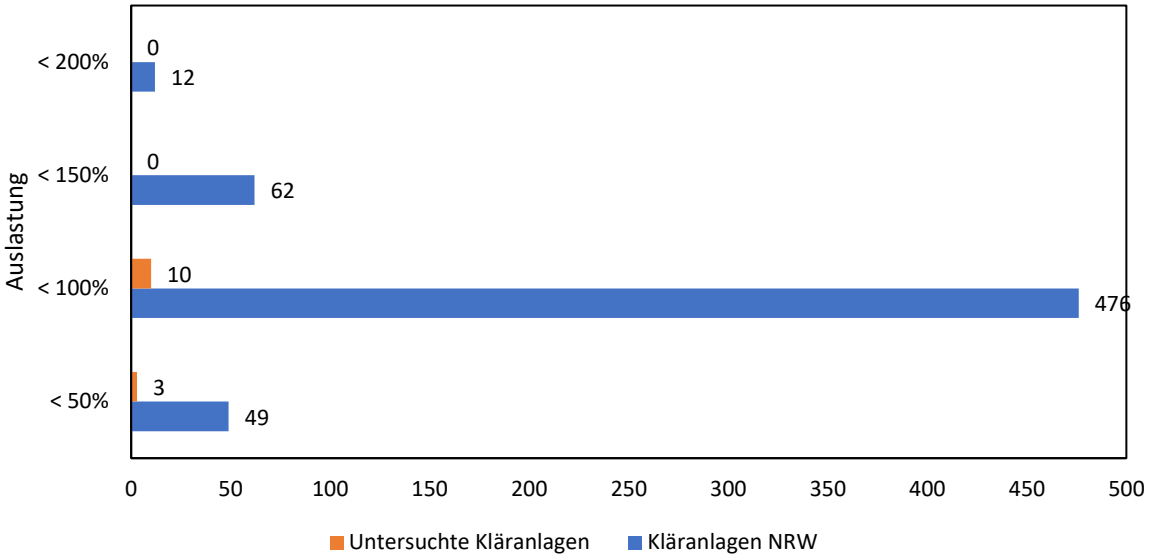


Abbildung 3-5: Vergleich der Auslastung basierend auf *ELWAS-Web*.

Anhand Abbildung 3-5 wird deutlich, dass die untersuchten Kläranlagen nur bedingt repräsentativ sind. Es zeigt sich, dass keine Kläranlagen betrachtet wurden, welche laut den *ELWAS*-Daten eine Auslastung von größer 100 % haben. (MULNV NRW, 2022) Problematisch ist bei diesen Kläranlagen, dass diese tendenziell eine höhere Anfälligkeit gegenüber Angriffen haben, da das Pufferpotenzial gegenüber Veränderung in der Reinigung der Anlage kleiner ausfällt. Auf den Einfluss der Auslastung auf die Anfälligkeit wird in Kapitel 4.1 genauer eingegangen. Im Schnitt weisen die Kläranlagen laut den ELWAS-Web Daten eine Auslastung von 78 % auf. Nach Daten des DWA-Leistungsnachweises 2018 liegt die Auslastung im Schnitt in NRW bei 68 % (DWA, 2019). Insgesamt zeigen die untersuchten Kläranlagen auch teilweise in den *ELWAS*-Daten höhere Auslastungen als in der Realität. Aufgrund der teilweise veralteten Daten in *ELWAS* ist die Plausibilität der hohen Auslastungen kritisch zu sehen. Hier wird vermutet, dass eine nicht aktualisierte Ausbaugröße im Einleiterkataster ELKA vereinzelt vorliegt.

Abbildung 3-6 stellt die Verteilung der Art der Denitrifikation für alle 599 kommunalen Kläranlagen in NRW dar.

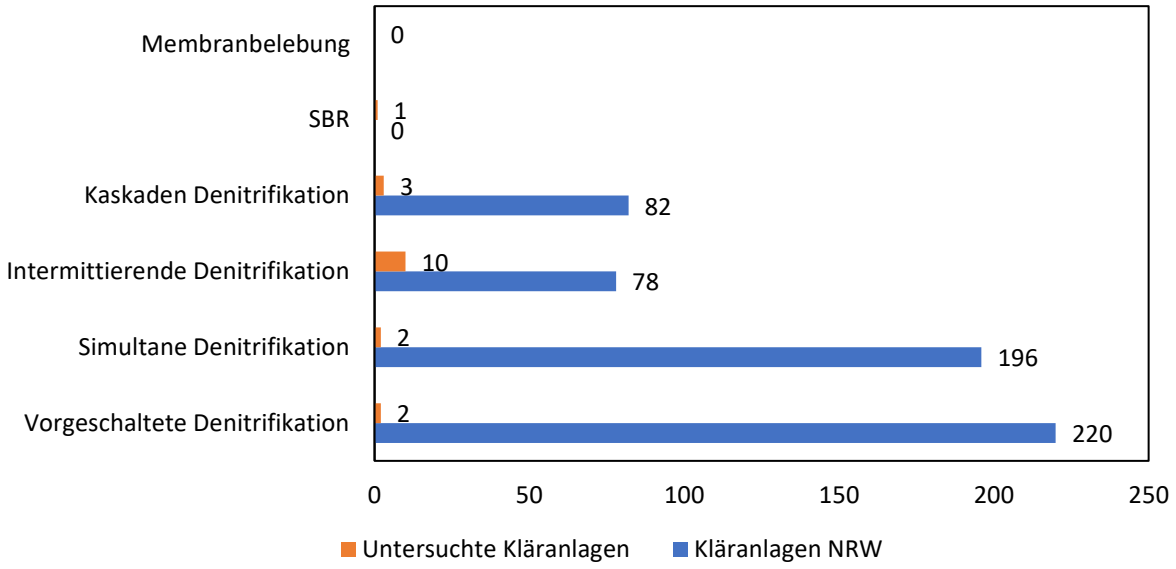


Abbildung 3-6: Vergleich der Verfahrenstechnik basierend auf *ELWAS-Web*.

Anhand Abbildung 3-6 wird deutlich, dass alle Arten der Denitrifikation bei den untersuchten Kläranlagen berücksichtigt werden. Die Datenlage ist hier nicht ganz korrekt, da der Unterschied zwischen intermittierender und simultaner Denitrifikation in *ELWAS* nicht immer korrekt erfasst wurde. Weiterhin können weitere Verfahrenstechniken genutzt werden, deren Anwendung aus den Daten nicht klar wird. Dazu gehört einerseits der Betrieb als Sequencing Batch Reaktor (SBR), eine dieser Kläranlagen wurde untersucht, und andererseits Membran Bio Reaktoren (MBR). Bei den besichtigten Kläranlagen war kein MBR vorhanden. Eine Einschätzung der Anfälligkeit dieses Systems kann im Vergleich zu den anderen somit nicht erfolgen. Zudem sind keine Daten bekannt, wie viele SBR und MBR Anlagen in NRW oder in Deutschland betrieben werden.

Kleinkläranlagen

Kleinkläranlagen dienen der Abwasserreinigung für geringe Abwassermengen und leiten im Jahr 26 Mio. m^3 Abwasser in Gewässer ein. Dies macht einen Anteil von 0,6 % des gesamten Abwassers aus (siehe Abbildung 3-7) (MULNV NRW, 2022). Kleinkläranlagen besitzen normalerweise keine technische Belüftung zur Wasseraufbereitung und reinigen täglich anfallendes Schmutzwasser von etwa 50 Einwohnern. Die Abwasserreinigung kann grob in drei Abschnitte eingeteilt werden, der mechanischen Vorbehandlung, der biologischen Behandlung ohne technische Belüftung und der anschließenden Abwassereinleitung. (DIN4261, 2008) Wenn elektrische Komponenten verbaut sind und es zu einem Stromausfall kommt besteht die Gefahr von Rückstau ins Gebäude oder des Einleitens von nur mechanisch gereinigtem Abwasser (Landratsamt-Ostalbkreis, 2022). Aufgrund der geringen Abwassermenge und der nicht immer vorhandenen Steuerungstechnik können Kleinkläranlagen vernachlässigt werden.

Industrielle Abwasserbehandlung

Die Schadstoffbelastung von industriellem Abwasser variiert je nach Art des Abwassers und Art des Industrie- oder Gewerbebetriebes stark und ist daher differenziert zu betrachten. Im Jahr 2020 fielen 724 Mio. m^3 Abwasser aus industriellen Direkteinleitungen an, was einem Anteil von 15,9 % am gesamt eingeleiteten Abwasser ausmacht (siehe Abbildung 3-7) (MULNV NRW, 2022). Neben den Sanitärabwasser und Niederschlagsabwasser fallen ebenfalls Produktionsabwasser und teilweise Kühlwasser an. Es ist zu berücksichtigen, dass diese Abwässer sowohl leicht als auch stark umweltbelastend sein können und daher nicht unkontrolliert bzw. unbehandelt in die Umwelt gelangen dürfen.

Erfolgt eine direkte Einleitung wird das Abwasser abschließend behandelt und dann in ein Gewässer eingeleitet. Hingegen wird bei der indirekten Einleitung in die Kanalisation das Abwasser zunächst ggf. einer Vorbehandlung beim Industrie- / Gewerbebetrieb unterzogen und anschließend erfolgt eine weitere Behandlung in einer kommunalen Kläranlage bevor das Abwasser in ein Gewässer eingeleitet werden kann. (MKULNV, 2012)

Insgesamt spielt die industrielle Abwasserbehandlung eine wesentliche Rolle in der Abwasserbehandlung. Es sind Angriffsszenarien möglich, in denen es sowohl zu direkten unkontrollierten Einleitungen von Abwässern in Gewässern kommt oder nicht vorbehandeltes Abwasser in kommunale Kläranlagen gelangt. Aus der möglicherweise höheren Belastung und Toxizität dieses Abwassers können so erhebliche Schäden in Gewässern resultieren oder z.B. Belebtschlämme auf kommunalen Kläranlagen langfristig Schaden nehmen.

Kanalisation/Abwasserableitung

Im Jahr 2020 wurden insgesamt 4.567 Mio. m^3 Abwasser in Gewässer eingeleitet. Davon gelangten 206 Mio. m^3 (~4,5 %) über Mischwasserentlastungen in Gewässer (MULNV NRW, 2022). Durch Angriffe auf das Kanalsystem oder den Zulauf von Kläranlagen könnte dieser Anteil deutlich vergrößert werden. Maximal wäre ein Anteil von ~56 % möglich. Damit würde ungeklärtes Abwasser in oberirdische Gewässer eingeleitet werden. Angriffe wären dabei beispielsweise auf Pumpwerke/Druckleitungen oder Abschlagbauwerke denkbar. Entstehende Risiken durch die Einleitung von ungeklärtem Abwasser sind hauptsächlich hygienische Risiken (beispielsweise E. coli Bakterien) und die Eutrophierung von Gewässern durch Nährstoffeinträge (Stickstoff, Phosphor). Unter bestimmten Randbedingungen können weitere Risiken durch die Einleitung von Chemikalien oder Arzneimitteln entstehen (Deutscher Bundestag, 2019).

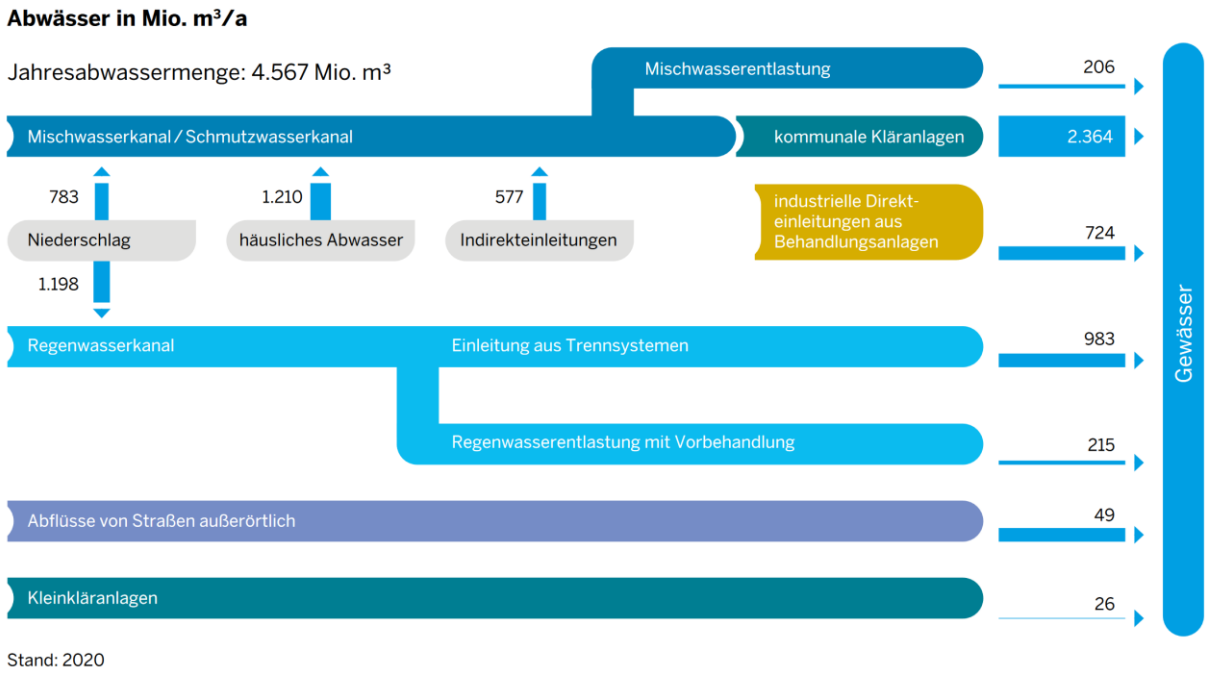


Abbildung 3-7: Herkunft und Menge des Abwassers im Jahr 2020 (in Mio. m^3/a) (MULNV NRW, 2022).

Übertragbarkeit

Die Ergebnisse des subKRITIS Projekt sollen möglichst auf alle Kläranlagen in NRW übertragen werden, um eine Einordnung des allgemeinen IT-Sicherheitsniveaus von Kläranlagen unterhalb der KritisV darzustellen. Dies ersetzt allerdings nicht die individuelle Untersuchung einer einzelnen Kläranlage auf ihre spezifischen Sicherheitslücken und Anfälligkeiten für Angriffe. Die Übertragbarkeit der Ergebnisse des Vorhabens subKRITIS können mit der vorgestellten Auswertung bewertet werden.

Im Projekt wurden 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, müssten auch diese auf ihre Sicherheit untersucht werden, um die Umwelt von 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 Wert auf die Kanalisation gelegt werden. 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 unterschiedliche 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.

3.2. Prozessverständnis der IT-technischen Komponenten der Kläranlage

Die Hauptaufgabe des Betreibers und des Personals besteht darin, die ordnungsgemäße Abwasserbeseitigung sicherzustellen. Hierin sind die Mitarbeiter ausgebildet und kompetent. Es kann und darf nicht vorausgesetzt werden, dass sie darüber hinaus über die notwendige Querschnittskompetenz verfügen, das Thema Informationstechnik in Gänze zu bedienen. Die Möglichkeit zur Spezialisierung auch mit Blick auf Steuerungstechnik und IT nimmt zu, wenn Anlagen größer sind und mehr Personal bzw. mehr finanzielle Mittel vorhanden sind. Betreiber größerer Anlagen haben leichter die Möglichkeit, Mitarbeiter mittels passender Fortbildungen zu motivieren und zu befähigen, sich der Thematik anzunehmen und/oder durch Bestellung oder Ausschreibung einen entsprechend leistungsfähigen Dienstleister zu beauftragen. Es besteht allerdings immer die Gefahr, dass ein gut ausgebildeter Mitarbeiter:in, der sich z.B. vom Elektrikermeister:in zum IT-Techniker:in mit Kenntnissen der Informationssicherheit fortgebildet hat, von einem anderen Unternehmen abgeworben wird. Dem zu begegnen sollten entsprechende Motivationsmöglichkeiten geschaffen werden. Auf kleineren bzw. mittelgroßen Anlagen ist zu sehen, dass intrinsisch motivierte Mitarbeiter sich zusätzlich privat für die Informationstechnik interessieren und sich über entsprechende Quellen im Internet, wie bspw. Heise Security (https://www.heise.de/security/) oder direkt beim BSI (https://www.bsi.bund.de/DE/Home/home_node.html) über die Thematik informieren und die erlangten Kenntnisse im Anlagenumfeld erfolgreich umsetzen. Darüber hinaus wurden bereits initiativ Kontakte und Kooperationen unter den Anlagenbetreibern und kommunalen Hilfsstellen, bspw. über das kommunale Rechenzentrum, auf- und ausgebaut, um die Kompetenzen zu stärken und verfügbare anlagenspezifische Erkenntnisse mit weiteren Personen im Umfeld zu teilen. Auch Fortbildungsmöglichkeiten über das KDW, die DWA, die DVGW berufliche Bildung oder beim BEW sollten stärker genutzt werden. Steuerungssysteme gehören längst zu den Kernprozessen von Kläranlagen und deren Sicherheit gegen Manipulation muss deshalb stärker in den Fokus gerückt werden.

Grundlage der Beurteilung einer Anlage bei externem Audit ist eine vollständige und aktuelle Dokumentation. Diese umfasst die jeweilige Betriebsdokumentation der Anlagen, Komponenten, Steuerungen, usw. in einem Netzstrukturplan und dazu gehörigen Komponentenlisten und Anlagenbeschreibungen. Dazu gehören aber auch die internen Richtlinien, die den Mitarbeitern ordnungsgemäßes Verhalten erläutern. Nur in sehr wenigen

Fällen konnte eine ordnungsmäßige, vollständige und aktuell gehaltene Dokumentation (in Gänze) vorgezeigt werden. Gelegentlich ging die Dokumentation auf die Initiative der Dienstleister zurück. Das kam der Qualität der Dokumentation zugute. Teilweise war den Mitarbeitern die Existenz von Richtlinien unbekannt oder unklar oder der Ort der Zugriffsmöglichkeit war nicht bekannt. Die Dokumentation der Betriebs- bzw. IT-Landschaft dient dazu, dass in Not- oder Krisenfällen, wenn also auch externe Kräfte hinzugezogen werden, entsprechend schnell gehandelt werden kann. Mittels Asset- und IP-Listen sowie Netzstrukturplänen wird es nicht nur dem anlagenbekannten Personal ermöglicht, in Notsituationen zu agieren, sondern auch externen Dienstleistern, die bei der Wiederinbetriebnahme bzw. der Forensik unterstützen. Anhand dieser Dokumentation verschaffen sich alle Beteiligten ein Gesamtbild der IT vor Ort. Sie erkennen Verbindungen zu Anlagenkomponenten und deren Steuerungen, erkennen die jeweiligen Installationen und deren Konfiguration und können daraufhin schnellstmöglich effiziente Maßnahmen definieren und diese effektiv umsetzen. Fehlen diese Informationen, wird dadurch die Arbeit zur Wiederherstellung der Leistung nicht nur unnötig hinausgezögert, sondern auch verkompliziert, da die Zusammenhänge erst einmal erschlossen werden müssen. Business Impact Analysen bzw. Business Continuity Pläne in Bezug auf die IT wurden nicht gefunden.

Vor der Befragung nach dem B3S WA wurde jeweils die gesamte Anlage begangen. Die Mitarbeiter erläuterten den Betrieb und die verschiedenen Komponenten. Dies umfasste die gesamte Steuerungstechnik von deren Stromversorgung über die Steuerungen für Schieber, Pumpen, Förderbänder, Schnecken, Zentrifugen, Pressen etc. inkl. der am Netz hängenden bzw. autark arbeitenden Sensorik. Auch die Netzkomponenten wie Switches, Firewalls, Racks, WLANs, Access Points, USVs, Glasfaser- bzw. Twisted Pair-Verbindungen und eingesetzte PCs, Laptops, Pads, Mobiltelefone und deren Software, z.B. Teamviewer für den Remotezugriff wurden erläutert (Informational Technology IT). Im Rahmen der Begehungen wurden bereits Netzpläne angeschaut bzw. die Funktionalität der Anlage anhand von Dokumentationen erläutert, die zu diesem Zweck auf der Anlage vorhanden war. Auch die physische Sicherung der Anlage durch Zaun, Torsystem und Zutrittsanlagen wie auch die Videoüberwachung wurden betrachtet. Wie bei jeder Begehung kritischer Infrastruktur wurde auch das Schließsystem selbst, dessen Nutzung zum Schutz kritischer Räume bzw. die Freischaltung des Zugriffs auf Steuerungen sowohl im Freien als auch in Räumen angeschaut. Dies umfasste Schlüssel und Tokens als Karte oder Schlüsselanhänger bzw. Schlüsselgriff. Im Rahmen der Begehung wurde auch über die Erfahrungen mit unautorisiertem Zutritt zur Anlage bzw. Vandalismus gesprochen. Dies umfasste auch Erfahrungen im Umgang mit autorisierten Lieferanten.

Im Anschluss an die Begehung erfolget dann die Befragung nach dem B3S WA wie im Kapitel 2.3 näher erläutert. Die Befragung wurde in aller Regel mit den Anlagenverantwortlichen, teils

assistiert von einem Elektriker bzw. sogar in Anwesenheit eines Mitarbeiters eines Dienstleisters bzw. der Stadt durchgeführt.

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

3.3. Beurteilung des IT-Sicherheitsniveaus

Der branchenspezifische Sicherheitsstandard für den Bereich Wasser/Abwasser (kurz: B3S WA) basiert auf der durch BSIG § 8.a Abs. 3 vorgegebenen Möglichkeit, dass sich Branchen selbst Standards aufstellen, deren Eignung dann durch das BSI festgestellt wird. Ziel bei der Entwicklung des B3S WA durch die DWA und den DVGW war es, einen einheitlichen Standard sowohl für KRITIS- als auch für kleinere Unternehmen zu schaffen. Deshalb unterscheidet der Standard die beiden B3S-Level

1. Kritische Infrastruktur und
2. Allgemein

Die sich aus dem Level „Allgemein“ ergebenden Maßnahmen sollten von jedem Unternehmen der Abwasserbehandlung erfüllt werden.

Der Standard bringt zudem die wesentlichen Komponenten eines jeden Managementsystems für Informationssicherheit mit. Das ist einmal die Bewertung der Risiken für einzelne Werte oder Wertegruppen jeweils vor und nach durchgeführten Maßnahmen. Und es ist die regelmäßige Wiederholung des Vorgehens, um die fortlaufende Wirksamkeit der Maßnahmen sicherzustellen.

Der B3S WA besteht aus folgenden Komponenten:

1. DVGW-Merkblatt W 1060 / DWA-M 1060
2. IT-Sicherheits-Leitfaden (Excel oder PDF)

   Das Handbuch zum IT-Sicherheits-Leitfaden ist nicht Bestandteil des Standards aber zum Verständnis unerlässlich.

Das Merkblatt hilft zunächst, die Begriffe zu verstehen. Was ist eine Abwasserbehandlungsanlage aus Sicht der Informationstechnik, welche Schutzziele werden verfolgt und wie leiten sich aus Risiken die ihnen entgegenwirkenden Maßnahmen ab? Was ist in Bezug auf die Risikobewertung zu berücksichtigen und wann sind Maßnahmen angemessen und geeignet?

Der IT-Sicherheitsleitfaden ist eine Excel-Liste, die von einer Website des DVGW heruntergeladen werden kann (IT-Sicherheitsleitfaden (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. Diese Variante wird zukünftig ausschließlich verfügbar sein. Das Grundschutzkompendium wird jährlich im Februar neu vom BSI herausgegeben. Für den jeweiligen B3S WA gilt aber immer das zum Zeitpunkt seiner Erstellung und Eignungsfeststellung gültige Kompendium. Im Falle subKRITIS also das von 2019. Für die vorliegende Untersuchung wurde die Version basierend auf dem BSI-Grundschutzkompendium verwendet.

Das Handbuch zum IT-Sicherheitsleitfaden beschreibt, wie dieser angewendet werden soll. Um das zu verdeutlichen, enthält es Prozessdiagramme, aus denen die Vorgehensweise detailliert ersichtlich ist. Wegen seines normativen Charakters und seiner ubiquitären Einsatzmöglichkeit in der Wasserwirtschaft wurde der B3S WA als Analysewerkzeug für das Projekt subKRITIS gewählt.

Das in Abbildung 3-8 dargestellte Schaubild zeigt exemplarisch die Vorgehensweise zur Auswahl eines Anwendungsfalles:

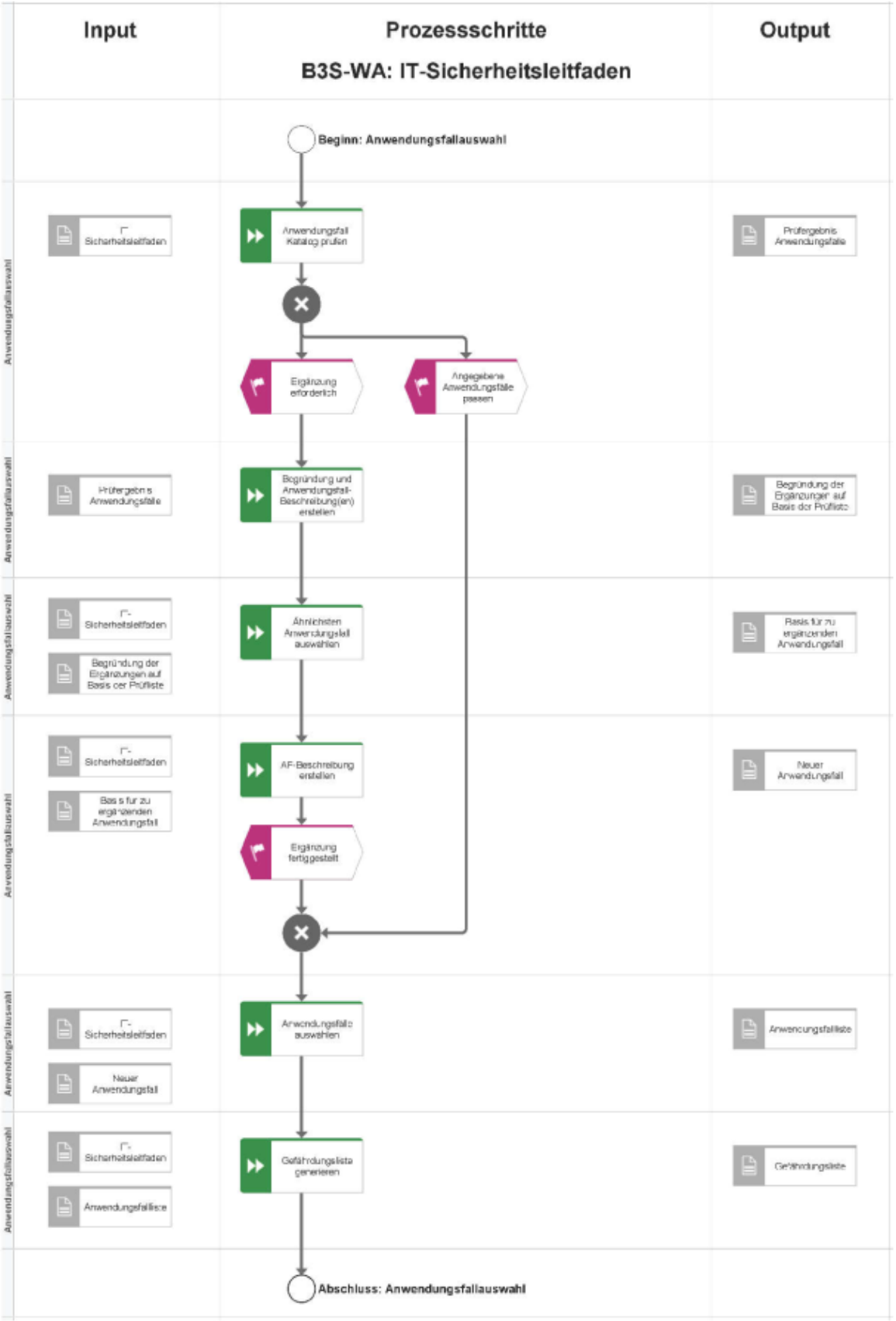


Abbildung 3-8: Prozessschritte des B3 WA zur Ermittlung der Anwendungsfälle aus dem Handbuch zum IT-Sicherheitsleitfaden.

3.3.1. Standardisiertes Auswertungsschema

Das Schaubild in Abbildung 3-9 zeigt den Prozessablauf des B3S WA in einer vereinfachten Darstellung (eigene Darstellung DVGW S&C GmbH):

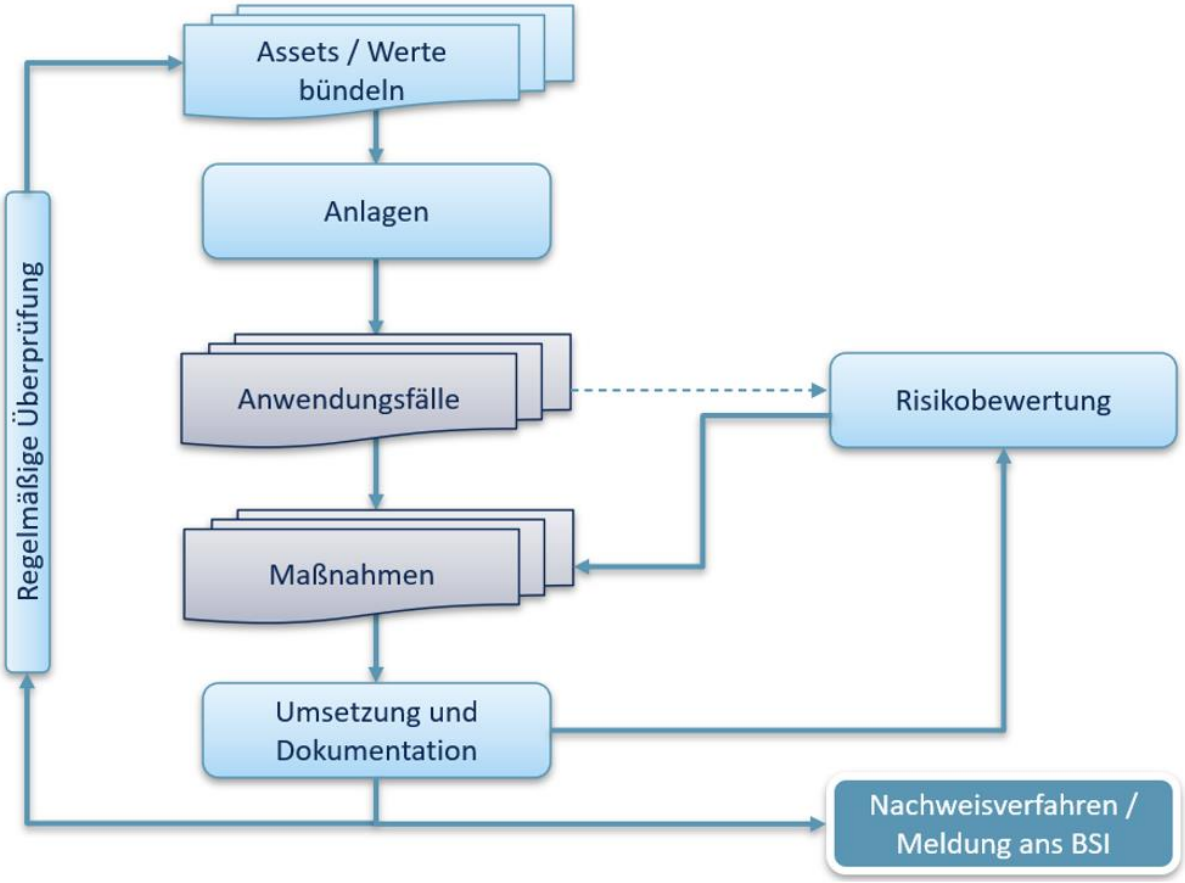


Abbildung 3-9: Vereinfachte Prozessdarstellung des Branchenspezifischen Sicherheitsstandards (kurz: B3S WA).

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. Im Idealfall können bestimmte Assets unmittelbar zusammengefasst oder gebündelt werden. 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 derselben Leitstelle gesteuert werden.

Im nächsten Schritt erfolgt die Bestimmung der **Anwendungsfälle**. Dort wird beobachtet, 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, daraus abgeleitete Anforderungen und ihnen entgegenwirkende Maßnahmen ergeben. Die **Risiken** lassen sich allerdings nicht mit geschlossenen Fragen **bewerten**, die mit ja oder nein zu beantworten wären. Dementsprechend müssen in die Beurteilung der Fragen immer die genauen örtlichen Gegebenheiten einfließen. Hierdurch wurde hin und wieder das Hinzuziehen von weiteren Mitarbeitern oder sogar beauftragter Dienstleister notwendig. Gleichzeitig wird dadurch aber auch sichergestellt, dass die bereits vorhandenen Sicherheitsmaßnahmen flexibel berücksichtigt werden können.

Die Analyse als Ergebnis der Untersuchung besteht aus der Beurteilung der Antwortqualität auf die Fragen aus dem B3S WA nach folgendem Schema:

Tabelle 3-1: Beurteilungsschema der Antwortqualität.

Bewertung	Bewertungstext
Sehr positiv	Maßnahmen sind getroffen, die der Gefährdung vollständig entgegenwirken.
gut	Es wurde eine Verbesserungsmöglichkeit festgestellt. Die Umsetzung ist freigestellt.
neutral	Es wurde eine Verbesserungsmöglichkeit festgestellt. Es ist durch den Geprüften zu bestimmen, ob diese wirtschaftlich sinnvoll und wirksam ist. Das Ergebnis ist zu dokumentieren. Sofern wirtschaftlich sinnvoll und wirksam, ist eine Verbesserungsmaßnahme bis zur nächsten Überprüfung zu definieren und nachweisbar umzusetzen.
unzureichend	Die Maßnahmen sind mit Blick auf die betrachtete Gefährdung unzureichend und es sollten zeitnah weitere Maßnahmen definiert, ergriffen und deren Wirksamkeit geprüft werden. Die Umsetzung ist zu dokumentieren.
nicht vorhanden	Maßnahmen, die der betrachteten Gefährdung entgegenwirken, wurden nicht getroffen. Die Definition und Umsetzung von Maßnahmen sind dringend geboten.
Ausschluss	Die laut B3S WA zu betrachtende Gefährdung ist nicht vorhanden.

Eine Beurteilung der Antwortqualität ist im Rahmen der normalen Anwendung des B3S WA nicht vorgesehen, sondern es sind alle Maßnahmen vollständig umzusetzen. Da es hier aber um die Beurteilung der Anlagensicherheit in Bezug auf die Gefährdungen und Anforderungen geht, wurden die Bewertungen wie dargestellt verwendet. Sie leiten sich aus den häufig für ISO 27001-Audits verwendeten Kategorien ab, die Hinweise (gut), Empfehlungen (neutral), Beanstandungen (unzureichend) und Abweichungen (nicht vorhanden) kennen. Was sehr positiv bewertet wurde, muss nicht weiter beachtet werden.

3.3.2. Wasserwirtschaftliche Relevanz der IT-Sicherheitsmängel

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. Dazu gehört auch, dass eine eingespielte Falschinformationen den Schaden durch eine Entscheidung des Personals verursacht und somit indirekt vom Angreifer ausgelöst wird. Ein informationstechnischer Mangel ist als Gefährdung zu verstehen, dem nicht vollständig durch geeignete Maßnahmen entgegengewirkt wird. Es wird dabei zwischen fünf verschiedenen Effekten unterschieden, die IT-Relevanz genannt werden. Diese sind in Tabelle 3-2 aufgelistet. Bei einem lesenden Zugriff können lediglich Daten gewonnen werden, allerdings kann kein direkter Einfluss auf die Prozesse der Kläranlage genommen werden. Werden Mängel in der „Infrastruktur" gefunden, aus welchen aber keine direkten Zugriffe auf eine Steuerungsebene resultieren, hat dies ebenfalls keine wasserwirtschaftliche Relevanz. Weiterhin wurden Mängel in der Planung von beispielsweise dem Regelbetrieb gefunden, die auch keine direkte wasserwirtschaftliche Auswirkung haben. Und zuletzt wurden Mängel gefunden, welche keinen direkten Einfluss auf IT-Systeme haben. Diese vier Effekte spielen somit für die wasserwirtschaftliche Seite keine Rolle. Der relevante Effekt ist, wenn es durch einen IT-Sicherheitsmangel möglich ist, „schreibend" auf Steuerungen oder die Leitstellensoftware zuzugreifen. Ein Beispiel dafür wäre, dass eine fehlerhafte Konfiguration von Routern und Switchen vorliegt.

Tabelle 3-2: Einordnung der IT-Relevanz von Sicherheitslücken.

IT-Relevanz	Beschreibung
Lesend	Liest von Steuerungen und kann so OT nicht direkt beeinflussen
Schreibend	Schreibt auf Steuerungen oder Leitstellensoftware
Infrastruktur	Bezieht sich auf Infrastruktur wie Router und Switche, die zunächst manipuliert werden müssten, bevor auf die Steuerungsebene zugegriffen werden kann.
Planung	Wenn zum Beispiel Applikationen nach ihrer Wichtigkeit für den Regelbetrieb priorisiert werden, hat das keinen unmittelbaren IT-Einfluss, ist aber auch nicht irrelevant.
Irrelevant	z.B. physische Sicherheit. Nicht insgesamt irrelevant, aber unter dem Aspekt unmittelbaren IT-Zugriffs auf das Steuerungsnetz.

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. Dies beinhaltet beispielsweise:

- Verstellung von Schiebern oder Pumpen
- Skalierung von Messergebnissen
- Regelung der Belüftung (Grenzwerte, Belüftungsdauern)
- Beeinflussung des Alarmsystems

- Schnelles Ein- und Ausschalten von Aggregaten, woraus eine Überhitzung resultiert

Weitere Angriffsmöglichkeiten wurden bereits in Abbildung 3-1 erwähnt. Ob einzelne Anlagen-Prozesse veränderbar sind oder aus der Liste herausfallen, 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. 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:

1. Bereitschaftsstörung: Dauer 4 h
    - Bei dieser Störung kommt es nach kurzer Zeit zu einer Meldung an einen Mitarbeiter, der sofort die Anlage besichtigt und den Fehler beheben kann.
    - Beispiele: Not-Aus Knöpfe gedrückt, Schieber zugestellt und Höhenstandsalarm wird gemeldet.
2. Wochenendangriff: Dauer 24 h
    - Durch den zeitgleichen Zugriff auf das PLS und/ oder das Alarmsystem werden keine Benachrichtigungen an Mitarbeiter gesendet. Der Angriff bleibt somit bis zur nächsten Besichtigung unbemerkt und kann dann von einem Mitarbeiter vor Ort behoben werden.
    - Beispiel: Ausfall Belüftung, Öffnen von Bypässen.
3. Versteckter Eingriff: Dauer ist unbekannt (Annahme 7 d)
    - Durch den Zugriff auf das PLS werden einzelne Hintergrundwerte verändert, ohne dass diese dem Mitarbeiter angezeigt werden. Die Veränderung fällt erst bei einer Überschreitung der Ablaufwerte auf. Nach einer längeren Fehlersuche kann der Eingriff festgestellt werden.
    - Beispiele: Veränderung von Reglungswerten der Belüftung, Herunterregeln der internen Rezirkulation.

Da alle Kläranlagen sowohl über eine Leitstellensoftware als auch über „schreibende" IT-Sicherheitsmängel verfügen, kann jede Kläranlage als wasserwirtschaftlich vulnerabel eingestuft werden.

3.4. Auswertung und Aufbereitung (IT)

3.4.1. Auswertung der B3S WA Befragung

Gefährdungen können für verschiedene Anwendungsfälle gleichartig vorhanden sein. So besteht die Gefährdung „Verlust gespeicherter Daten“ gleichermaßen für Anwendungsfälle wie „Lokale SPS Programmierung und Wartung“, „SPS Programmierung und Wartung von zentraler Stelle auf der Anlage“, „SPS (Speicherprogrammierbare Steuerung) Programmierung und Wartung über Fernzugriff (von anderem Standort aus)“, „Systemzugang (steuernd) im gesicherten Kontrollraum“ und „Remote-Zugang (lesend, von anderem Standort aus)“, um nur einige zu nennen. 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. Der nachfolgenden Tabelle 3-3 ist die Zahl der Antworten nach der Bewertung und nach Größenklassen der Antworten in absoluten Werten zu entnehmen. Die Abbildung 3-10 stellt das Ergebnis graphisch dar.

Tabelle 3-3: Summe der Antworten der B3S-Befragung auf den 13 Kläranlagen tabellarisch nach Bewertung und nach Größenklassen.

Bewertung der Antwort	GK 3 2 KA	GK 4 7 KA	GK 5 4 KA	Gesamtergebnis
Sehr positiv	11	74	26	111
Gut	33	146	115	294
Neutral	23	134	103	289
Unzureichend	19	51	37	107
Nicht vorh.	14	22	17	53
Ausschluss	15	33	7	55
Summe	115	460	305	880

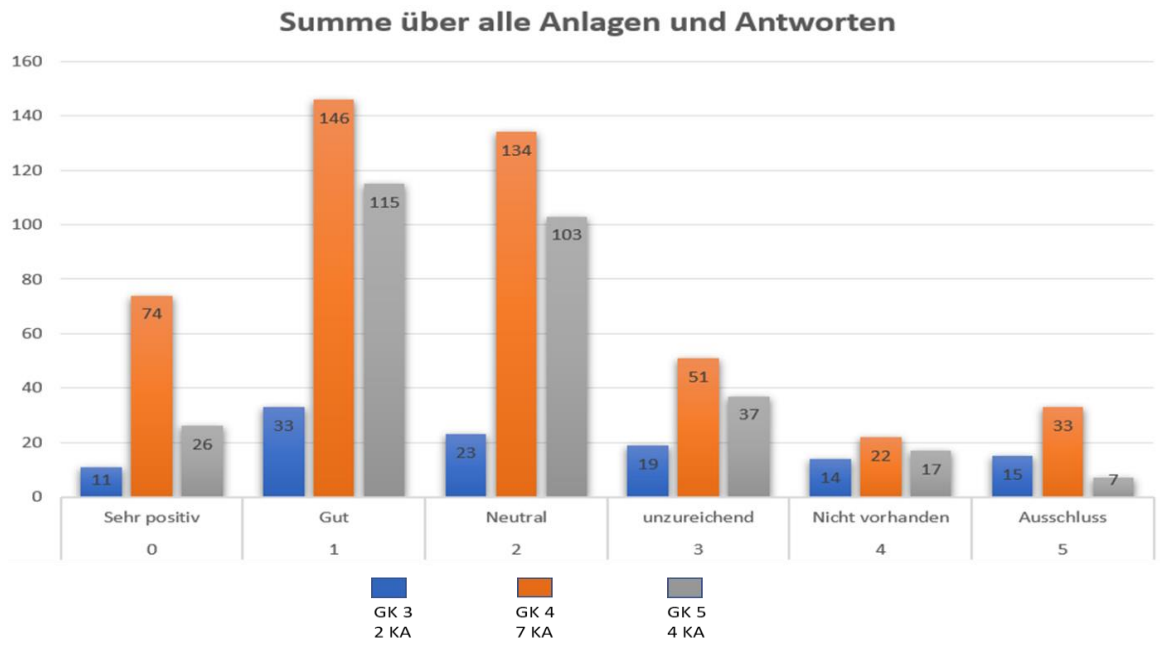


Abbildung 3-10: Summe der Antworten der B3S-Befragung grafisch nach Bewertung und nach Größenklassen.

Abbildung 3-10 zeigt die Antworten der 2 Anlagen der Größenklasse 3, 7 Anlagen der Größenklasse 4 und 4 Anlagen der GK 5. Die absoluten Zahlen der Antworten zeigen, dass mit zunehmender Anlagengröße mehr Fragen diskutiert wurden. Für die GK 3 waren es 58 Fragen/ Anlage, für die GK 4 waren es 66 Fragen/ Anlage und für die GK 5 schließlich 94 Fragen/ Anlage. Dieses Ergebnis ist nicht nur auf die unterschiedliche Zahl der Anwendungsfälle, sondern auch auf die Fähigkeit der Anlagenbetreiber zur Auskunft zu verschiedenen Assets zurückzuführen.

Um die Qualität der Antworten nach Größenklasse vergleichen zu können, müssen die Werte einander normiert gegenübergestellt werden. Dies geschieht in Abbildung 3-11. Hier werden die Antworten anhand relativer Werte nach Bewertung und nach Größenklassen einander gegenübergestellt.

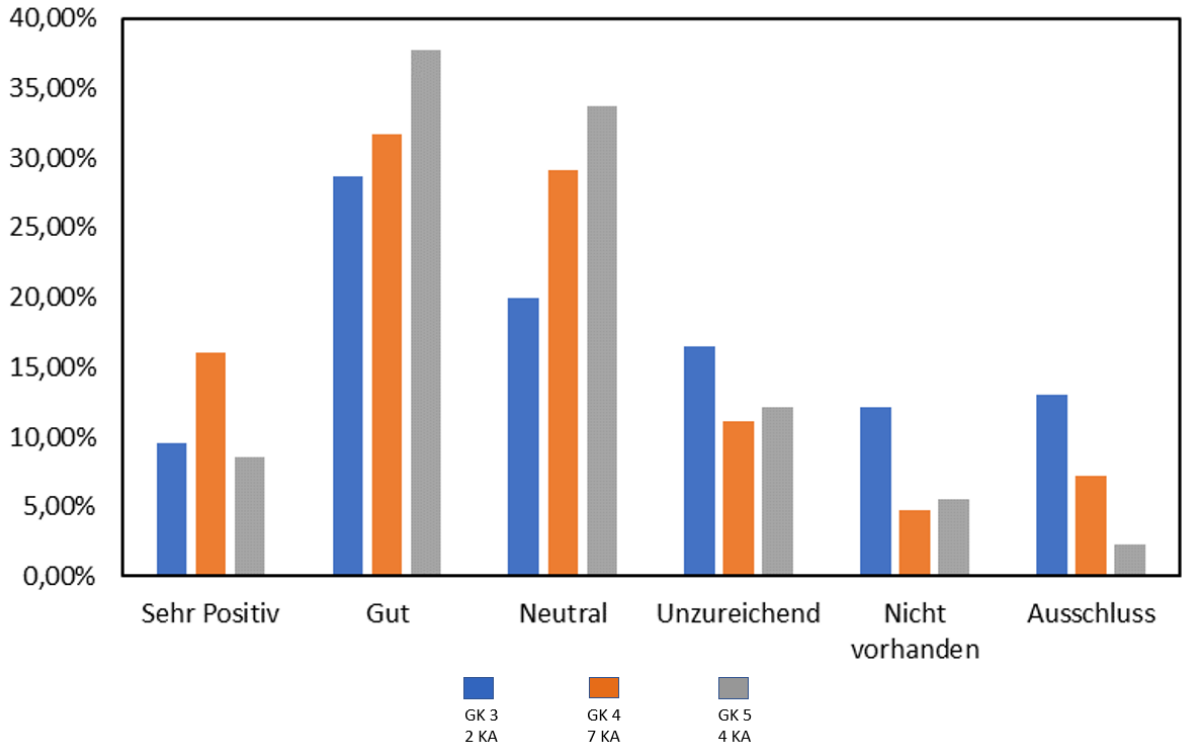


Abbildung 3-11: Ergebnisse der B3S-Befragung - relative Werte nach Bewertung und nach Größenklassen.

Anhand der Abbildung **3-11** wird deutlich, dass größere Kläranlagen in der Informationssicherheit besser zu bewerten sind. Darüber hinaus wird aufgezeigt, dass die meisten Antworten mit „Sehr positiv“, „Gut“ oder mit „Neutral“ bewertet wurden und dies unabhängig der jeweiligen Größenklassen.

Der BSI Grundschutz fasst Maßnahmen in Schichten zusammen. Alle Maßnahmen im Umfeld von Anwendungen werden zum Beispiel der Schicht „APP: Anwendungen“ zugeordnet. Die Schichten sind:

- APP: Anwendungen
- CON: Konzeption und Vorgehensweise
- DER: Detektion und Reaktion
- IND: Industrielle IT
- INF: Infrastruktur
- ISMS: Sicherheitsmanagement
- NET: Netze und Kommunikation
- OPS: Betrieb (engl.: Operations)
- ORP Organisation und Personal
- SYS: IT-Systeme

Auch wenn die Fragen zu den einzelnen Schichten im B3S WA nicht gleichmäßig verteilt sind, kann das Schichtkonzept zu drei Zwecken verwendet werden:

1. Feststellung der Stärken und Schwächen für einzelne Anlagen.
2. Weitere Vergleichsmöglichkeiten zwischen Anlagen und Größenklassen.
3. Ableitung, in welchem Bereich eine Unterstützung der Anlagenbetreiber notwendig und besonders sinnvoll ist.

Eine nach Schichten aufgeschlüsselte Auswertung aller Fragen und für alle Größenklassen von Anlagen zeigt Abbildung 3-12. Es sei noch einmal auf die nicht gleichmäßige Verteilung der Fragen / Schicht im B3S WA hingewiesen.

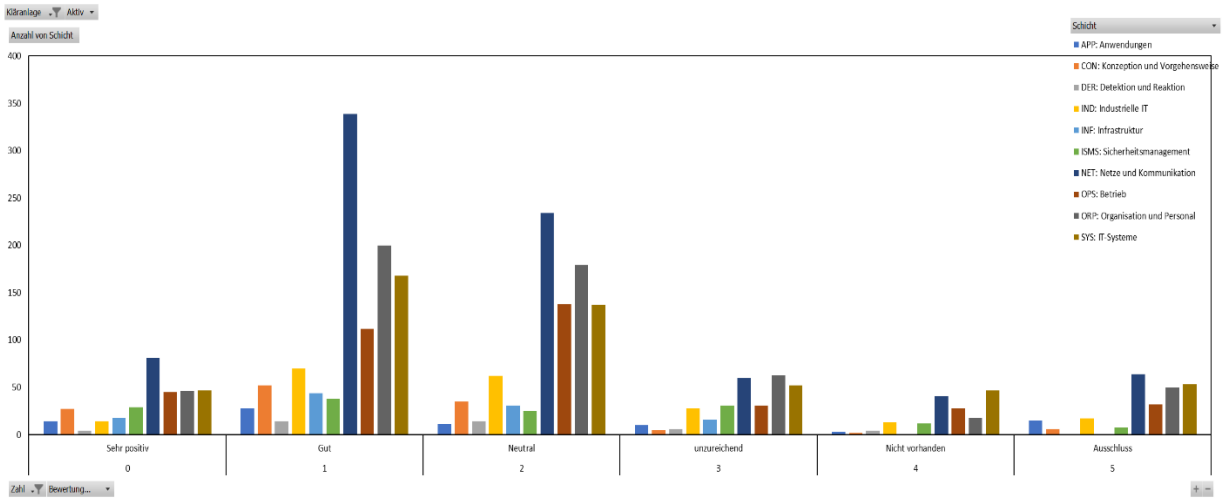


Abbildung 3-12: Antworten nach Schichten aus dem Grundschutz - Kompendium.

Abbildung 3-12 verdeutlich, dass die meisten Fragen aus dem B3S WA im Rahmen dieser Untersuchung aus den 4 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. Der vertikale Maßstab zeigt die Zahl der Fragen zur Schicht über alle Anlagen.

Eine normierte Auswertung der Antworten nach Schichten ist der Abbildung 3-13 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, da die jeweilige Gesamtzahl zu gering ist.

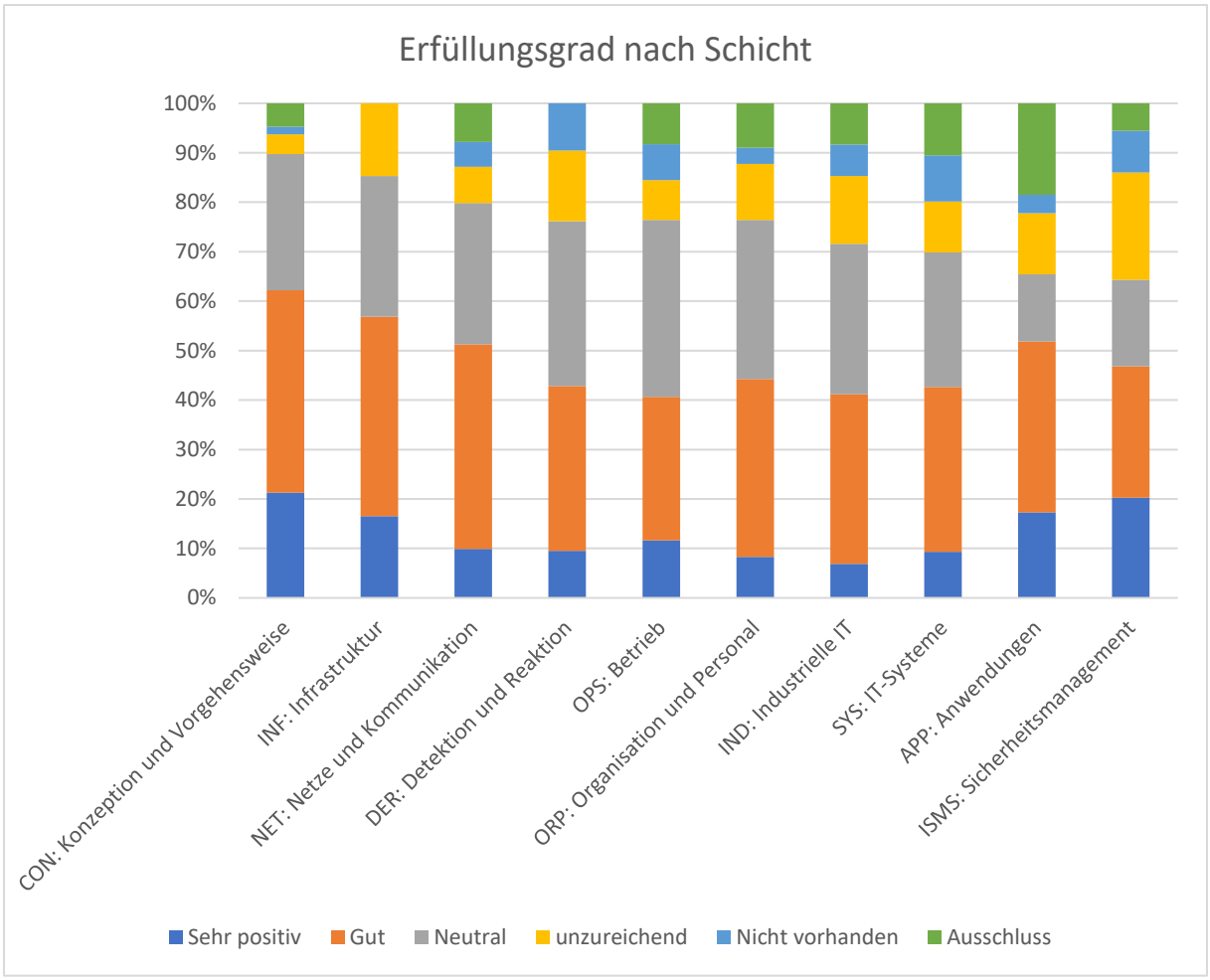


Abbildung 3-13: Antworten nach Schichten normiert.

Die Abbildung 3-13 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. Die Antworten sind links positiv und fallen nach rechts in Richtung negativer Antworten ab.

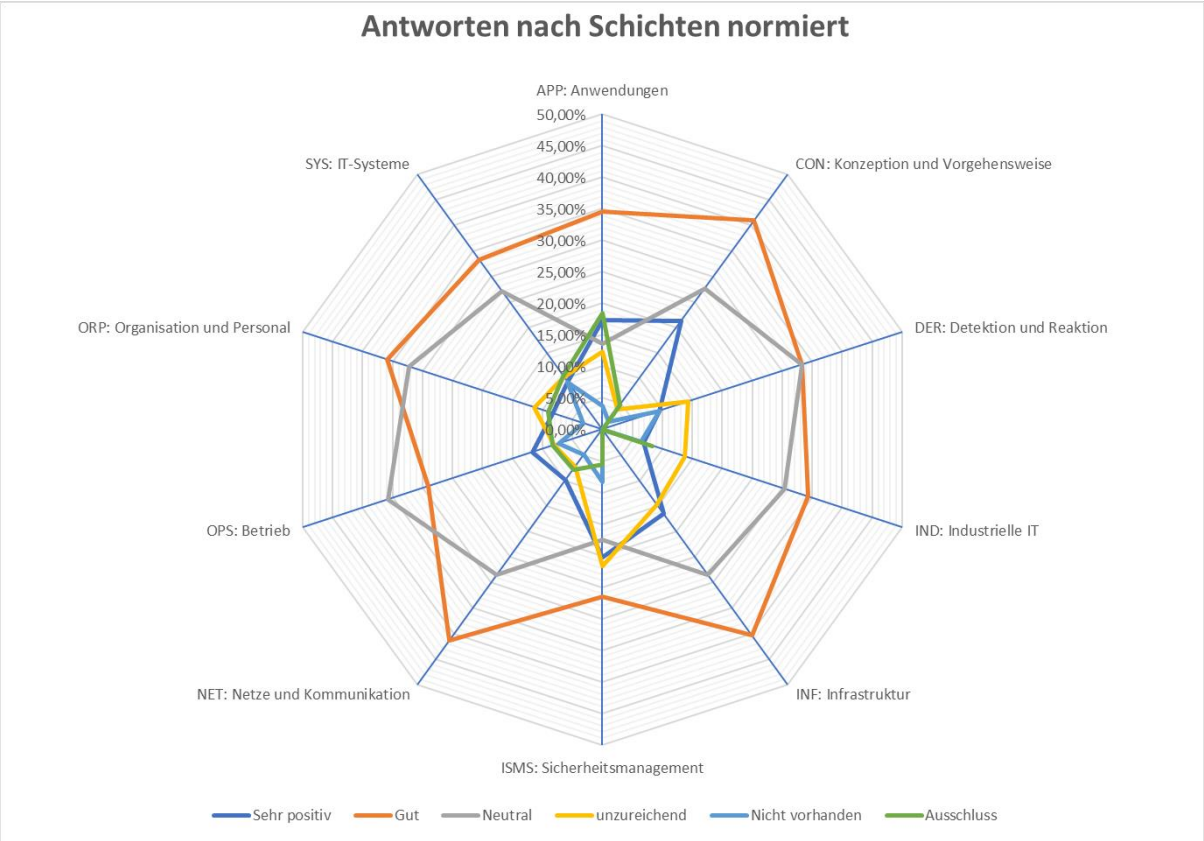


Abbildung 3-14: Antworten nach Schichten normiert.

Im Antrag wurde beschrieben, dass die Ergebnisse in Form von Netzdiagrammen dargestellt werden sollen. Dies geht auf einen Vorläuferstandard zum B3S WA zurück, dessen Ergebnisse mit dieser Diagrammform optimal dargestellt werden konnten. Deshalb ist hier der Inhalt von Abbildung 3-14 als Netzdiagramm dargestellt, was die Übersichtlichkeit nicht fördert. Von der weiteren Verwendung von Netzdiagrammen zur Ergebnisdarstellung sehen wir daher ab.

Kapitel 3.3.2 teilt die Gefährdungszeiträume nach Bereitschaftsstörungen mit 4 h Dauer, Wochenendangriffen mit 24 h Dauer und versteckten Eingriffen mit 7 d Dauer, jeweils bis zum Nachweis von Störungen, ein. Das bedeutet nicht, dass eine Kompromittierung der IT oder OT einer Anlage unmittelbar in einen Angriff mündet. Eine Kompromittierung kann durchaus erfolgen, ohne dass ein Angreifer über Monate oder gar Jahre Gebrauch davon machen müsste. Ein Angreifer kann einen gewonnenen Zugriff schlafend stellen und später gemeinsam mit den Zugriffen auf weitere Anlagen nutzen, um so einen weit größeren Schaden zu verursachen oder ein weit größeres Drohpotenzial für Erpressungen aufzubauen.

3.4.2. Verknüpfung Wasserwirtschaft zur Informationstechnik

Für die Präsentation der Abschlussveranstaltung und für diesen Abschlussbericht sollen die Daten einzelner Anlagen nicht verwendet werden, um die Anlagenanonymität zu wahren. Um

trotzdem aufzeigen zu können, welche Konsequenzen aus den Untersuchungen für einzelne Anlagen ableitbar sind, haben wir die fiktive Kläranlage *Schlingensiepen* kreiert und ihr die Eigenschaften einer Mischung aus den untersuchten Anlagen gegeben.

Die technische Auswertung der Simulationsergebnisse einerseits und der Befragungsergebnisse nach dem B3S WA findet in Excel statt. Die Datenstrukturen unterscheiden sich in beiden Fällen stark. Deshalb werden zwei Tabellen verwendet. Die eine Tabelle erlaubt die Auswirkung (engl. Impact) auszuwerten. Die andere Tabelle wird dazu genutzt, bei Grenzwertüberschreitungen die Anforderungen zu ermitteln, die Wirkung auf den schreibenden Einfluss auf Steuernetz oder die Leitstelle haben. So kann rückwärts aus den Folgen, die für eine Anlage betrachtet werden, ermittelt werden, was verbessert werden muss, damit diese Folgen gar nicht erst eintreten.

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 3-15: Verknüpfung Wasserwirtschaft ← → Informationstechnik: Erklärte Werte überschritten/ Abschlag erzeugt, dem entgegenwirkende Maßnahmen.

Die Abbildung 3-15 zeigt für die virtuelle Anlage *Schlingensiepen* auf der linken Seite die Anlagenteile, die bei Manipulation übers Internet zu einem Schaden (Überschreitung der erklärten Werte/ Abschlag von Abwasser) führen würden. Zudem ist angegeben, welcher Fehler für den jeweiligen Anlagenteil eintreten würde. Beispielhaft seien hier die Pumpwerke genannt, die entweder ausfallen oder deren Messsonden manipuliert sein können. Der betrachtete Zeitraum beträgt im Beispiel 7 Tage. Die rechte Seite der Abbildung zeigt, mit welchen Maßnahmen dem durch vollständige Umsetzung 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. Das sind dann die „Quick Wins“.

Die Abbildung 3-16 bis Abbildung 3-18 zeigen, wie die Simulation für die drei betrachteten Zeiträume zuerst schwache Auswirkungen ausweist, die sich im Verlauf der Zeit in Richtung der Überschreitung erklärter Werte „verschlimmern“. Ausgewertet werden alle Anlagen der Untersuchung gemeinsam (Ausnahme die virtuelle Anlage *Schlingensiepen*). Der vertikale Maßstab zeigt also die Zahl der Anlagen, für die jeweils „Schwache Auswirkungen“ und / oder „Erklärte Werte überschritten“ ermittelt wurden. Horizontal werden die jeweils betroffenen Verfahrensstufen gezeigt.

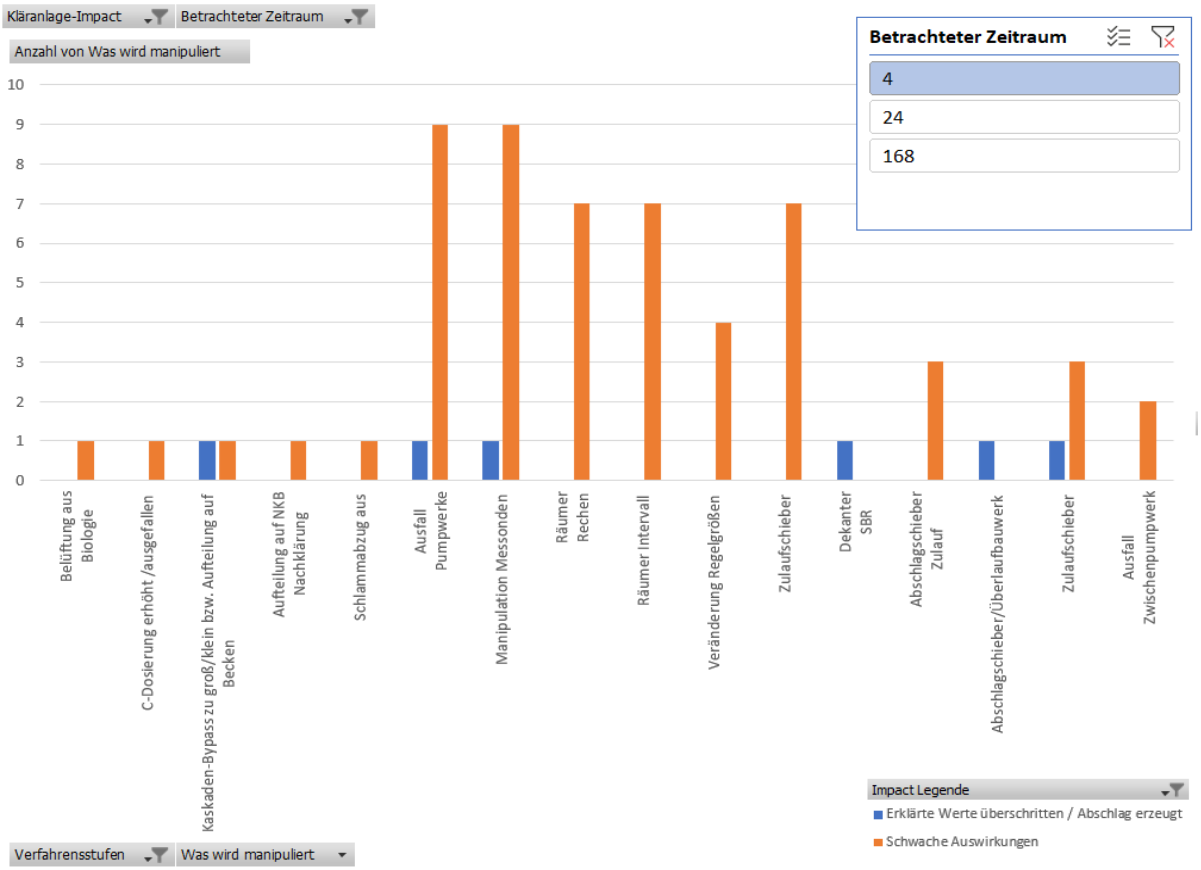


Abbildung 3-16: Schäden aus der Simulation subsummiert über alle untersuchten Anlagen – 4 Stunden.

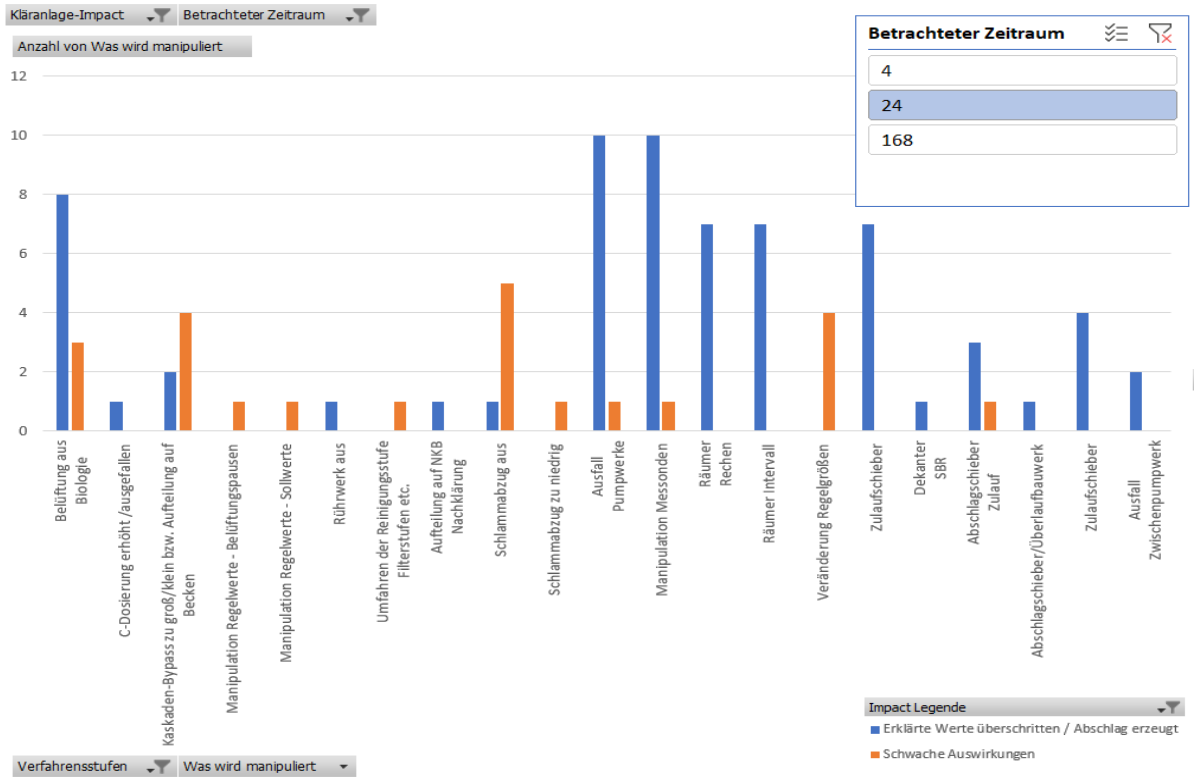


Abbildung 3-17: Schäden aus der Simulation subsummiert über alle untersuchten Anlagen – 24 Stunden.

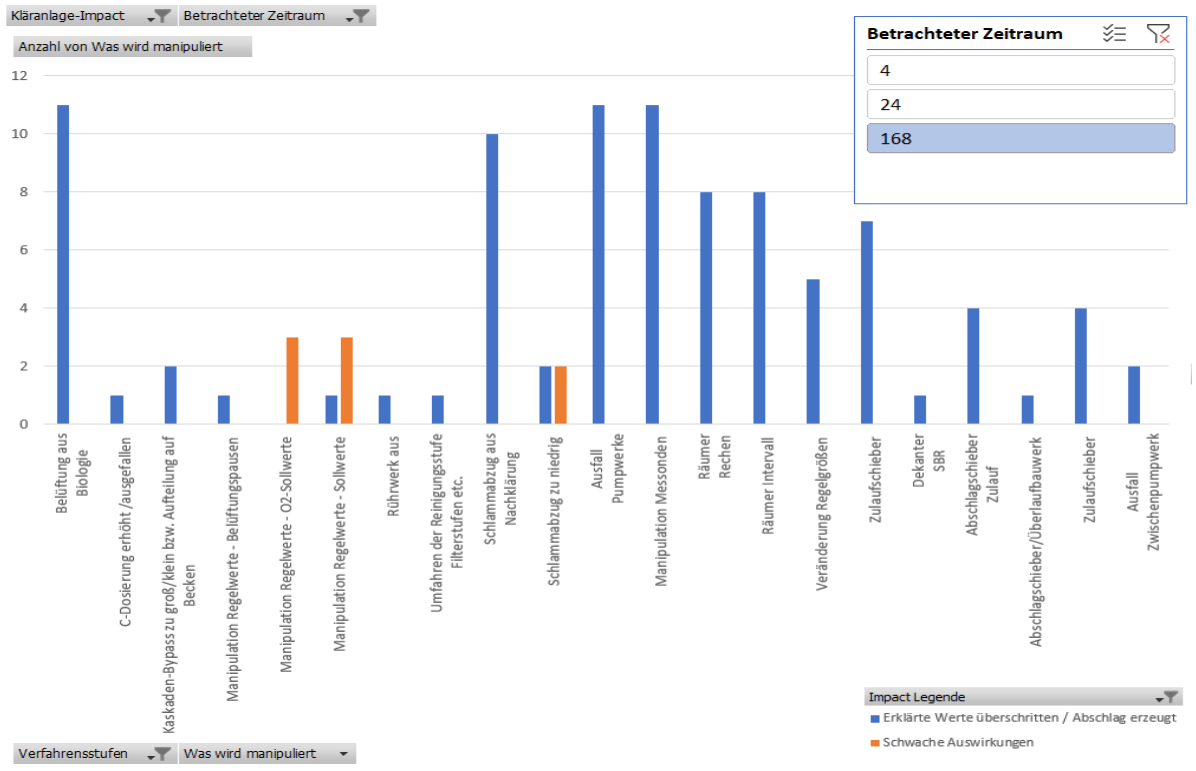


Abbildung 3-18: Schäden aus der Simulation subsummiert über alle untersuchten Anlagen – 7 Tage (168 h).

Die drei aufeinanderfolgenden Abbildungen zeigen jeweils in der äußersten linken Spalte deutlich die Entwicklung möglicher Schäden über der Zeit. Während in Abbildung 3-19, also nach 4 Stunden, „Belüftung aus – Biologie“ nur auf einer Anlage zu „Schwachen Auswirkungen“ führen würde, zeigt Abbildung 3-20, berechnet nach 24 Stunden, bereits für 8 Anlagen das „Überschreiten erklärter Grenzwerte“ und zusätzlich für 3 Anlagen „Schwache Auswirkungen“. Abbildung 3-21 weist dann nach 7 Tagen für 11 Anlagen das „Überschreiten erklärter Grenzwerte“ aus. Für das Abschalten der Biologie ist das sicher ein erwartbares Ergebnis, aber die Auswertung liefert solche Ergebnisse für alle betrachteten Verfahrensstufen. Damit lässt sich individuell und in Summe ermitteln, welche Alarmierung benötigt wird, um das Überschreiten erklärter Grenzwerte zu verhindern, bzw. rechtzeitig davor zu warnen. Zur Verdeutlichung zeigen die Abbildung 3-19 bis Abbildung 3-21 die Möglichkeiten der Auswertung für unsere Demoanlage *Schlingensiepen* im gleichen zeitlichen Ablauf.

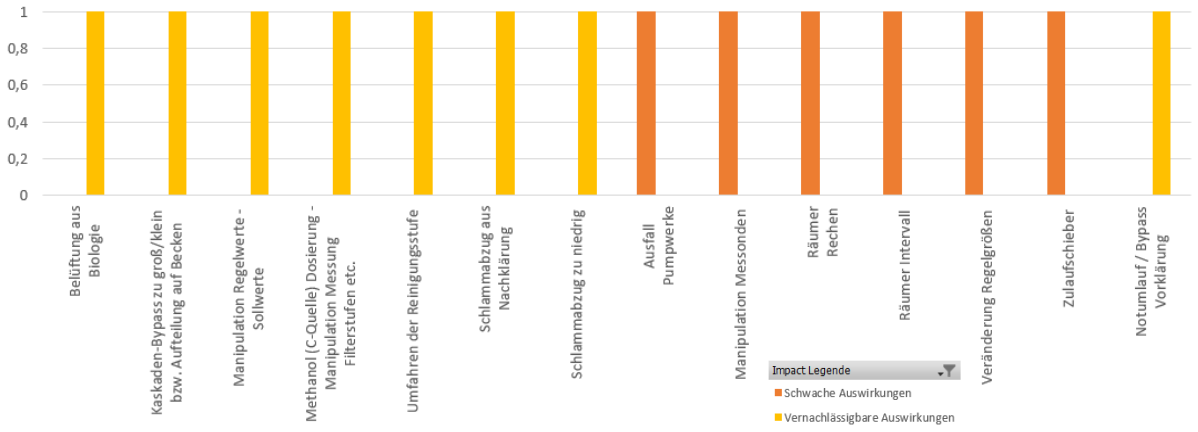


Abbildung 3-19: Schäden aus der Simulation Demoanlage Schlingensiepen – 4 Stunden.

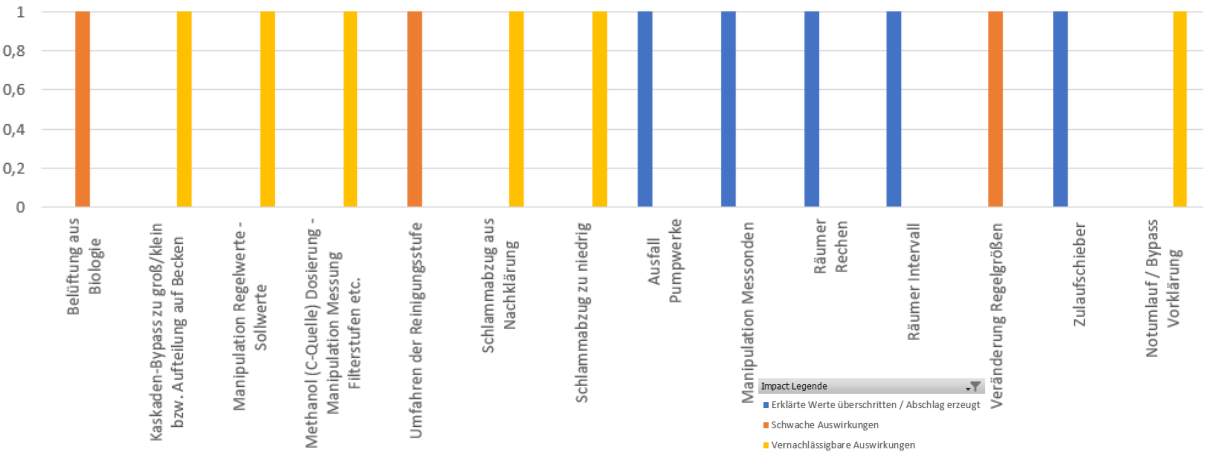


Abbildung 3-20: Schäden aus der Simulation Demoanlage Schlingensiepen– 24 Stunden.

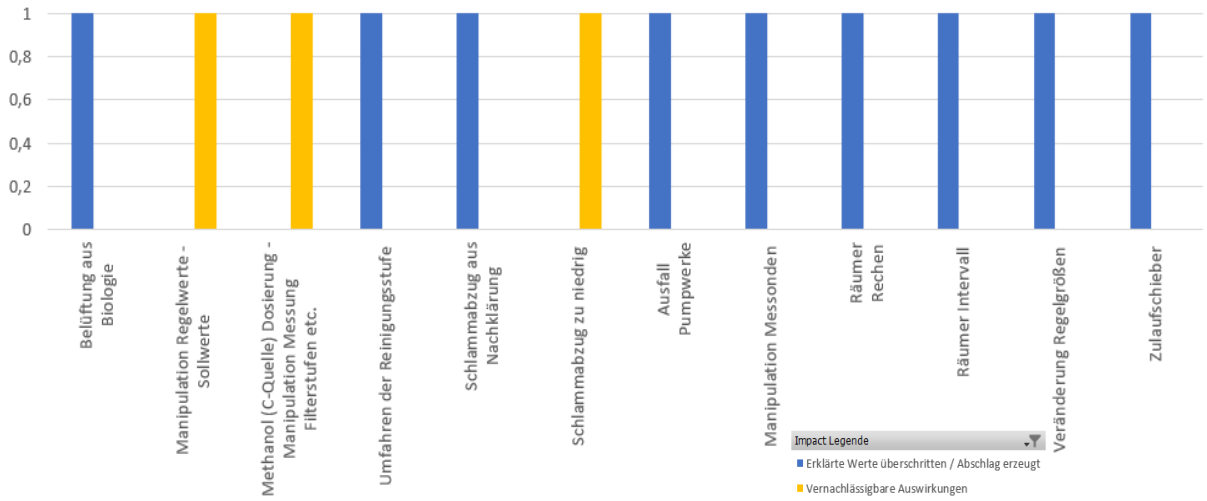


Abbildung 3-21: Schäden aus der Simulation Demoanlage Schlingensiepen – 7 Tage.

Aus Abbildung 3-19 bis Abbildung 3-21 ist für die Zeitpunkte 4 Stunden, 24 Stunden und 168 Stunden (7 Tage) die Entwicklung der Schäden von „vernachlässigbaren Auswirkungen“ hin zu „Erklärte Werte überschritten“ für einzelne Verfahrensstufen nachvollziehbar. Aus dieser Betrachtung ergeben sich Priorisierungen für die Schwachstellen auf der wasserwirtschaftlichen Seite. Eine genaue Erläuterung dazu folgt in Kapitel 3.5.3.

Zusammengefasst ist festzustellen, dass die verwendete und weiter entwickelte Methodik sowohl die Schwachstellen identifizieren, als auch auf der IT-Seite die Maßnahmen benennen kann, die der leichten Ausnutzbarkeit entgegenwirken. Wichtig ist festzuhalten, dass die Inhalte immer den jeweiligen Anlagenspezifika angepasst werden muss. 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.

3.5. Auswertung und Aufbereitung (Wasserwirtschaft)

3.5.1. Auswertung Begehungen und Befragungen

Im Nachfolgenden werden die sicherheitsrelevanten Aspekte mit direktem wasserwirtschaftlichem Bezug, die auf den Kläranlagen untersucht wurden, übersichtlich dargestellt und die Risiken priorisiert. Bei der Begehung der Kläranlagen erfolgte zunächst eine Prüfung der allgemeinen Außensicherung, beispielsweise Zutrittskontrollen und Zaunanlagen, und einfacher wasserwirtschaftlicher Aspekte. Dabei wird sich an DVGW W 1050 Merkblatt 11/2019: „Objektschutz von Wasserversorgungsanlagen“ orientiert. Ein analoges Merkblatt gibt es für Abwasseranlagen bisher nicht. Folgende Abbildung 3-22 zeigt den Anteil der untersuchten 13 Kläranlagen, die relevante Sicherheitsaspekte (nicht) erfüllen.

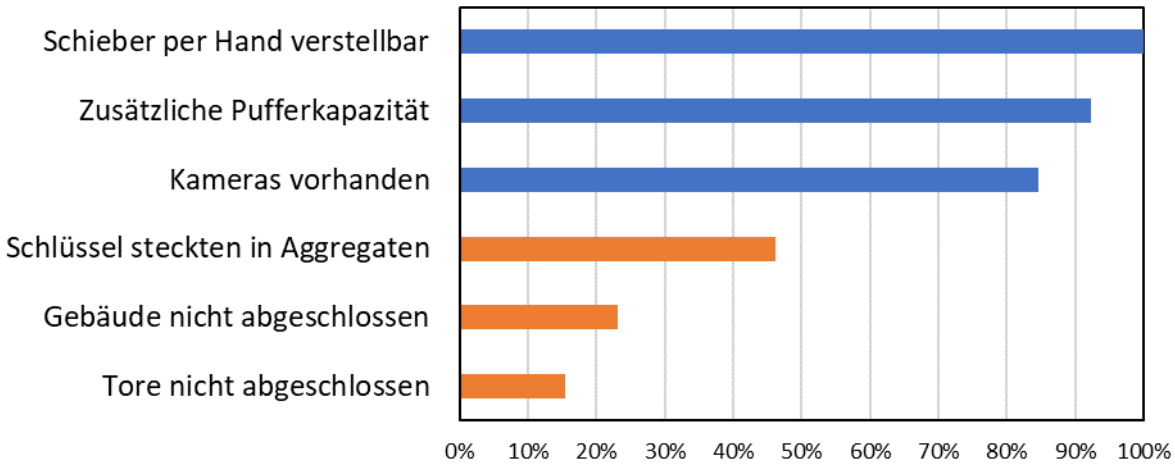


Abbildung 3-22: Identifikationen von Schwachstellen - allgemeine relevante Sicherheitskonzepte (blau – positiv, orange – negativ).

Auf allen Kläranlagen sind per Hand verstellbare Schieber vorhanden. Diese sind notwendig um auf Ausfälle des PLS oder Cyberangriffe zu reagieren aber insofern problematisch, dass an diesen durch physisches Bedienen ein einfacher Eingriff in die Verfahrenstechnik möglich ist. So können beispielsweise Rücklaufströme unterbrochen werden. Zusätzlich sind diese Schieber zumeist nicht über IT-Schnittstellen mit Alarmsystemen gekoppelt, wodurch eine Veränderung nur bei einer Kontrolluntersuchung auffallen kann. An einigen Kläranlagen hätten durch diese Schieber-Verstellung innerhalb kürzester Zeit Überflutungen des Kläranlagen-Geländes ausgelöst werden können. Daher sollte bei kritischen Schiebern darauf geachtet werden, dass diese an ein Alarmsystem gekoppelt werden. Weiterhin sollten alte Schieber, welche nicht mehr im Gebrauch sind abgebaut oder so eingestellt werden, dass sie keinen Schaden anrichten können.

Abbildung 3-23 zeigt verschiedene Ausführungen von Schiebern. Zu sehen ist, dass einige Schieber physisch einfach zu verstellen sind und dies nur durch Knopfdruck oder komplett ohne Sicherung möglich ist. Die optimale Ausführung ist hierbei eine Ausführung mit Schlüsselschalter wie im nachstehenden Bild rechts gezeigt. Die Sicherung des Umschaltens vor Ort von Automatik- auf Handmodus kann alternativ auch über Vorhängeschlösser an einem Wahlschalter erfolgen. So wird ein vor äußeren physischen Eingriffen gesicherter Handbetrieb ermöglicht. Wichtig ist, dass kein Drehantrieb ohne Handrad vorhanden ist, damit ein Handbetrieb möglich ist. Weiterhin gibt es Steuerungen, welche nur über das PLS in den Handbetrieb wechseln können und somit eine rein händische Umschaltung blockiert ist. Eine solche Schaltung sollte vermieden werden, damit die Handsteuerung bei Komprimierung der IT möglich ist.

Zudem muss bei Schlüsselschaltern darauf geachtet werden, dass diese möglichst witterungsgeschützt ausgeführt sind und Korrosionsschäden durch regelmäßige Wartungen

vermieden werden. Weiterhin ist es notwendig - damit Schlüssel nicht stecken bleiben - möglichst wenige Schlüssel für die Schieber zu benötigen. Eine Lösung dafür können auch andere digitale Instrumente sein, mit denen die Schieber zu betätigen sind.

Abbildung 3-23: Arten von Schiebern: links: Schieber nur mit Handrad ohne elektrischen Anschluss (Handrad befindet sich am Schieber), oben rechts: elektrischer Schieber mit Handrad und Druckknopf zur Änderung auf den Handbetrieb, unten rechts: elektrischer Schieber mit Schlüssel für Handverstellung. (eigene Aufnahmen)

Sind reine Handschieber (vgl. Abbildung 3-23 links) und diese an kritischen Stellen verbaut, sollten sie so abgesichert werden, dass kein Eingriff möglich ist. Dafür kommt eine Absicherung durch Schlösser, Ketten oder ggf. auch ein Abbau in Frage.

Ein positiver Aspekt ist die zusätzliche Pufferkapazität, die auf vielen Anlagen vorhanden ist. Dies sind beispielsweise Becken aus altem Bestand, die bei einer Betriebsstörung gefüllt werden können und ermöglichen bei Angriffen, welche bspw. eine längere Reparaturdauer erfordern, Abwasser zurückzuhalten.

Für die Außenschutzsicherung und Überwachung sind über 80 % der Kläranlagen mit Kameras ausgestattet. Diese haben einen abschreckenden Charakter und können Angriffe vorbeugen, aber auch bei einer möglichen Problemsuche helfen. Selbst zur Abschreckung verbaute Kamera-Attrappen können für die Vorbeugung physischer Angriffe hilfreich sein. Vorhandene Kameras sind aber nicht zwingend positiv zu bewerten. Hier kommt es im Nachgang darauf an, ob und wie die Kameras im System integriert sind und in wie fern eine Absicherung der Oberflächen realisiert ist. Ansonsten könnten Angreifer diese nutzen.

Weiterhin wurde festgestellt, dass auf fast 50 % der Anlagen vereinzelt Schlüssel in Aggregaten - wie Steuerungspanelen von Schiebern oder Pumpen - steckten. Dadurch können ohne Probleme teils massive Auswirkungen auf die Kläranlagen erzeugt werden. Zudem steckten teilweise Schlüssel, die auch für die meisten anderen Aggregate der Kläranlagen passten. Dies ist ein einfacher Sicherheitsaspekt der auf allen Kläranlagen enger kontrolliert werden sollte. Gleiches gilt für unabgeschlossene Gebäude. Dies wurde mehrmals auf Kläranlagen beobachtet und auch mehrfach als aufgefallene Störung bei Besichtigungen festgestellt. Die Betriebsgebäude waren davon nicht betroffen. Schnelle Abhilfe ist durch die Nachrüstung von Türschließern oder den zukünftigen Einbau von selbstverschließenden Türen zu empfehlen. Zusätzlich muss stärker auf die erste Barriere, sprich die Zugangstore und -türen, geachtet werden. Diese waren nur auf wenigen Anlagen verschlossen, wodurch ein Eindringen auf die Anlagen auch tagsüber kein Problem darstellte und ohne Kontrolle erfolgen konnte. Der häufigste angeführte Grund waren mangelnde Kapazitäten für die Kontrolle der Besucher.

Ein weiterer wichtiger sicherheitsrelevanter Aspekt ist das Vorhandensein von Notstromaggregaten. Bei einem Großteil der Kläranlagen ist ein Notstromaggregat vorhanden. Lediglich bei einer Anlage war kein Notstromaggregat vorhanden, allerdings ist der Bau in Planung. Unterschiede waren u.a. bei der Instandhaltung sichtbar. Die für den schnellen Einsatz notwendige Vorheizung des Notstromaggregates war nicht durchgehend der Fall. Die Funktionsprüfung der Notstromaggregate wurden bei über ¾ der Kläranlagen regelmäßig durchgeführt (s. Abbildung 3-24). Die Abstände variierten allerdings von Viertel jährlich bis monatlich.

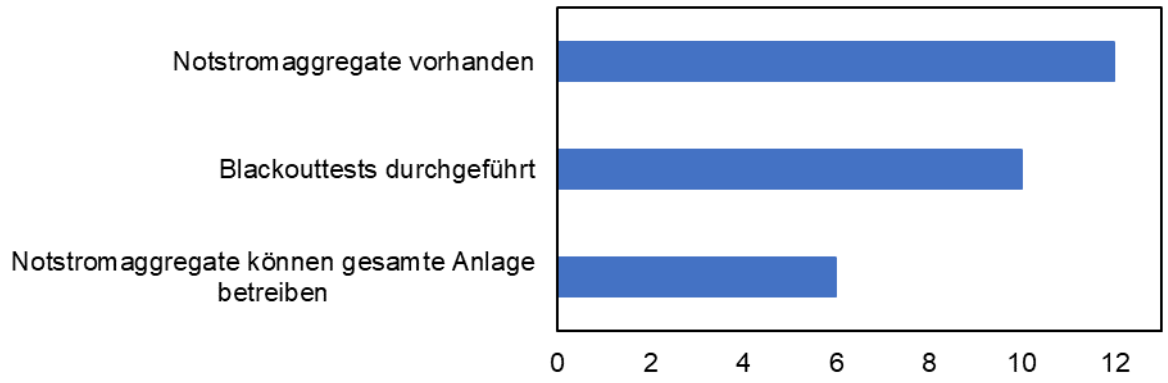


Abbildung 3-24: Identifikation von Schwachstellen – Stromausfall.

Berichtet wurde auch, dass erst durch die Blackouttests regelmäßig (Folge-)Probleme gefunden wurden, welche anschließend behoben werden konnten. Dies zeigt die Wichtigkeit der Tests auf. Blackouttests, bei denen die gesamte Anlage vom Netz genommen wurde, fanden hingegen nur bei ungefähr der Hälfte der Aggregate statt. Dies sollte auf allen Anlagen

ebenfalls regelmäßig durchgeführt werden. Ein Beispiel liefert dafür eine der Kläranlagen, bei der zwar das Notstromaggregat funktionierte, dieses aber bei einem Stromausfall nicht anlief und somit seiner Funktion nicht gerecht werden konnte. Weiterhin ist rund die Hälfte der Notstromaggregate so ausgelegt, dass nur der Wasserweg aufrechterhalten wird (der Schlammweg nicht) und so nur eine rudimentäre Abwasserreinigung stattfinden kann. Dies kann bei Ausfällen von mehreren Stunden problematisch sein, da gleichzeitig auf den wenigsten Kläranlagen für Stromausfälle vorgegebene Anschlüsse für eine externe Notstromversorgung durch beispielsweise das THW gegeben sind. Welche Anschlüsse gefordert sind, muss mit dem lokalen THW abgestimmt werden. Dieses Szenario ist mit einem Angriffsszenario zu vergleichen, bei dem die Belüftung ausfällt und würde zu denselben Konsequenzen für die Ablaufwerte und mögliche Implikationen für die Biozönose führen. Hier ist eine Absprache mit Hilfswerken oder ähnlichen Organisationen in der Nähe der Kläranlage notwendig, um einen abgestimmten Notfallplan zu haben. Einen weiteren kritischen Punkt stellt die Versorgung der Notstromaggregate mit Diesel oder Gas dar. Zumeist existieren keine Reserven für die Kläranlagen. Hier könnte durch Kontakt mit lokalen Versorgern und Tankstellen ebenfalls für eine Sicherheit für längere Ausfallzeiten geschaffen werden. Vorab sollte Kontakt zum lokalen Krisenstab aufgenommen werden, um die dortige Verteilung der Treibstoffversorgung anzufragen. Dies wird in den regelmäßig stattfindenden Krisenstabsübungen behandelt. Die meisten Kläranlagen haben genug Reserven vor Ort, um den Wasserweg für mehrere Tage aufrechtzuerhalten. Ein Kläranlagenbetreiber machte darauf aufmerksam, dass der Versuch unternommen wurde, eine Reserve zu schaffen, aber dass es in der Umgebung dafür keine Kapazität gab. Bei einem mehrtägigen Stromausfall sind somit die meisten Kläranlagen nicht mehr aus eigener Kraft betreibbar. Als zusätzliche Reserve könnte auch die eigene Stromversorgung genutzt werden. Allerdings ist bei den meisten Anlagen die Notstromversorgung nicht darauf ausgelegt, ihr eigenes Gas zu verbrennen. So könnte auch Strom von eigenen Photovoltaik- oder Windkraftanlagen genutzt werden.

Ein unerlässlicher Punkt für die Kontrolle des Ausfalls der Notstromversorgung oder anderer Angriffe auf eine Kläranlage ist die regelmäßige Kontrolluntersuchung an Wochenenden und Feiertagen. Die Inhalte und die Häufigkeit von Kontrolluntersuchungen werden in NRW in der Selbstüberwachungsverordnung kommunal (SüwV-kom) definiert. In dem Zeitraum ohne Kontrolluntersuchung ist die Anlage unbewacht und erhöht das Risiko eines möglichen Angriffes und das Ausmaß der Folgen. Insgesamt werden 12 der 13 Kläranlagen innerhalb von 24 h an Wochenenden und Feiertagen begangen. Somit findet an jedem Tag im Jahr eine Kontrolluntersuchung der Kläranlage statt. Lediglich eine Kläranlage wird an Feiertagen und Wochenenden nicht besichtigt. Dies entspricht den geforderten Zeiten nach SüwV-kom, bietet allerdings ein großes Zeitfenster für mögliche Angriffe (s. Abbildung 3-25).

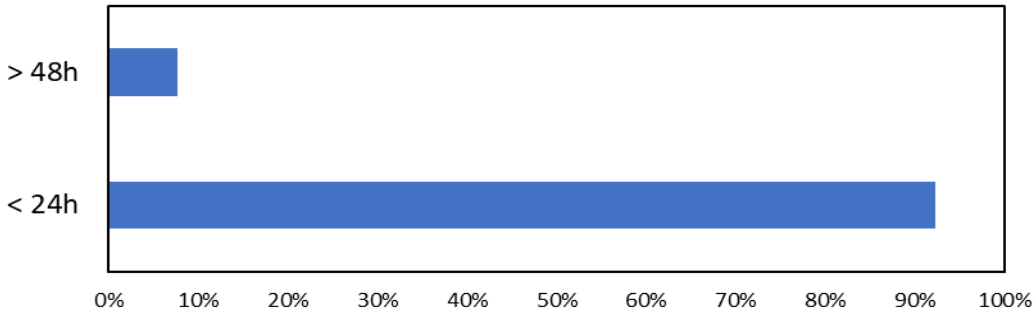


Abbildung 3-25: Anteil an Kläranlagen, welche in einem Zeitraum von über 48 h bzw. 24 h nicht begangen werden.

Der Inhalt der Kontrolluntersuchungen unterschied sich dabei deutlich zwischen den Kläranlagen. Als Resultat der Befragungen kann gezogen werden, dass wenn der Umfang einer Kontrolluntersuchung zunimmt, tendenziell eher etwas übersehen wird. Aufgrund negativer Erfahrungen bei den Kontrolluntersuchung, bspw. dass einzelne Punkte der Anlage vergessen wurden, wurden auf einigen Anlagen Kontrolluntersuchungsprotokolle eingeführt. Diese beinhalteten teilweise nur Listen zum Abhaken, zum Teil mussten aber auch Werte von Zählern abgelesen werden. Durch letzteres versprachen sich die Kläranlagenmeister:innen sicherzustellen, dass die Angestellten die gesamte Anlage abgehen. Zudem wechselten auf einigen Kläranlagen das Bereitschaftspersonal zwischen Samstag und Sonntag, damit weitere Aspekte auffallen können.

Zwischenpumpwerke (bspw. für den Rücklaufschlamm) sind auf allen Kläranlagen vorhanden. Diese bieten zumeist eine einfache Angriffsfläche, um Überflutungen bzw. Austritte von Abwasser/Schlamm zu erzeugen. Nachfolgende Abbildung 3-26 zeigt ausgewählte mögliche Angriffspunkte an den untersuchten Kläranlagen.

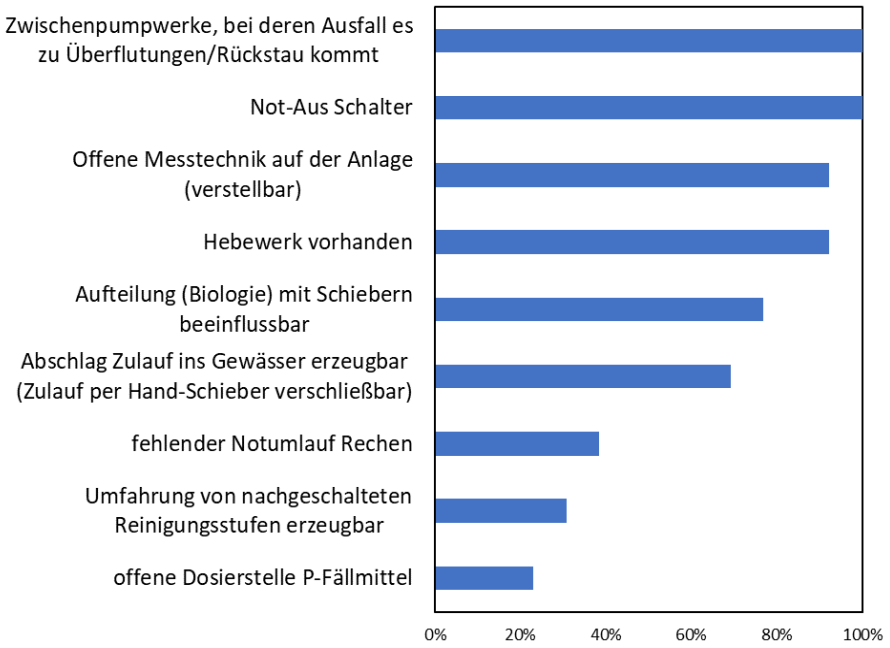


Abbildung 3-26: Anteil an Kläranlagen, mit abwasserwirtschaftlich problematischen Angriffspunkten.

Häufig ist durch das Herunterdrehen eines Schiebers der Ablauf verschließbar und die Pumpen würden anschließend das Abwasser über die Schwellen befördern, sodass dieses austreten würde. Im Betrieb sollten solche kritischen Schieber in das Alarmsystem mit aufgenommen werden und eine Veränderung von beispielsweise dem Automatik- in den Handbetrieb sofort zu einer Störmeldung führen. Auf den meisten Kläranlagen sind ebenfalls Hebewerke für den Abwasserstrom vorhanden. Bei diesen Bauwerken gelten dieselben Gefahren wie bei den Zwischenpumpwerken. Zusätzlich können aber auch durch Rückstaue Schäden entstehen oder Abschläge in Gewässer resultieren.

Aus Arbeitssicherheitsgründen sind auf allen Kläranlagen Not-Aus-Schalter vorhanden. Diese bieten bei Einbruch auf einer Kläranlage die einfachste Möglichkeit, Einfluss auf die Verfahrenstechnik der Abwasserreinigung zu nehmen. Da ein simples Drücken der Schalter i.d.R. aber auch ein Alarm verursacht, kann hierauf schnell reagiert werden. Diesem Angriffspunkt wird daher eine geringe Relevanz zugemessen, solange das Alarmsystem nicht auch ausgeschaltet wird.

Eine weitere Angriffsstelle bietet die auf den Kläranlagen verbaute Messtechnik, da diese meistens offen verbaut und ohne Eingabe von Passwörtern eine Einflussnahme möglich ist. So ist es beispielsweise möglich, dass Skalierungsfaktoren von Messwerten verändert werden und die Anlage somit falsch geregelt wird. Auf diese Weise wäre ein dauerhaft unbemerkter Angriff möglich. Dies würde erst durch länger erhöhte Ablaufwerte auffallen. Ein einfacher Schutz ist bereits durch die Notwendigkeit eines Passwortes möglich oder dem Entziehen von

Schreibrechten auf außengelegenen Bildschirmen. Zusätzlich wurden auf einer Kläranlage offene LAN-Kabel gefunden, mit denen ein direkter Zugriff in das PLS möglich ist.

Zusätzlich zu den Schiebern an den Pumpwerken sind andere wichtige Funktionen von Schiebern die Aufteilungen auf die Belebungsbecken. Erfolgt eine Aufteilung ist dies zumeist durch einzelne nur händisch verstellbare Schieber realisiert. Diese lassen sich i.d.R. einfach verstellen und können zu einer Überbelastung einzelner Becken führen. Wie hoch dieser Schaden ausfällt, ist dann von der unterschiedlichen Größe der Becken und der Auslastung der Kläranlage abhängig. Bei über der Hälfte der Kläranlagen ist ebenfalls ein Schieber im Zulauf der Kläranlage verbaut. Über diese lässt sich der Zulauf regulieren und ein Abschlag in Gewässer erzwingen. Bei mehr als 20 % der Kläranlagen sind diese Schieber nicht in das Alarmsystem eingebunden, wodurch mit einer simplen Verstellung des Schiebers ein direkter Abschlag des Abwassers in den Vorfluter resultiert. Auf diese Schieber sollte ein großer Stellenwert beim Alarmsystem gelegt und es sollte sichergestellt werden, dass hier keine externe Bedienmöglichkeit durch ggf. steckende Schlüssel gegeben ist.

Zwei weitere Punkte sind das Fehlen des Notumlaufs am Rechen oder das Vorhandensein von Notumläufen an weiteren Behandlungsverfahren. Sind Umgehungen vorhanden, sind diese meist relativ einfach über Schieberstellungen verwendbar und es kann teilweise erheblich in den Reinigungsprozess eingegriffen werden. Sind diese nicht vorhanden, wie am Rechen, könnte es durch den Ausfall des Rechens zu einem Rückstau oder zu einer Überflutung kommen. Notumläufe sind für den Betrieb von Kläranlagen und Wartungsarbeiten notwendig, allerdings sollte darauf geachtet werden, dass diese nicht mit wenig Aufwand unbemerkt Schaden verursachen können.

Als letzter Punkt sind offene Phosphorfällmitteldosierstellen aufzuführen. Auf einigen Kläranlagen wurden offene Ventile für die Zuführung des Fällmittels verbaut, wodurch diese ohne großen Aufwand zugedreht und so eine Fällmittel Dosierung verhindert werden kann. Dies kann je nach Dosierort und Phosphorbelastung einen erheblichen Einfluss auf die Ablaufwerte haben.

Insgesamt zeigen diese Angriffspunkte, dass viele Probleme durch eine andere Bauausführung oder ein Alarmsystem verhindert werden können. Auf einigen Kläranlagen wurde dabei festgestellt, dass sich bei der Ausführung des Alarmsystems keine Gedanken dazu gemacht wurden, dass auch ein Angriff geschehen kann oder wodurch Schäden entstehen könnten. Häufig wurde eine Veränderung eines gemessenen Parameters aufgenommen, welcher zu einem Schaden führen kann, aber diese Änderung löste keinen Alarm aus.

Aus den Besichtigungen haben sich eine Reihe weiterer Angriffsmöglichkeiten ergeben mit denen ein Schaden auf einer Kläranlage erreicht werden kann. Eine Auflistung aller Betrachteter Fälle ist Tabelle 3-4 zu entnehmen. Des Weiteren werden die direkten Folgen dargelegt und wie viel Prozent der untersuchten Kläranlagen mit der angegebenen Manipulation angreifbar sind.

Tabelle 3-4: Anteil an Kläranlagen, die von möglichen Angriffsszenarien betroffen wären.

Ort	Was wird manipuliert	Beispielhafte Folgen (spezifische bei jeder Kläranlage erläutert)	Anteil
Zulauf	Messsonde	Keine Infos über hydraulischen und parametrischen Zustand des Zulaufs	85 %
	Zulaufschieber	Zu viel Wasser in der Anlage, hydraulische Überlastung	54 %
		Ungewollter Abschlag von Schmutzwasser in den Vorfluter	54 %
	Abschlagschieber	Ungewollter Abschlag in den Vorfluter	38 %
Zulauf-pumpwerk	Ausfall	Rückstau -> ggf. Überflutungen auf der Anlage oder Abschlag ins Gewässer	92 %
	Manipulation Messsonden	Rückstau -> ggf. Überflutungen auf der Anlage oder Abschlag ins Gewässer	92 %
Rechen	Räumer - Ausfall	Siehe unten	100 %
	Räumer Intervall	Überlauf des Rechens bei Verstopfung	100 %
	Zulaufschieber	Rückstau und möglicherweise Abschlag in den Vorfluter	46 %
	Notumlauf	Grobstoffe gelangen in nächste Reinigungsstufe, auf Dauer ein Problem	69 %
	Veränderung Regelgrößen	Überlauf oder Ausfall des Rechens	100 %
Sandfang	Belüftung aus	Absatz von mineralischen Stoffen am Grund, Versandung weiterer Verfahren	100 %
	Sandabzug aus	s.o.	100 %
	Veränderung Regelgrößen	s.o.	100 %
Vorklärung	Schlammabzug aus	Verschlammung am Grund	54 %
		Verschleppung von Stoffen in die nächste Stufe führt zu Überlastung der Biologie	54 %
	Notumlauf	s.o.	54 %
Zwischen pumpwerk	Ausfall	Überflutungen / Abschläge	69 %
Belebung	Kohlenstoffdosierung	Erhöhte CSB-Ablaufwerte	31 %
	Kaskaden-Bypass zu groß/klein	C-Mangel oder zu viel C u. N-im Ablauf	15 %
	Rührwerk aus	Keine Durchmischung, Hemmung anoxische Prozesse (keine Deni)	100 %
		Schlammabsatz am Grund	100 %
	Belüftung aus	Keine Aeroben Prozesse mehr möglich (keine Nitrifikation)	100 %
		Schlammabsatz am Grund	100 %
	Belüftung zu hoch	Verschleppung O_2 in Deni und hohe E-Kosten	100 %
	Manipulation Regelwerte	Keine Kontrolle mehr über biologische Reinigungsleistung	100 %

	Messsonde aus	keine Steuerung möglich oder nur über Vergleichswerte	100 %
		Blindfahrt, Einschränkung Deni/ hohe E-Kosten/keine Nitrifikation	100 %
	Interne Rezirkulation - aus	Zu hohe Nitrat Ablaufwerte	38 %
	Interne Rezirkulation verändert	Zu hohe Nitrat Ablaufwerte	38 %
Phosphor-Elimination	Manipulation Messsonde	Erhöhte P-Ablaufwerte / ggf. Erhöhung pH-Wert	92 %
	Manipulation Dosierung	Erhöhte P-Ablaufwerte / ggf. Erhöhung pH-Wert	15 %
	Manipulation Regelungstechnik	Erhöhte P-Ablaufwerte / ggf. Erhöhung pH-Wert	100 %
Nach-klärung	Aufteilung auf Becken	hydraulische Überbelastung einzelner Becken, Schlammaustrag	77 %
	Räumer aus	Schlammaustrag	92 %
	Rücklaufschlammabzug verändert	Biologie Zerstört durch zu hohen Abzug an Schlamm	100 %
		Biologie verändert durch Änderung des Rücklaufverhältnisses	100 %
	Überschussschlammabzug verändert	Bei Ausfall - Ansammlung TS, kann zu Austrägen führen	100 %
		Bei hohem Schlammabzug, Überlastung oder Überlauf Eindicker Störung Faulprozesse	100 %
Filterstufen	Umfahren der Reinigungsstufe	Für Notfälle gedacht, dauerhaft aber nicht Einhaltung von selbst gesetzten niedrigen Grenzwerten	23 %
	Veränderung Spülung	Falsche Klassierung im Mehrschichtfilter	38 %
Ablauf	Schieber	Zu hohe eingeleitete Abflussmengen	8 %
Spezifische	Dekanter Herabfahren	Austrag von Schlamm	8 %
	Auspumpen aus NKB	Kollabieren der Wände und Austrag Schlamm	8 %

Zuletzt können die beobachteten Angriffspunkte nach der zugehörigen Verfahrensstufe aufsummiert werden (s. Abbildung 3-27). Dabei wird deutlich, dass es an jeder Verfahrensstufe Ansatzpunkte für eine Manipulation gibt. Zudem bieten einige Kläranlagen spezifische Ansatzpunkte an Verfahren, die nicht an jeder Kläranlage verwendet werden. Die meisten Angriffspunkte bietet die Belebung, die das Herzstück der Abwasserreinigung darstellt und deshalb für den Reinigungsprozess integral ist. Es sollte deshalb besonderer Wert auf diese Verfahrensstufe gelegt werden.

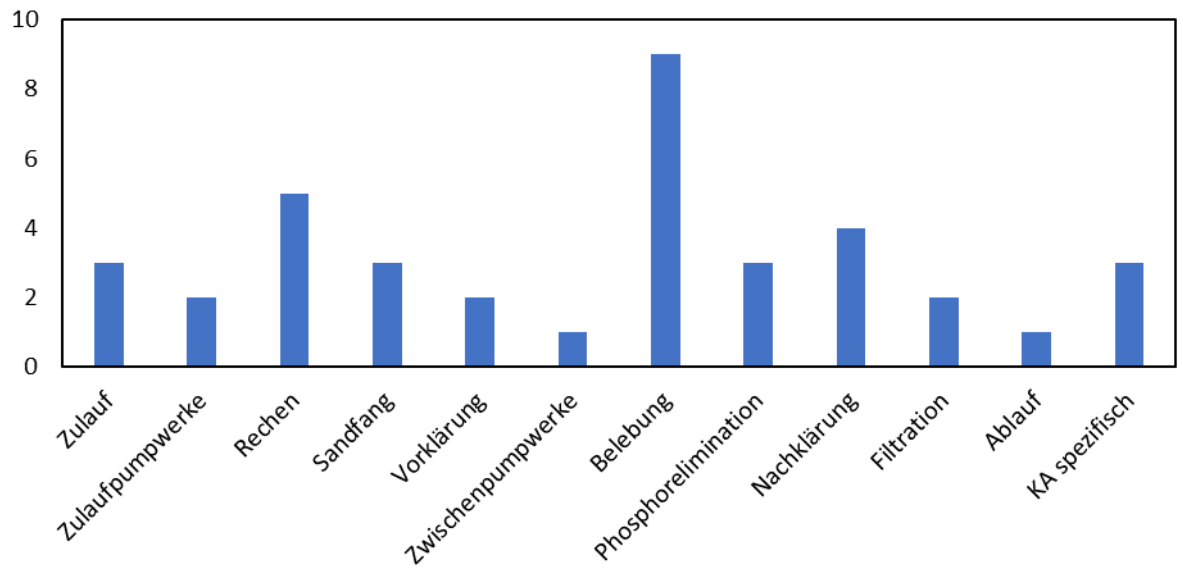


Abbildung 3-27: Identifikation von Schwachstellen – Verfahrensschritte.

3.5.2. Simulation

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 im Vergleich und der Identifizierung der kritischen Vulnerabilitäten unter Berücksichtigung unterschiedlicher Angriffsziele und Szenarien. Darauf aufbauend können Aussagen getroffen werden, auf welche Bereiche mit Sicherheitsmaßnahmen besonders geachtet werden muss. Zudem können diese Szenarien bei zukünftigen Betriebsproblemen oder bei einem Cyberangriff Ideen für eine Fehlersuche geben.

Die Anlagen werden mit den vorhandenen Daten möglichst realitätsnah dargestellt. Für viele Kläranlagen sind allerdings aus dem Betrieb nur begrenzt Daten vorhanden. Auf Basis der eingeschränkten Datengrundlage wurden vereinfachte Simulationen und Modellierungen vorgenommen. Beispielsweise wird die Veränderung der Ablaufwerte der Kläranlage nur über die Stickstoff- und Kohlenstoffkonzentration betrachtet. Die mechanische Reinigung ist nicht Teil einer Simba-Simulation. Angriffe auf diese Verfahrensstufe werden über theoretische Schlüsse bewertet. Gleiches gilt, wenn aus Angriffen Rückstaue ins Kanalsystem oder in Klär- /Überlaufbecken resultieren. Ein beispielhaftes Schaubild einer modellierten Kläranlage ist in Abbildung 3-28 zu sehen.

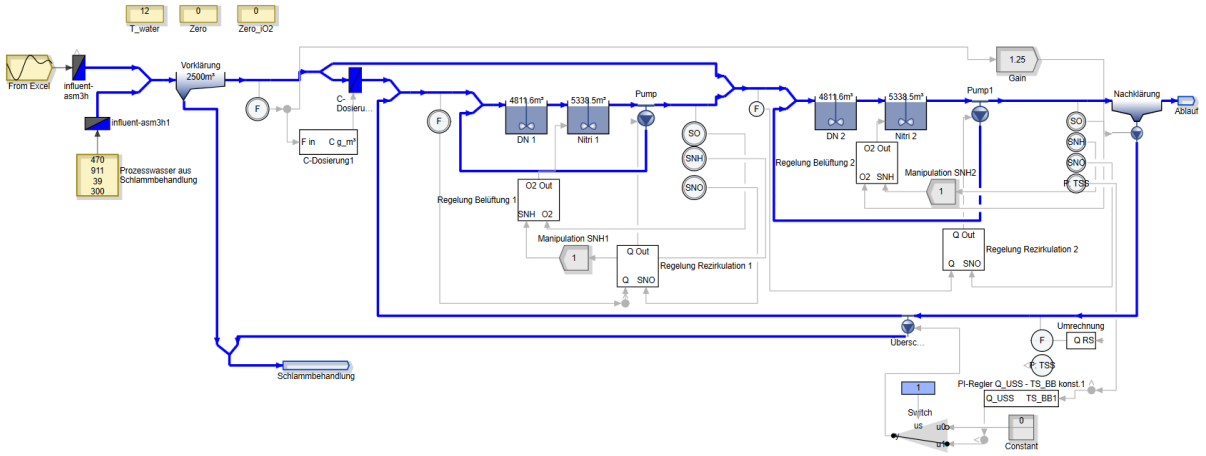


Abbildung 3-28: Beispielhafte Simulation einer Kläranlage inkl. aller Verfahrensschritte mit Hilfe von Simba. (eigene Darstellung)

Modellkalibrierung

Die Modelle wurden zunächst auf alle bekannten Zulaufdaten, Volumina, Wasserführungen und Betriebsparameter eingestellt. Anschließend erfolgte eine Kalibrierung der unbekannten Werte, so dass die Ablaufwerte möglichst nah mit der Realität übereinstimmten.

Dabei wurden die folgenden Schritte durchgeführt:

- Festlegung des Zuflusses mit Hilfe des Hochschulgruppe Simulation (HSG-Sim)-Ansatzes,
- Kalibrierung der Belebung durch Anzahl von Rührbecken und Wahl von Messstellen,
- Menge des Rücklaufschlammes, der internen Rezirkulation sowie des Überschussschlammes.

Verzichtet wurde hingegen auf Grund der geringen Datendichte auf:

- Überprüfung und Plausibilisierung der Zulauffraktionierung,
- Anpassung der gemessenen Parameter an die übermäßige Beprobung an Wochentagen,
- Einbeziehung von Wochenschwankungen,
- Einbeziehung von Jahresschwankungen,
- Einbeziehung von Regenereignissen,
- Einbeziehung von Temperaturschwankungen,
- Einbeziehung der Phosphatfällung.

Viele dieser Parameter können einen erheblichen Einfluss auf die Vulnerabilität der Kläranlagen haben und sollten im Rahmen weiterer Untersuchungen betrachtet werden. Besonders große Unterschiede sind auf Grund der Temperaturabhängigkeit der biologischen Abbauprozesse zwischen den Winter- und Sommermonaten zu erwarten. Ein verstärktes

Risiko geht auch von Cyberangriffen kombiniert mit Regenereignissen durch die erhöhte hydraulische Belastung einher. Dies ist insbesondere für erzwingbare Abschläge relevant, kann aber auch zu schnelleren Schlammabtrieben in einer Anlage führen. Als Vereinfachung wird an dieser Stelle ein trockener Wintertag modelliert. Dafür wird die von der DWA empfohlene Bemessungstemperatur von 12°C gewählt.

Priorität hat in der Kalibrierung das Einhalten der Betriebsparameter, um eine Veränderung dieser darstellen zu können. Nachrangig wird dabei das genaue Erreichen der Ablaufparameter geführt, da die Vulnerabilitäten auch durch prozentuale Zu- und Abnahmen darstellbar sind. Ein beispielhafter Abgleich zwischen den Modellparametern und den Betriebsparametern ist in Tabelle 3-5 zu sehen.

Tabelle 3-5: Beispielhafte Parameter der Kalibrierung eines Kläranlagenmodells.

Parameter	Einheit	Betriebsdaten (TW)	Modell kalibriert
Anmerkungen: Filtration wird nicht modelliert			
Betriebsdaten (Werte für den Winter)			
RV	-	0,5	0,5
$TS_{Belebungsbecken}$	g/l	3,4	3,4
$TS_{Überschussschlamm}$	g/l	5	3,4
$Q_{Überschüssschlamm}$	m³/d	25	205
$Q_{Primärschlamm}$	m³/d	150	150
Mittelwerte Abfluss			
CSB	mg/l	12	13,41
NH_4-N	mg/l	0,29	0,52
NO_3-N	mg/l	0,68	0,67
N_{gesamt}	mg/l	1,76	1,34

Die Validierung des Modells erfolgte anschließend über die gemessenen Ablaufparameter. Ein Abgleich beispielhafter Abflussmesswerte und modellierten Ablaufparameter nach 300 Tagen Einfahrbetrieb sind in Tabelle 3-5 (siehe oben) zu sehen. Wie im Beispiel zu sehen konnten zumeist die Mittelwerte im Abfluss weitestgehend erreicht werden. Für eine genauere Modellierung wären stündliche Zu- und Abflussdaten notwendig gewesen, welche allerdings für keine Kläranlage zur Verfügung standen.

Angriffsszenarien

Die bereits vorgestellten Angriffe können in physischer Form oder als rein digitale Eingriffe durchgeführt werden. Einen noch größeren Schaden kann durch eine Kombination aus beiden Formen verursacht werden, dafür wird aber auch ein größerer Angriffsaufwand benötigt. Zudem muss es sich bei dieser Art um gezielte Angriffe auf Kläranlagen handeln. Hinsichtlich der Qualität und Quantität der Vulnerabilität zwischen erfolgreichem Angriff und Identifikation

sowie Behebung spielen viele Faktoren eine wesentliche Rolle. Die Dauer eines Angriffes ist der relevanteste Faktor. Dafür werden drei Szenarien betrachtet: Bereitschaftsstörung (Simulationsdauer 4 h), Wochenendangriff (Simulationsdauer 24 h) und ein versteckter Angriff (Simulationsdauer 7 d). Die Szenarien wurden in Kapitel 3.3 bereits ausführlich erläutert.

Ergebnisse

Für die Modellierung der Angriffe wurde jeweils ein Grunddatensatz gewählt, in dem die Kläranlage über 300 Tage eingefahren wird. Anschließend werden die verschiedenen Angriffe mit den unterschiedlichen Dauern modelliert. In Tabelle 3-6 sind beispielhafte Angriffe und die Form der Umsetzung in der Modelliierung aufgezeigt.

Tabelle 3-6: Beispielhafte Angriffe und deren Umsetzung in der Modellierung.

Ort	Angriff	Umsetzung in Modellierung	Szenarien
Zulaufpumpwerk	Ausfall	Keine realistische Abbildung möglich	
Rechenanlage	Ausfall	Keine realistische Abbildung möglich	
Sandfang	Ausfall	Keine realistische Abbildung möglich	
Zwischenpump-werk	Ausfall/ Öffnung des Trennbauwerkschiebers	Keine realistische Abbildung möglich	
Vorklärung	Öffnung Notumlauf	100% in Umleitung	4 h, 24 h
Phosphor-Elimination	Manipulation Sonde	Keine realistische Abbildung möglich	
Belebung	Belüftung-Ausfall	Abschaltung Luftzufuhr	4 h, 24 h
	Belüftung-Manipulation Regelung	Veränderung O2-Sollwerte/ Messwerte	4 h, 24 h, 7 d
		Veränderung Ammonium-Schaltwerte/ Messwerte	4 h, 24 h, 7 d
	Rührwerke-Ausfall	Keine realistische Abbildung möglich	
Nachklärung	Schlammabzug	Ausfall RLS Pumpwerk	4 h, 24 h
		Veränderung RLS Abzug	4 h, 24 h, 7 d
		Ausfall ÜSS Abzug	4 h, 24 h
Filtration	Ausfall	Keine realistische Abbildung möglich	

Für die Bewertung der Anfälligkeit der Anlage gegenüber Angriffen werden die simulierten Ergebnisse mit den Werten des Erlaubnisbescheides und den erklärten Werten verglichen. Die folgende Auswertung erfolgt in einem drei Stufen System. Mit grün werden die Szenarien gekennzeichnet, aus denen kaum bemerkbare Veränderungen der Ablaufparameter

resultierten. Mit gelb ist gekennzeichnet, wenn es bereits zu einer deutlichen Zunahme der Parameter kommt, diese aber noch nicht die erklärten Werte überschreiten. In Rot ist schließlich dargestellt, wenn es zu einer Überschreitung der erklärten Werte/ der Werte des Erlaubnisbescheides kam.

3.5.3. Ergebnisse Simulation

Ein Beispiel für die Ergebnisse der Simulation ist in Tabelle 3-7 gegeben. Zu sehen ist die Bewertung mit grün, gelb und rot für die Überschreitung der erlaubten Ablaufwerte. Zudem ist zusätzlich eingetragen nach wie vielen Stunden eine Überschreitung der Grenzwerte im Modell festgestellt wurde.

Tabelle 3-7: Simulationsergebnisse der unterschiedlichen Angriffsszenarien differenziert nach den Reinigungsstufen.

Ort	Angriff	4 h	24 h	7 d
Belebung (Belüftung)	Bypass leitet gesamtes Abwasser in 2.Stufe			Nach 13 h
	Abschaltung der Luftzufuhr		Nach 7 h	
	Veränderung NH_4-Messwerte +50 %			
Nachklärung	Ausfall Rücklaufschlamm Abzug			Nach 14 h
	Ausfall Überschussschlammabzug Abzug			
Kombinierter Angriff	“Worst case”	Nach 3,5 h		

Die Auswertungstabellen der Kläranlagen zeigen dabei wie das Beispiel, dass es bei allen Kläranlagen innerhalb eines Tages zu Grenzwertüberschreitungen im Ablauf kommen kann. Eine Übersicht der kürzesten Dauern auf den Kläranlagen ist in Abbildung 3-29 zu sehen. Dabei ist die Dauer bis zu einer Grenzwertüberschreitung sowohl für Einzelangriffe aus auch für kombinierte Angriffe für jede Kläranlage zu sehen. Bei kombinierten Angriffen, die ein „worst case” Szenario auslösen fallen – wie zu erwarten – die Dauern bis zu

Grenzwertüberschreitungen kleiner aus. Insgesamt können so innerhalb von weniger als 4 Stunden bei ~30% der Kläranlagen eine Grenzwertüberschreitung ausgelöst werden. Damit kann selbst bei dem Auslösen eines Alarmsystems eine Grenzwertüberschreitung nicht ausgeschlossen werden. Dabei ist anzumerken, dass es je nach Wetterlage oder möglichen Spülstößen von Industrieeinleitern bereits in kürzeren Zeiträumen zu Überschreitungen kommen kann. Wenn es zu einem Störfall auf einer Kläranlage kommt sollte deshalb immer ermittelt werden, wie es zu dem Vorfall gekommen ist und die Frage gestellt werden, ob es sich dabei um einen Cyberangriff handeln könnte. Weiterhin ist zu sehen, dass es bei allen kombinierten Angriffen zu einer Dauer < 24 h kommt und somit immer Grenzwertüberschreitungen innerhalb des Zeitraumes zwischen Kontrollgängen entstehen können.

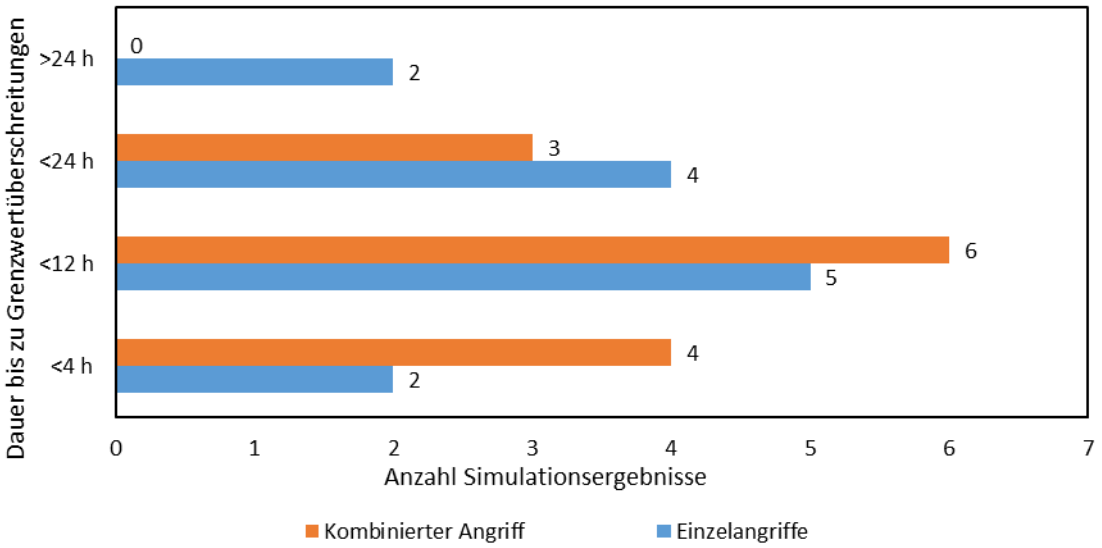


Abbildung 3-29: Simulationsergebnisse – Anzahl der simulierten Dauern bis zur Überschreitung von Grenzwerten.

Werden die Verfahren verglichen, bei denen es am ehesten zu den Grenzwertüberschreitungen kommt, zeigt sich das in Abbildung 3-30 dargestellte Bild. Bei allen Kläranlagen zeigt sich, dass der Ausfall der Belüftung und der Ausfall des Rücklaufschlamm-(RLS)-Abzuges (analog zu Ausfall der zugehörigen Pumpen, Ausfall der Räumer oder Herabfahren eines Dekanters) die kritischsten Bereiche auf allen Kläranlagen darstellen. Alle anderen möglichen kritischen Angriffspunkte sind für jede Kläranlage unterschiedlich und variieren mit dem genauen Design der Anlage und können nicht verallgemeinert werden. Für die Veränderungen von Regelungsparametern wurden in der Simulation mit geringen Abweichungen gerechnet. Die Analyse zeigte, dass die Auswirkungen unterschiedlich groß ausfallen, von der Höhe der Abweichung abhängig sind und erst nach längerer Zeit auftreten. Eine Erkennung von einer Hintergrundmanipulierung ist beispielsweise durch Beobachtungen des Blasenbilds möglich oder der Kontrolle von Belüftungszeiten.

Weiterhin müssen auch langfristige Effekte beobachtet werden, welche nicht modelliert werden können. Beispielsweise kann es zu einer Schädigung der Biozönose des Belebtschlammes kommen, wenn diese längere Zeit ohne Sauerstoffzufuhr bleibt. So ist bereits bei einem Ausfall der Belüftung von mehr als 8 Stunden - je nach Bakterienkultur - mit nicht reversiblen Einflüssen auf den Belebtschlamm zu rechnen. Sehr robuste Belebtschlämme können bis zu 5 Tage ohne Sauerstoff auskommen.

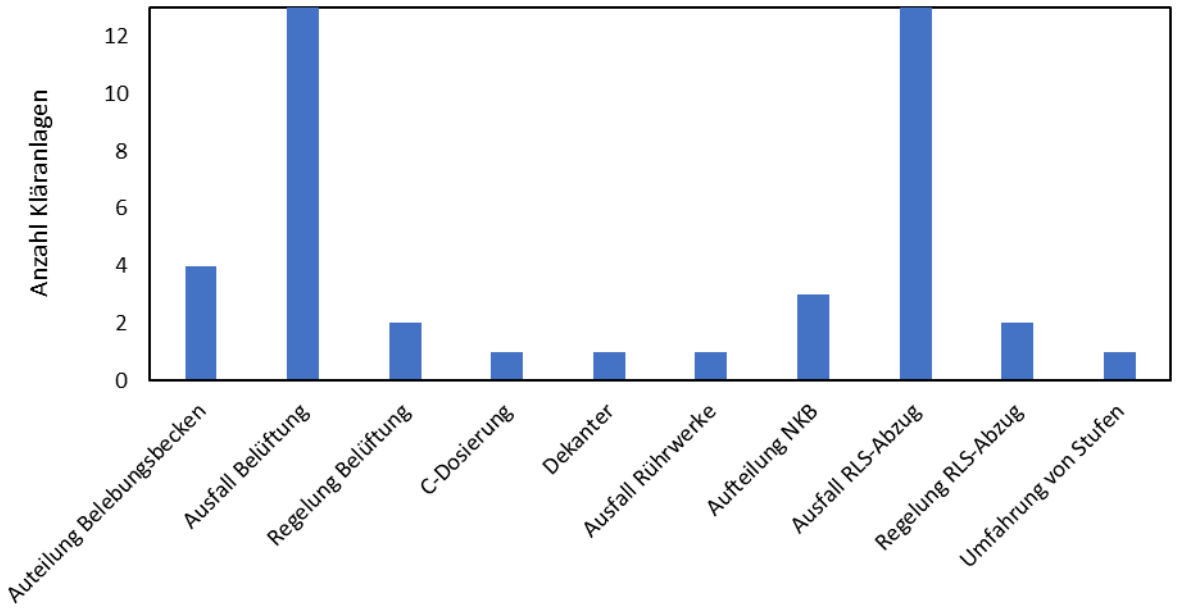


Abbildung 3-30: Simulationsergebnisse - Kritische Bereiche mit erhöhten Ablaufwerten.

Neben den erhöhten Ablaufwerten lassen sich auch die kritischen Bereiche für die Auslösung von Überflutungen oder Abschlägen aufzeigen. Diese sind in Abbildung 3-31 dargestellt. Zu sehen ist, dass es hier keinen einzelnen Fall gibt, der auf allen Kläranlagen vorliegt. Allerdings stellen die Pumpwerke die kritischsten Bereiche dar. Auf allen untersuchten Kläranalgen waren Zulauf- oder Zwischenpumpwerke zu finden, bei deren Ausfall aus dem Rückstau Überflutungen oder Abschläge resultieren würden. Daher sollte sehr auf den dauerhaften Betrieb dieser geachtet werden, oder dass ein stromloses verfügbares Puffervolumen davor verfügbar ist. Die anderen Bereiche konzentrieren sich hauptsächlich auf falsche Einstellungen von Schiebern. Ob von Schiebern Gefahren ausgehen, ist stark vom Kläranlagenaufbau abhängig und davon, ob diese händisch oder elektronisch gesteuert sind. Vor- und Nachteile davon sind, dass diese durch einen Cyberangriff steuerbar sind, aber gleichzeitig auch, dass eine Verstellung durch ein Alarmsystem entdeckt werden kann. Dabei wurde bei den Kontrolluntersuchungen häufig beobachtet, dass Schieberstellungen nicht mit in Alarmsysteme aufgenommen werden, auch wenn Sie in kritischen Bereichen installiert waren.

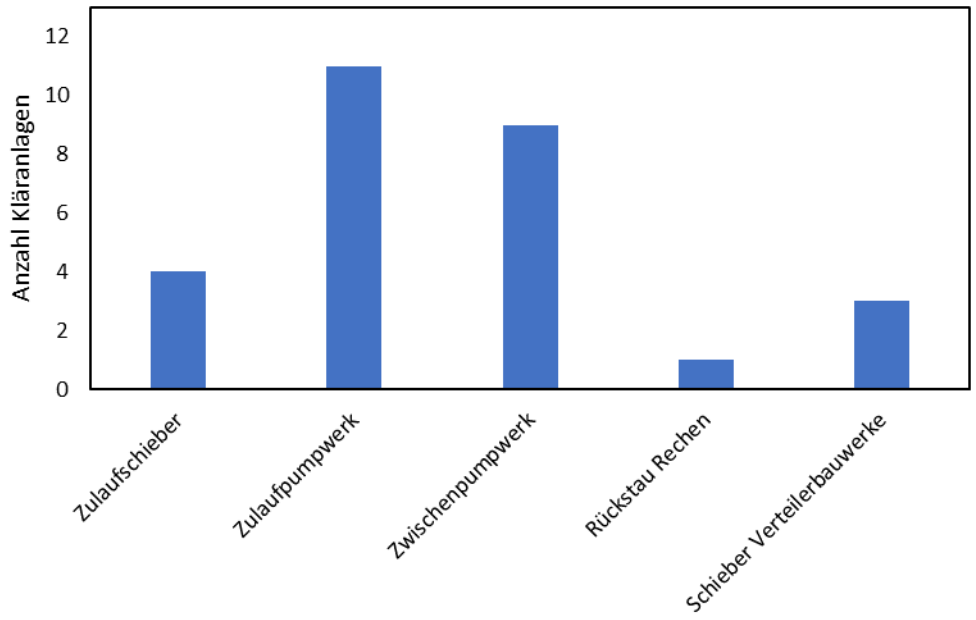


Abbildung 3-31: Simulationsergebnisse - Kritische Bereiche Überflutungen.

Die weiteren Angriffsszenarien für die keine realistische Abbildung mit der Modellierung möglich sind können ebenfalls zu erheblichen Schäden führen. Als Beispiel sei der Ausfall von Rührwerken in der Belebung zu nennen. Auf einigen Kläranlagen, die komplett durch Belüfter durchmischt werden, spielt dies keine Rolle. Werden beispielsweise auf Kläranlagen reine Denitrifikationsbecken genutzt, kann durch den Ausfall der Rührwerke auch die komplette Denitrifikation zum Erliegen kommen und schnell die Ablaufwerte erhöht werden. Auch durch mutwillige Demolierung sind Kläranlagen komplett zerstörbar. Sind beispielsweise Becken ineinander integriert (beispielsweise Nachklärbecken in Belebungsbecken), kann durch gezieltes Abpumpen oder Ablassen von Wasser aus diesen Becken ein Kollaps von Wänden erzeugt werden und damit eine komplette Kläranlage langfristig außer Betrieb genommen werden. Diese Angriffe sind ebenfalls individuell und müssen auf jeder Kläranlage evaluiert werden.

Den Kläranlagen wird empfohlen, den jeweils kritischen (in der Auswertung als rot markierten) Bereichen besondere Aufmerksamkeit zu schenken, sowohl bei Kontrolluntersuchungen als auch bei einem zukünftigen Umbau von Verfahren oder der Einrichtung/ Ausbau eines Alarmsystems.

3.6. Fazit

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 und dieses sollte ausgebaut werden. An den kritischen Stellen (beispielsweise Überwachung Schieberstellungen durch Wasserstandsmessungen) sollte dies möglichst durch ein separates unabhängiges Alarmsystem ergänzt werden.

Weiterhin bietet die Handsteuerung von Aggregaten physische Angriffspunkte, aber gleichzeitig auch die Möglichkeit auf Angriffe zu reagieren. Hier muss versucht werden einen 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) zu einem Alarm führen.

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 Durchführungen von „Blackouttests" sind zur Kontrolle der Aggregate dringend zu empfehlen.

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 Kontrolluntersuchung an Wochenenden und Feiertagen können diese nur teilweise ersetzen, sind aber unerlässlich, sollte es zu einem Ausfall der Alarmsysteme kommen. Wie eine Kontrolluntersuchung durchgeführt wird, ist abhängig von der Größe und der Auslastung des Personals. Die Einführung eines Kontrolluntersuchungsprotokolls oder einer Checkliste ist sinnvoll, damit alle kritischen Bereiche beobachtet werden. Zudem bietet bei einem größeren Personalstamm eine Wochenendaufteilung die Möglichkeit, Veränderungen besser zu erkennen.

4. Wasserwirtschaftliche Relevanzanalyse

Das Ziel der wasserwirtschaftlichen Relevanz Analyse ist festzustellen, welche Risiken sich auf der wasserwirtschaftlichen Seite aus den Vulnerabilitäten der abwasserwirtschaftlichen Seite ergeben. Als Fazit werden daraus Priorisierungen von Schutzmaßnahmen und Schutzbedarf abgeleitet.

4.1. Relevanzanalyse der Ergebnisse der SIMBA-Simulation

Aus den Ergebnissen der Simba-Simulation ergeben sich für jede Kläranlage eine Anzahl von Angriffsmöglichkeiten als auch eine Dauer bis zu den Grenzwertüberschreitungen. Insgesamt sind allgemein gültige Aussagen auf Grund der geringen untersuchten Kläranlageanzahl nicht zu treffen. Allerdings können erste Tendenzen ermittelt werden. Bei einer größeren Anzahl von Anlagen könnten die Zusammenhänge besser beurteilt und weitere Aussagen getroffen werden. Dies zeigt sich in den folgenden Grafiken an dem Bestimmtheitsmaß der

Zusammenhänge. Hier konnten bisher größtenteils keine gefestigten Korrelationen aufgezeigt werden. Die Auswertung in diesem Unterkapitel bezieht sich ausschließlich auf die abwasserwirtschaftliche Seite und bezieht Angriffsstellen der IT-Sicherheit sowie Auswirkungen auf Gewässer nicht mit ein. Im Folgenden werden die betrachteten Angriffsmöglichkeiten mit wesentlichen Eigenschaften der Kläranlagen verglichen, um Aussagen zur Priorisierung von Kläranlagen zu treffen.

Kläranlagengröße

Werden die Angriffsmöglichkeiten mit der Kläranlagengröße (vgl. Abbildung 4-1) verglichen, zeigt sich, dass mit der Anlagengröße tendenziell auch die Anzahl der Angriffsmöglichkeiten zunimmt. Dies ist damit zu begründen, dass es bei den größeren Kläranlagen häufig mehr Aggregate gibt, die somit mehr Raum für Veränderungen bieten. Es wird dabei sowohl die Größenklasse aufgezeigt, als auch die angeschlossenen EW, um die Unterschiede in den GK darstellen zu können. Die Kurven zeigen deutlich, dass es bei den Kläranlagen einige Ausreißer gibt, was mit dem individuellen Aufbau der Kläranlagen zusammenhängt. Somit bieten größere Kläranlagen mehr Spielraum, um Schäden anzurichten, welche in Summe längere Reparaturzeiten benötigen oder eher unentdeckt bleiben könnten.

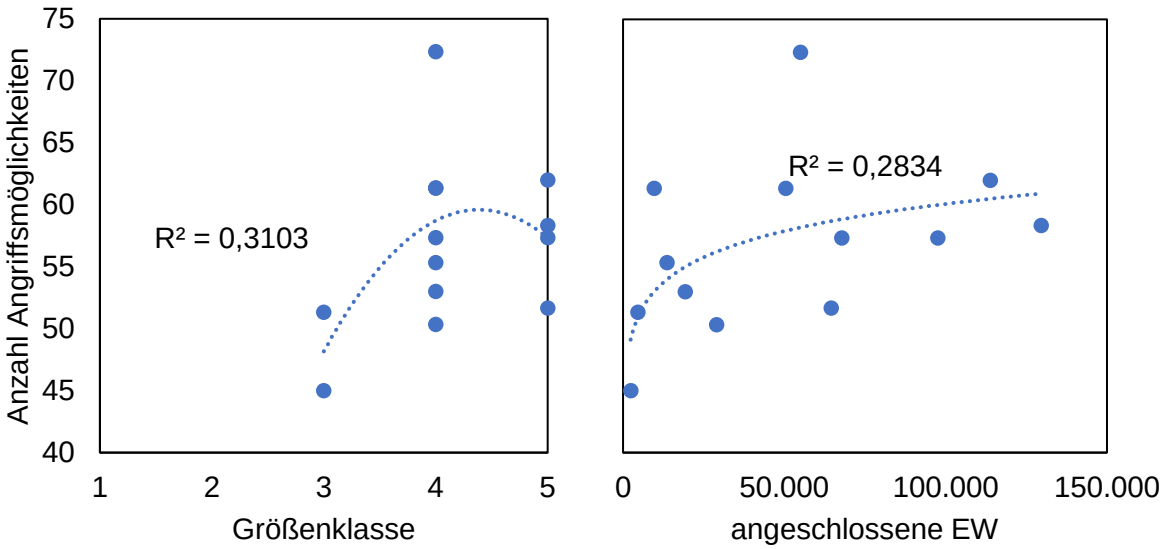


Abbildung 4-1: Vergleich der Angriffsmöglichkeiten mit der Größe der Kläranlagen unter Angabe des Bestimmtheitsmaßes.

Zusätzlich kann die Anfälligkeit der Anlage mit der Anlagengröße verglichen werden. Für die Anfälligkeit wird der Durchschnitt aus den Simulationsergebnissen aller Angriffe gezogen. Dafür wird zunächst jede Angriffsmöglichkeit für jede Angriffsdauer und Kläranlage mit einer Punktzahl bewertet:

- 0 = nicht möglich,
- 1 = keine Betrachtung möglich oder keine Auswirkungen
- 2 = leicht erhöhte Ablaufwerte

- 4 = Überflutungen erzeugt / Ablaufgrenzwerte überschritten

Diese Punktzahlen werden anschließend durch die Dauer des Angriffs geteilt und als Ergebnis der Anfälligkeit der Anlage wird der Durchschnitt für alle Einträge gebildet. Als Ergebnis entsteht eine Zahl zwischen 0 (niedrig) und 0,377 (hoch) welche die Anfälligkeit der Anlage wiedergibt. In Abbildung 4-2 ist der Vergleich zwischen Anfälligkeit und Größe der Kläranlagen zu sehen. Hier ist bei Betrachtung der angeschlossenen Einwohner kein Zusammenhang erkennbar. Werden die Größenklassen betrachtet zeigt sich ein ähnliches Bild wie bei den Angriffsmöglichkeiten. Mit den bisher vorhandenen Daten scheint es somit keinen Zusammenhang zu geben zwischen der reinen Kläranlagengröße und der Anfälligkeit.

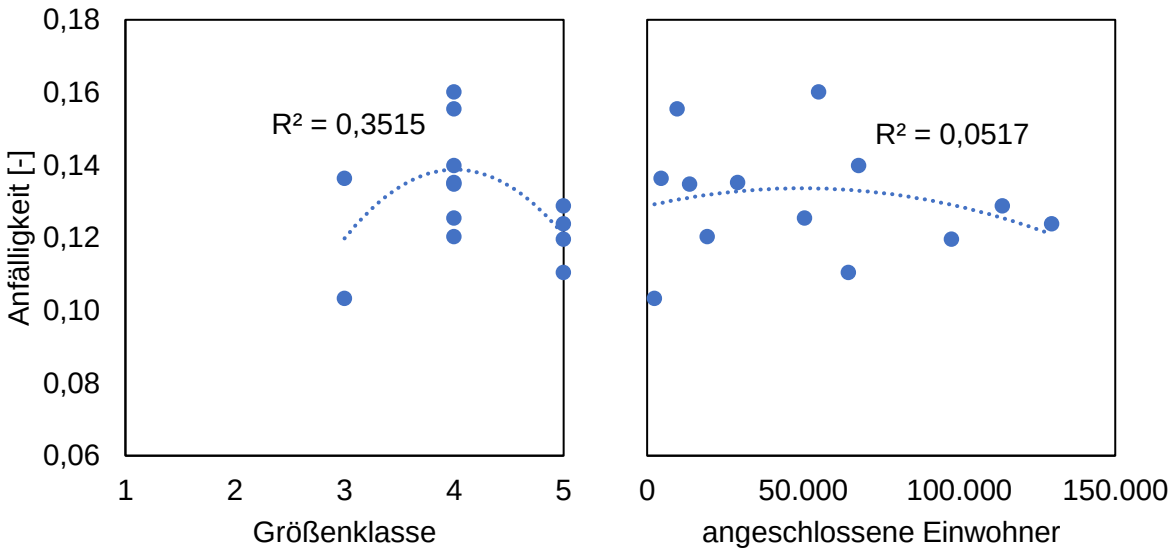


Abbildung 4-2: Vergleich der Anfälligkeit mit der Größe der Kläranlagen unter Angabe des Bestimmtheitsmaßes.

Als letztes kann die Größe der Kläranlagen noch mit der Dauer verglichen werden, welche in der Simulation ermittelt wurde, wann es in einem worst-case Szenario zu einer Überschreitung der Grenzwerte im Ablauf kommt. Diese Ergebnisse sind in Abbildung 4-3 dargestellt. Zu sehen ist, dass besonders die kleineren Kläranlagen eine längere Zeit vorweisen, bis es zu einer Grenzwertüberschreitung kommt. Für eine Erklärung für diesen Zusammenhang können die hydraulische Aufenthaltszeit und die Auslastung der Kläranlagen bessere Hinweise geben.

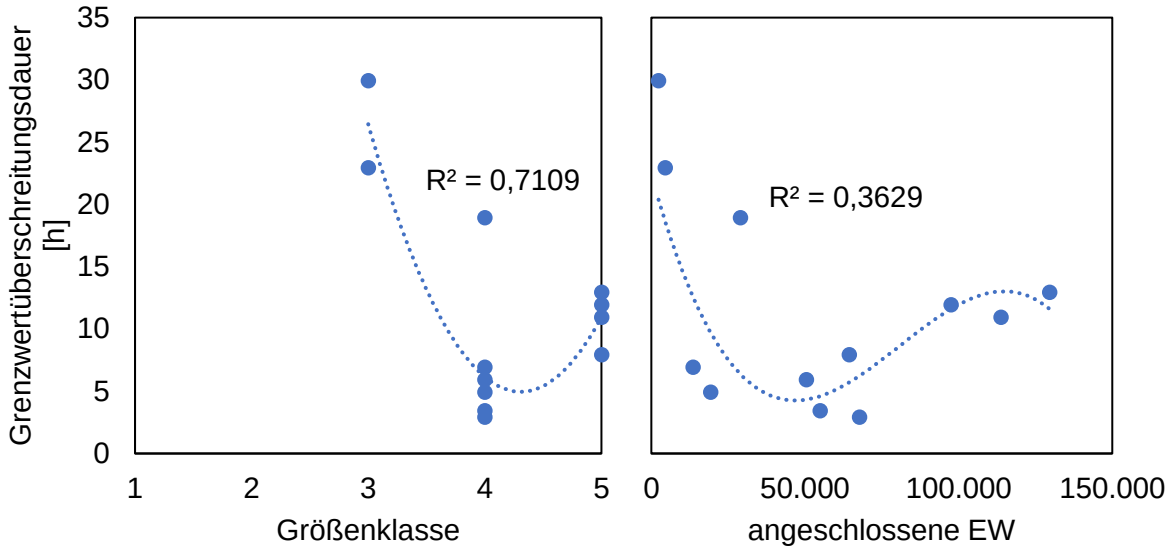


Abbildung 4-3: Vergleich der Dauer bis zur Grenzwertüberschreitung im worst-case mit der Größe der Kläranlagen unter Angabe des Bestimmtheitsmaßes.

Auslastung

Als Auslastung der Kläranlagen wird als Quotient aus angeschlossenen Einwohnern und Ausbaugröße ermittelt. Dies gibt einen Hinweis auf mögliche Pufferkapazitäten in der Kläranlage. Die Annahme ist, dass mit höherer Auslastung eine höhere Anfälligkeit bzw. schnellere Grenzwertüberschreitungsdauern einhergehen. Dafür ist ein Vergleich dieser Parameter in Abbildung 4-4 gegeben. Zu sehen ist, dass die Anfälligkeit der Kläranlage mit der Auslastung ansteigt. Bei der Grenzwertüberschreitungsdauer ist hingegen kein Zusammenhang erkennbar.

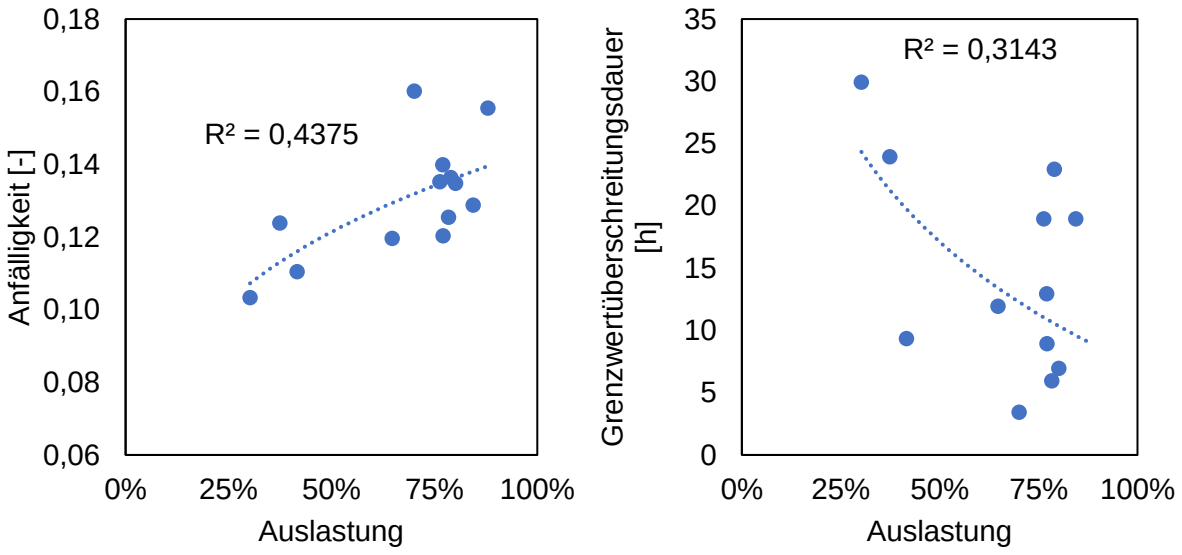


Abbildung 4-4: Vergleich der Anfälligkeit und der Dauer bis zur Grenzwertüberschreitung im worst-case mit der Größe der Kläranlagen unter Angabe des Bestimmtheitsmaßes.

Hydraulische Aufenthaltszeit

Die mittlere hydraulische Aufenthaltszeit vom Abwasser in der Simba-Modellierung enthält nur die Aufenthaltszeit in den biologischen Reinigungsstufen. Diese wurden mit Hilfe der genutzten Volumina und Volumenströme ermittelt. Sowohl der Rechen als auch der Sandfang sowie Zeiten in Leitungen werden vernachlässigt. Da kaum Daten zu stündlichen Messungen vorliegen, wurden die Modelle nicht hydraulisch optimiert. Daher sind diese Angaben nur bedingt aussagekräftig. Die Aufenthaltszeiten in den anderen Reinigungsstufen werden hier nicht weiter berücksichtigt, da diese auch nicht in der Modellierung genutzt wurden.

Ein Vergleich zwischen der hydraulischen Verweilzeit im Modell und der Größenklasse sowie der Grenzwertüberschreitungsdauer ist in Abbildung 4-5 zu sehen. Deutlich wird, dass die hydraulische Verweilzeit nicht mit der Größenklasse zusammenhängt. Ebenso hängt diese nur bedingt mit der Auslastung der Kläranlage zusammen. Der wichtigste Punkt ist der individuelle Kläranlagenaufbau. Wird die hydraulische Verweilzeit mit der Dauer bis zu Grenzwertüberschreitungen verglichen, zeigt sich hingegen ein deutlicherer Zusammenhang. Somit ist diese Dauer insbesondere von der hydraulischen Aufenthaltszeit abhängig. Auch bei einem Vergleich mit der Anfälligkeit zeigt sich, dass diese mit der hydraulischen Aufenthaltszeit absinkt, da diese in die Anfälligkeit durch die Grenzwertüberschreitungsdauer einfließt.

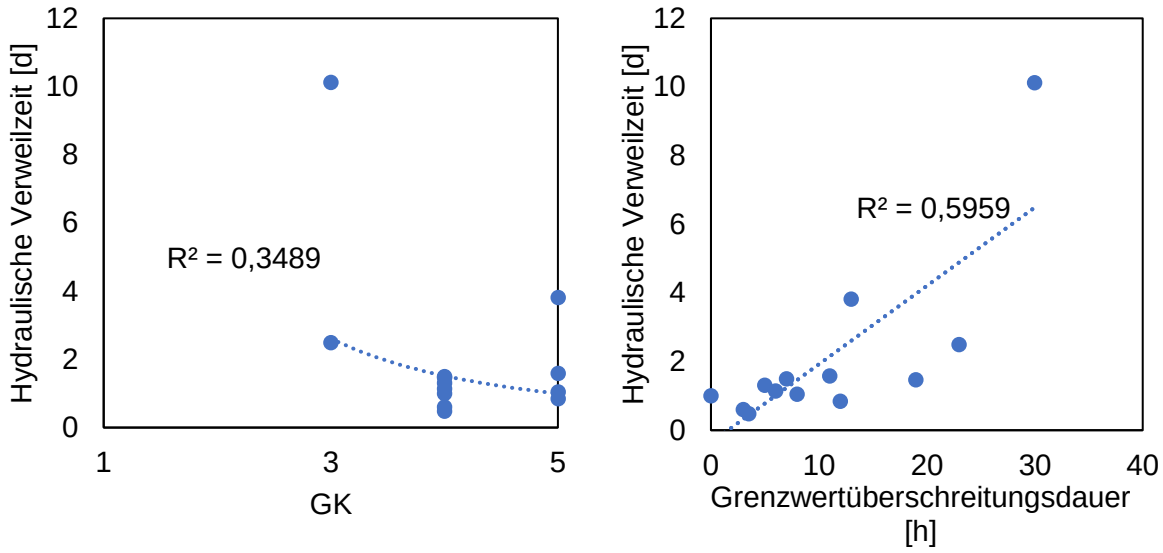


Abbildung 4-5: Vergleich der GK und der Dauer bis zur Grenzwertüberschreitung im worst-case mit der hydraulischen Verweilzeit unter Angabe des Bestimmtheitsmaßes.

Belebungsverfahren

Ein Vergleich zwischen den genutzten Hauptverfahren der Belebung ist auf Basis der bisher durchgeführten Analysen nicht möglich. Bei den klassischen Verfahren der simultanen, intermittierenden, alternierenden, Kaskaden, nachgeschalteten oder vorgeschalteten Denitrifikation konnten keine Unterschiede festgestellt werden. Hier wird aber vermutet, dass

es Unterschiede geben könnte. Beispielsweise durch die notwendige Rezirkulation bei der vorgeschalteten Denitrifikation gibt es mehr Angriffsstellen und die Denitrifikation würde bei einem Ausfall der Rezirkulation schnell zu erhöhten Nitratablaufwerten führen.

Da Membranverfahren bisher nicht betrachtet wurden, kann hierzu keine Aussage getroffen werden. Der Vergleich zu SBR-Anlagen zeigt, dass die SBR Anlagen durch den Batchbetrieb und das dafür notwendige Pufferbecken ein hohes Rückhaltevermögen aufweisen. Ob diese Pufferkapazität allerdings im Angriffsszenario genutzt wird und ob das Abwasser zurückgehalten werden kann, ist stärker von der Steuerung oder von Absicherungen abhängig als bei den konventionellen Verfahren. So könnte es möglich sein, dass das Schlamm-Abwasser Gemisch direkt über einen Dekanter ausgetragen wird, ohne dass es zu einer relevanten Aufreinigung kommt. Ob Kläranlagen, die als Hauptverfahren SBR einsetzen, allgemein anfälliger sind, kann somit nicht beantwortet werden, sondern dies ist Einzelfall abhängig.

Bei der Beckenart (Längsbecken, Mischbecken oder Umlaufbecken) konnten bisher auch keine Zusammenhänge erschlossen werden.

4.2. Gefährdungsabschätzung wasserwirtschaftlicher Infrastruktur

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.

4.2.1. Ansatz

Die Methodik für die Gefährdungsabschätzung wurde im Projekt über ein Geoinformationssystem (GIS) basiertes Modell aufgebaut, mit welchem die folgenden Fragen beantwortet werden sollen:

- Was sind die Auswirkungen eines Cyberangriffes / Stromausfalles, wenn wenig geklärtes bis nicht geklärtes Abwasser in Gewässer eingeleitet wird?
- Wo und wie stark werden Umweltqualitätsnormen in Fließgewässern überschritten?
- Welche Strukturen und schützenswerte Gebiete sind von den Angriffen betroffen?
- Wie ist das Risiko wasserwirtschaftlich einzuordnen?

Die Methodik des Ansatzes ist in Abbildung 4-6 dargestellt. Das GIS-Modell basierte ausschließlich auf frei und öffentlich verfügbaren Daten (Open Data Ansatz). In GIS wurden dazu die folgenden Daten verwendet:

- die 13 Kläranlagen der BR Detmold,
- die Gewässer mit den Abflüssen MQ (mittlerer Abfluss) und MNQ (mittlerer Niedrigwasserabfluss) und Gewässertiefen,

- angrenzende Flora-Fauna-Habitat (FFH) Gebiete, geschützte Biotope, Naturschutzgebiete,
- und Wasserschutzgebiete sowie die Standorte von Wasserwerken als vulnerable Gebiete.

Die Daten wurden größtenteils aus den Portalen *ELWAS-web* und *GEOportal.NRW* gewonnen. Zusätzlich wurden Daten, die nicht automatisch exportiert werden können, nach Korrespondenz mit dem Landesamt für Natur, Umwelt und Verbraucherschutz Nordrhein-Westfalen (LANUV NRW), der Bezirksregierung Detmold und der Geschäftsstelle des Interministeriellen Ausschusses zum Aufbau der Geodateninfrastruktur in NRW (IMA GDI.NRW) zur Verfügung gestellt. Eine Auflistung aller verwendeter Daten ist in Anhang 1 zu finden.

Diese Informationen wurden durch das Modellsystem GREAT-ER (Geography-Referenced Regional Exposure Assessment Tool for European Rivers) ergänzt, welches als Emissions- und Gewässermodell dient, um eine Abschätzung und Risikobewertung von Umweltkonzentrationen chemischer Stoffe zu liefern (USF, 2020). Als zu untersuchende Parameter wurden Stickstoff und Phosphor ausgewählt.

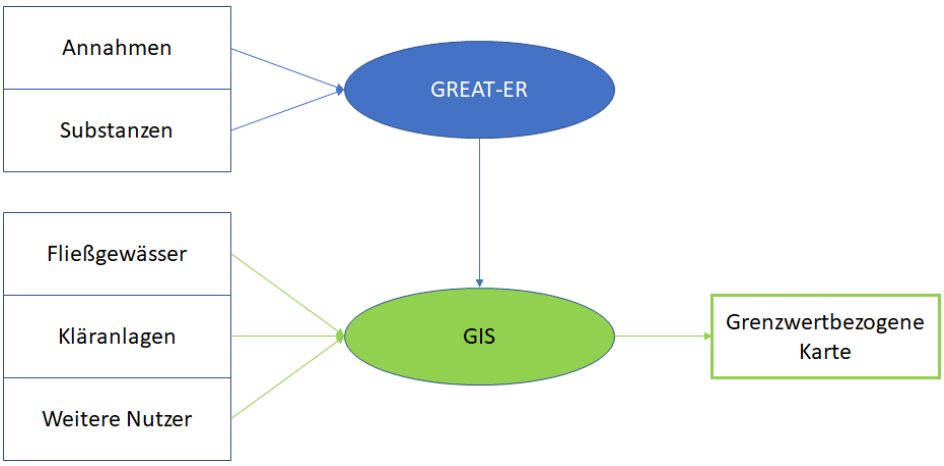


Abbildung 4-6: Modellaufbau der GIS-Ansatzes zur Gefährdungsabschätzung

Für das Modellsystem wurden die Daten umfangreich aufbereitet. Dazu gehört eine Projektion des Koordinatensystems und die Überführung der Fließgewässer in ArcHydro durch eine Überführung der Start- und Endpunkte in HydroJunctions und der Linien in HydroEdges (vgl. Abbildung *4-7***Fehler! Verweisquelle konnte nicht gefunden werden.**). Den dargestellten Flusssegmenten werden anschließend Abflussdaten hinzugefügt und die Kläranlagen werden als Einleitungsstellen hinzugefügt. Die Verwaltung und das Einladen der Daten geschieht anschließend über eine Datenbank nach einem in ArcHydro hinterlegtem Schema.

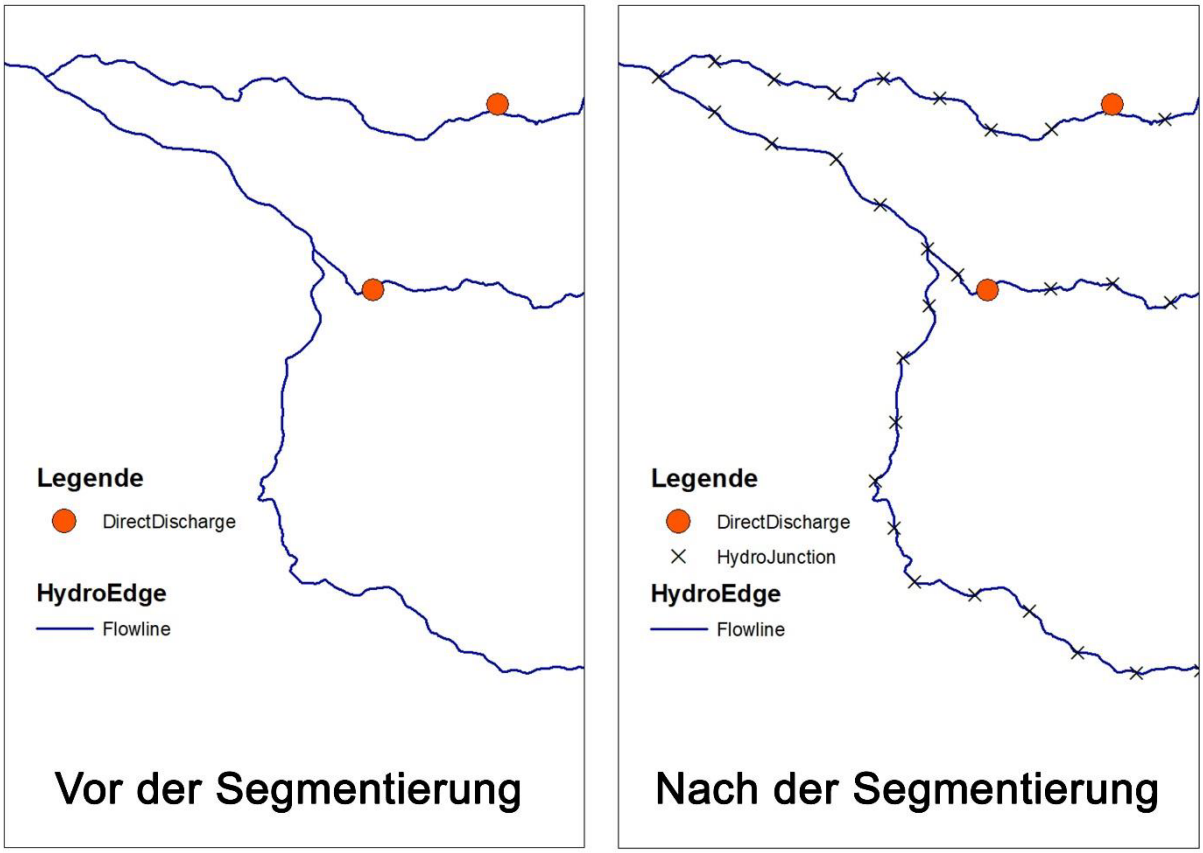


Abbildung 4-7: Flusssegment in den Ausgangsdaten links, Flusssegment nach der Datenaufbereitung.

Anschließend wurden Szenarien mit den verschiedenen Abflüssen der Gewässer sowie verminderte Reinigungsleistungen der Kläranlagen durch Cyberangriffe von 50 %, 25 % und 0 % Klärleistung gerechnet. Die Klärleistungen wurden gewählt, um sowohl einen Eingriff darzustellen der auf die Reinigungsleistung einwirkt, als auch die direkte Einleitung von Abwasser. Die Einleitung von abtreibendem Schlammwasser wurde nicht modelliert, stellt jedoch aufgrund der signifikanten Umweltauswirkungen ein mögliches Objekt für weitere Untersuchungen dar. Die Ergebnisse können anschließend als grenzwertbezogene Karte dargestellt werden.

Alle ausgewählten Szenarien unterscheiden sich in Bezug auf die Art eines Angriffs nicht voneinander. Sie stellen die Auswirkungen von erfolgreichen Angriffen unterschiedlicher Wirkung dar, betrachten aber keine kläranlageninternen Auswirkungen auf Systeme und Prozesse und stellen somit Worst-Case-Szenarien zur Abschätzung der Auswirkungen dar.

4.2.2. Ergebnisse Modellierung

Die wichtigsten Bausteine der Simulationsszenarien stellen die eingeschränkte Reinigungsleistung von 0 % und 50 % und die unterschiedlichen Abflüsse MNQ und MQ der Gewässer dar. Simuliert wurden die Stoffströme von Phosphor und Stickstoff. Szenario 1 stellt das Worst-Case-Szenario und somit die Grundlage für eine Bewertung des Risikos dar.

Die Kombination von 0 % Klärleistung und dem mittleren Niedrigwasserabfluss MNQ stellt die größte Gefahr für anschließende Gewässer und Schutzgebiete dar. Hier treffen die Extrema der Betrachtungen aufeinander. Die 13 untersuchten Kläranlagen sind durch einen Cyberangriff gestört und das Abwasser wird ungeklärt in ein Gewässersystem mit dem geringsten betrachteten Abfluss geleitet.

Im Folgenden werden die Ergebnisse für die Stoffströme Stickstoff und Phosphor für das Szenario 1 vorgestellt. Zunächst gilt es als Mindestanforderungen die Emissionen zu betrachten, diese werden allerdings in allen Szenarien überschritten. Daher werden im Folgenden die Konzentrationen nach Vermischung im Gewässer betrachtet. Die höchste Konzentration von Phosphor (vgl. Abbildung 4-8), die im Gewässer berechnet wurde, beträgt 28.1 mg/l und überschreitet die Anforderungen an den sehr guten ökologischen Zustand von Fließgewässern für Orthophosphat-Phosphor (o-PO_4-P) von 0,02 mg/l gemäß OGewV 2016 um den Faktor 1.405. Die Länge des Fließweges, die von Grenzwertüberschreitungen betroffen ist, beläuft sich auf 84 km. In der nachstehenden Grafik ist die Verteilung der berechneten Phosphor-Konzentrationen im Gewässernetz dargestellt. Dies erfolgt als Quotient aus der erwarteten Umweltkonzentration (PEC – Predicted Environmental Concentration) und dem Umwelt Qualitätsstandard (EQS - Environment Quality Standard). Nimmt der Quotient PEC/EQS Werte > 1 an, so werden zugehörige Qualitätsstandards überschritten und orange dargestellt. Ergeben sich Werte zwischen ½ und 1, sind die Konzentrationen stark erhöht. Für Phosphor gilt ein Grenzwert von 0,02 mg/l und für Stickstoff 13 mg/l. Entlang der Fließwege, für die eine Überschreitung der Umweltqualitätsnormen berechnet wurde, liegen neun Naturschutzgebiete, drei FFH-Gebiete, 23 geschützte Biotope und zwei Wasserwerke.

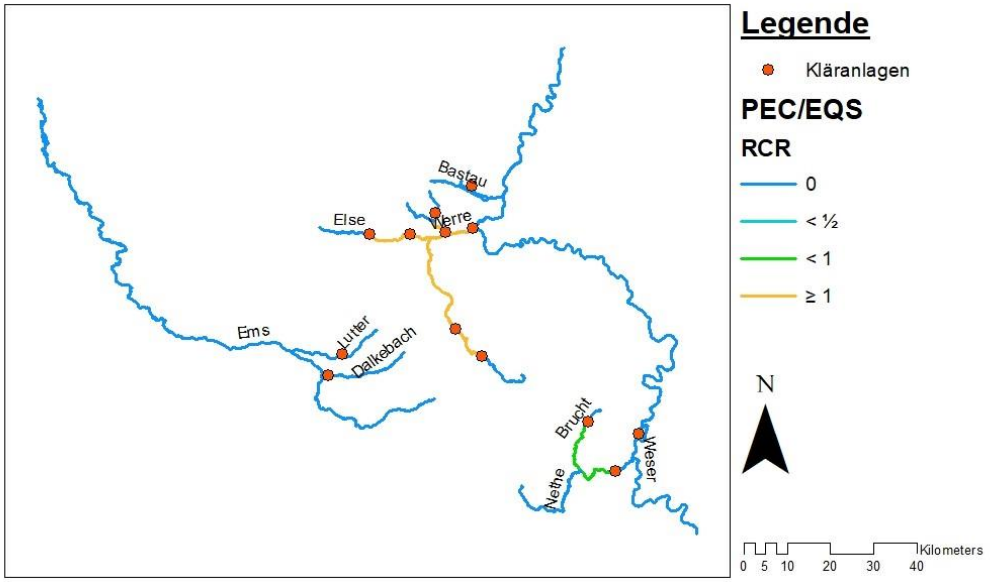


Abbildung 4-8: Ergebnisse der Modellierungen von Phosphor bei 0 % Klärleistung und MNQ Abfluss.

Die höchste gemessene Stickstoffkonzentration im Arbeitsgebiet beträgt mit 174 mg/l das dreizehnfache der Umweltqualitätsnorm. Es wurde eine von Grenzwertüberschreitungen betroffene Länge von 31 km errechnet. Darüber hinaus liegen ein FFH-Gebiet, ein Naturschutzgebiet, elf geschützte Biotope und ein Wasserwerk in weniger als 10 m Entfernung von mit Überschreitungen betroffenen Flüssen. Die Berechnungen sind in Abbildung *4-9* zu sehen.

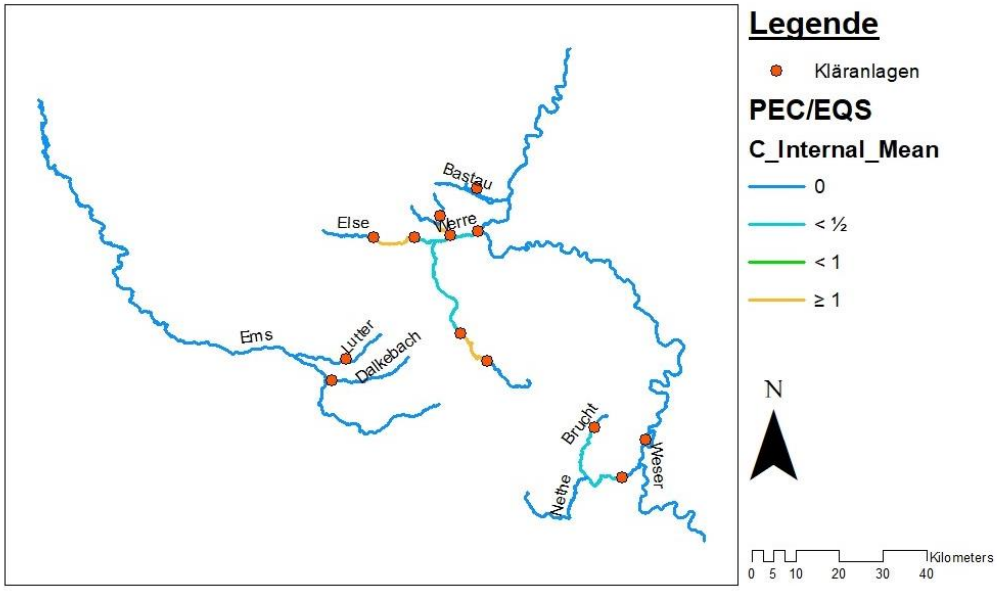


Abbildung 4-9: Ergebnisse der Modellierungen von Stickstoff bei 0 % Klärleistung und MNQ Abfluss.

In Tabelle 4-1**Fehler! Verweisquelle konnte nicht gefunden werden.** werden die Ergebnisse aller simulierten Szenarien zusammengefasst. Die Ergebnisse verdeutlichen das Ausmaß

eines Komplettausfalls. Es würde sich unter den Annahmen des Modells eine starke Verunreinigung über mehr als 80 km Flusslänge im Worst-Case-Szenario ereignen.

Tabelle 4-1: Tabellarische Darstellung der Simulations-Ergebnisse zur Fließgewässerbelastung

Stoffstrom, Klärleistung	MNQ		MQ	
	Höchste Konzentration [mg/l]	Länge der Qualitätsnormüberschreitung im Fluss [km]	Höchste Konzentration [mg/l]	Länge der Qualitätsnormüberschreitungen im Fluss [km]
Phosphor, 0 %	28	84	8	81
Phosphor, 50 %	14	84	4	81
Stickstoff, 0 %	174	31	48	22
Stickstoff, 50 %	87	30	24	13

Bei einem Ausfall der Kläranlagen besteht ein Risiko je nach Kombination der variablen (Fracht der Kläranlagen und Durchfluss des Gewässers) und konstanten Größen (Abwasservolumen), die in dem Modell verwendet werden. Aus den Ergebnissen lässt sich ableiten, dass in diesem Fall der Einfluss des Abflussgeschehens auf die resultierenden Konzentrationen im Gewässer einen gewichtigeren Faktor darstellt als die Reinigungsleistung. Dies ist allerdings auch von der Abflusshöhe der Gewässer abhängig. Die Resilienz ist für die größten Fließgewässer im Arbeitsgebiet – Weser und Ems – am höchsten.

Aus dieser Erkenntnis lässt sich ableiten, dass insbesondere Gewässer mit einem hohen Anteil an Kläranlagenabfluss am gefährdetsten sind. Dies bezieht sich aber nicht nur auf eine Kläranlage. Falls es zu einem kollektiven Ausfall kommt wie in der Modellierung, lagen die höchsten Nährstoffkonzentrationen im Gewässerabschnitt rund um den Zufluss der Else in die Werre vor, da hier eine hohe Kläranlagendichte vorliegt.

Weiterhin entsteht nicht nur ein Risiko im Falle eines kollektiven Versagens der Kläranlagen. Fallen nur eine oder wenige Anlagen aus, besteht ein geringeres Risiko einer starken Verunreinigung aufgrund der geringen Frachten in Relation zu den vergleichsweisen hohen natürlichen Abflüssen der Vorfluter. Entscheidend für die Ausmaße des resultierenden Schadens ist, in welchem Maß und für welchen Zeitraum eine oder mehrere Anlagen ausfallen. Anhand der in ELWAS hinterlegten Stammdaten können Aussagen darüber getroffen werden, von welcher Anlage die potenziell größte Gefahr ausgeht. An dieser Stelle gilt, dass von der Kläranlage, die das am stärksten belastete Abwasser in den Vorfluter mit dem geringsten Abfluss im Gewässer einleiten würde, die größte Gefahr ausgeht.

Als Schaden im Gewässer wird angesehen, wenn die Belastung im eingeleiteten Abwasser hoch genug ist, um letztendlich im Volumenstrom des Flusses zu einer Qualitätsnormüberschreitung zu führen. Werden mehrere Anlagen gleichzeitig Opfer eines Angriffes, dann summieren sich sowohl die Schadstofffrachten als auch die Volumenströme im Verlauf des Fließweges.

Die Ergebnisse liefern mit den prognostizierten Schadstoffkonzentrationen Richtwerte für konkrete Auswirkungen auf die anschließenden Ökosysteme, wie Algenblüten oder Fischsterben. Jedoch wurden in der Arbeit nur Qualitätsnormen als Grenzwert zur Entstehung von Schäden verwendet. Zudem wurden nur die 13 untersuchten Kläranlagen berücksichtigt und nicht alle in den Flussgebieten vorhandenen KA-Einleitungen. Hier sind weitere Untersuchungen notwendig, um zu zeigen, welche zeitlichen und gewässerspezifischen Faktoren letztendlich zum konkreten Eintritt dieser Schäden führen. Insbesondere ist dafür auch relevant, welche Verschmutzungen für beispielweise Trinkwassergewinnung noch akzeptabel sind und nicht zu einer Gefährdung der Trinkwasserversorgung führen.

4.2.3. Risikoanalyse

Aus den Ergebnissen der Modellierung und den Erkenntnissen der IT-Sicherheit wird gezeigt, wie eine Risikoanalyse durchgeführt werden kann. Dazu wird die Risikoanalyse des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK) für die Trinkwasserversorgung verwendet und auf die Gegebenheiten dieser Studie angepasst. Die Ergebnisse der Modellierungen erlauben nur eine indirekte Quantifizierung des Schadensmaßes durch eine Anzahl geschädigter Personen, wie der Leitfaden für die Trinkwasserversorgung es darstellt. Wird anstelle der Anzahl geschädigter Personen der Einwohnergleichwert der Kläranlagen verwendet, können Aussagen über das Schadensmaß abgeleitet werden (Wienand & Hasch, 2019). Um ein vollständiges Bild des Risikos nach diesem Ansatz zu erlangen, müsste eine detaillierte Analyse für jede Anlage im Einzelnen durchgeführt werden. Dazu sind spezielle Kenntnisse der Anlagen, deren Komponenten und der Verhältnisse vor Ort erforderlich. Zudem muss definiert werden, ab wann eine Einleitung in ein Gewässer als Schaden und wie die Höhe des Schadens beurteilt wird. Dieses Wissen kann nicht allein aus öffentlich zugänglichen Daten abgeleitet werden. Eine repräsentative Risikoanalyse kann in der Zusammenarbeit mit dem betreibenden Personal erarbeitet werden. Eine Übersicht der erforderlichen Kenntnis von Details kann anhand der vom BBK vorgeschlagenen Checklisten (Wienand & Hasch, 2019, S. 76 ff.) erlangt werden.

Circa zwei Drittel der betrachteten Anlagen in der BR Detmold sind der Klasse 4 zugehörig, deren Einwohnerwerte zwischen 10.000 und 100.000 E liegt. Da allen Kläranlagen bei der Ermittlung des Einwohnerwertes die gleichen Voraussetzungen zu Grunde liegen, wird dieser als geeignetes Werkzeug für die Abschätzung des Schadensausmaßes angesehen. Dahinter

steht das Prinzip, dass für alle angeschlossenen Einwohner die Behandlung von Abwasser beeinträchtigt wird und gleichsam auch für diese Betroffenen ein Schaden entsteht. Eine Eintrittswahrscheinlichkeit lässt sich nur schwer voraussagen. Der Leitfaden klassifiziert einen Eintritt als wahrscheinlich, wenn das Ereignis alle zehn bis einhundert Jahre stattfindet (Wienand & Hasch, 2019). Anhand von aktuellen Zahlen und Berichten zu Cyberangriffen wird die Eintrittswahrscheinlichkeit eines erfolgreichen Cyberangriffs als hoch eingestuft. An dieser Stelle sollte auch die Beachtung des technischen Fortschritts Beachtung finden, der aufgrund der informationstechnischen Entwicklungen ein zusätzliches Risiko für die Gefährdung der Kläranlagen darstellt. Abbildung 4-10 zeigt ein Beispiel einer Risikomatrix, anhand derer eine Einordnung des resultierenden Risikos in der Trinkwasserversorgung möglich ist. Das Schadensausmaß wird in den Vulnerabilitätsklassen 1 (gering) bis 5 (hoch) dargestellt, welche jeweils in Bereichen der betroffenen Einwohner liegen. Unter der Annahme einer Eintrittswahrscheinlichkeit von unter zehn Jahren, würde sich für den unteren Einwohnerwerte der Größenklasse 4 von 10.000 ein mittleres bis hohes Risiko ergeben, welches durch die schwarze Ellipse in Abbildung 4-10**Abbildung *4-1*** dargestellt wird. Deutlich wird, dass sich selbst für die untere Schwelle der Größenklasse 4 das Risiko eines erfolgreichen Angriffs mit weitreichenden Folgen auf einem alarmierenden Niveau befindet, woraus sich ein dringlicher Handlungsbedarf ableiten lässt.

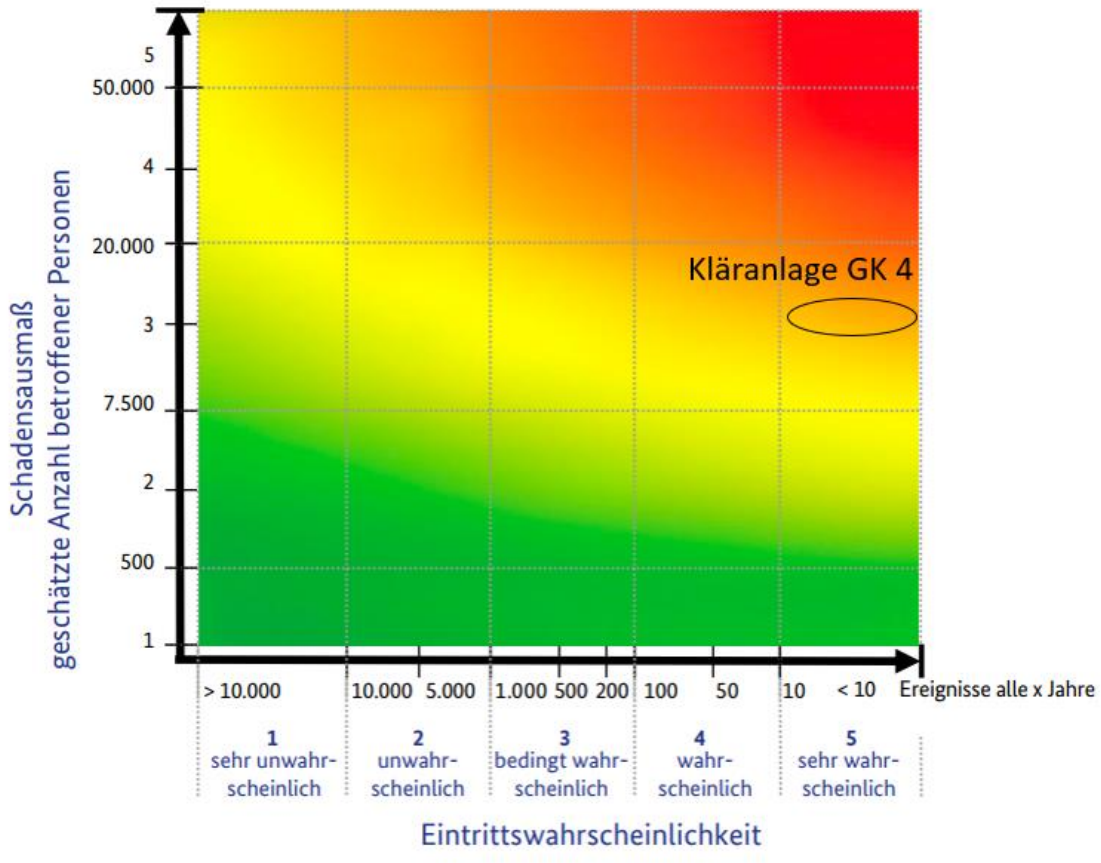


Abbildung 4-10: Beispiel einer Risikomatrix für das resultierende Risiko bei einem Cyberangriff auf eine Kläranlage (Vgl. *(Wienand & Hasch, 2019)*).

Im Rahmen der Erkenntnisse der Recherche ist weiterhin zu erwähnen, dass derartige Einschätzungen für den Ausfall der Abwasserreinigung bisher nicht existieren. Neben einer Abschätzung des Risikos anhand der betroffenen Personen durch die Einwohnergleichwerte wäre auch eine Klassifizierung des Schadensausmaßes anhand der Anzahl von potenziell betroffenen, schützenswerten Strukturen und Gebieten im Abstrom jeder Anlage denkbar. Dazu ist in Abbildung 4-11 verdeutlicht, dass die meisten Fließgewässer in der Bezirksregierung Detmold wasserabhängige Schutzgebiete passieren.

Eine getrennte Betrachtung von Trinkwassergewinnungsanlagen liefert ferner eine Grundlage für die Priorisierung bestimmter Kläranlagen. Durch eine Überschreitung der Umweltqualitätsnormen im Einzugsgebiet einer Trinkwassergewinnungsanlage, beispielsweise durch die Gewinnung von Uferfiltrat, können mögliche Gefahren für die Versorgungssicherheit entstehen. Diese gilt es gegenüber der Ökologie generell zu priorisieren, um den bestmöglichen Schutz für die Gesellschaft zu gewährleisten. An dieser Stelle ist darauf hinzuweisen, dass zum Zeitpunkt der Modellierung keine Informationen zur Trinkwasserversorgung durch Uferfiltrat oder Rohwasserentnahme im Gebiet der BR Detmold vorlag. Rohwasserentnahmen finden in der Region nicht statt und Uferfiltrat wird teilweise anteilig in Trickwassergewinnungsanlagen verwendet. Im erhöhten Umfang ist dies an anderen Standorten in NRW der Fall, an denen eine Priorisierung als sinnvoll zu erachten ist. Hier sind Kläranlagen im Oberlauf von beispielsweise Trinkwassertalsperren als besonders kritisch einzustufen.

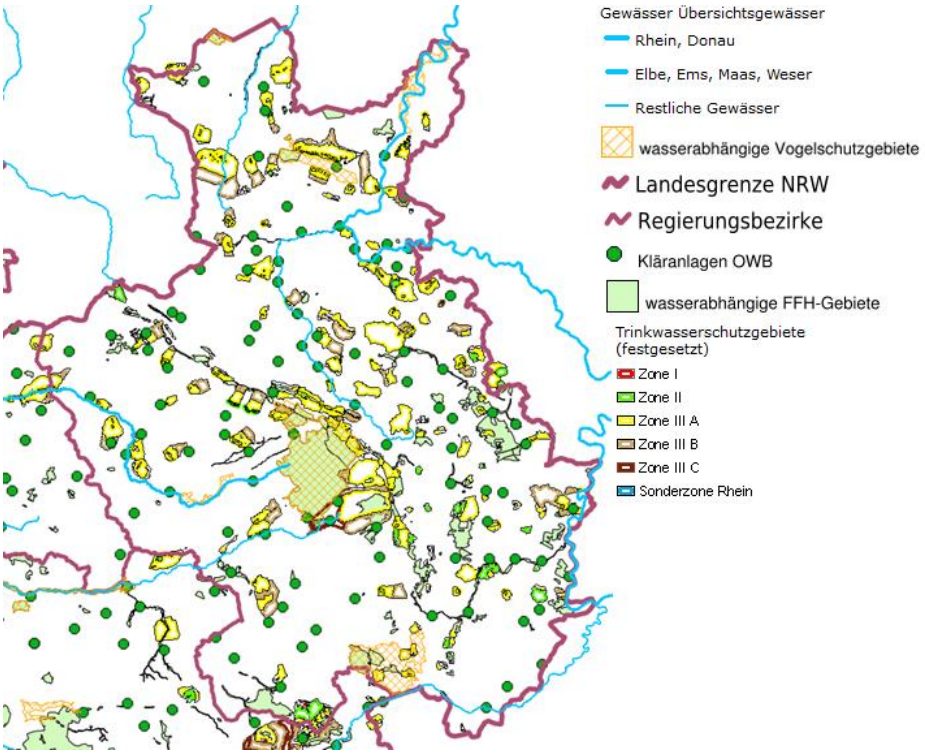


Abbildung 4-11: Bezirksregierung Detmold mit Fließgewässern, Kläranlagen und schützenswerten Gebieten (ELWAS-*Web*).

Eine Annäherung an die Einschätzung des Risikos durch mehrere Matrizen veranschaulicht die Vielseitigkeit der Problematik und würde darüber hinaus einen wichtigen Beitrag zu der Einschätzung der konkreten Gefahrenlage leisten. In allen Fällen der Klassifizierung eines potenziellen Schadens anhand von betroffenen Personen oder schützenswerten Strukturen und Gebieten bekommt die Herausforderung der Quantifizierung eines solchen Schadens eine zentrale Bedeutung für das Endergebnis einer Risikoanalyse. In den folgenden Abbildungen (vgl. Abbildung 4-12 und Abbildung 4-13) werden die beschriebenen Risikomatrizen beispielhaft dargestellt.

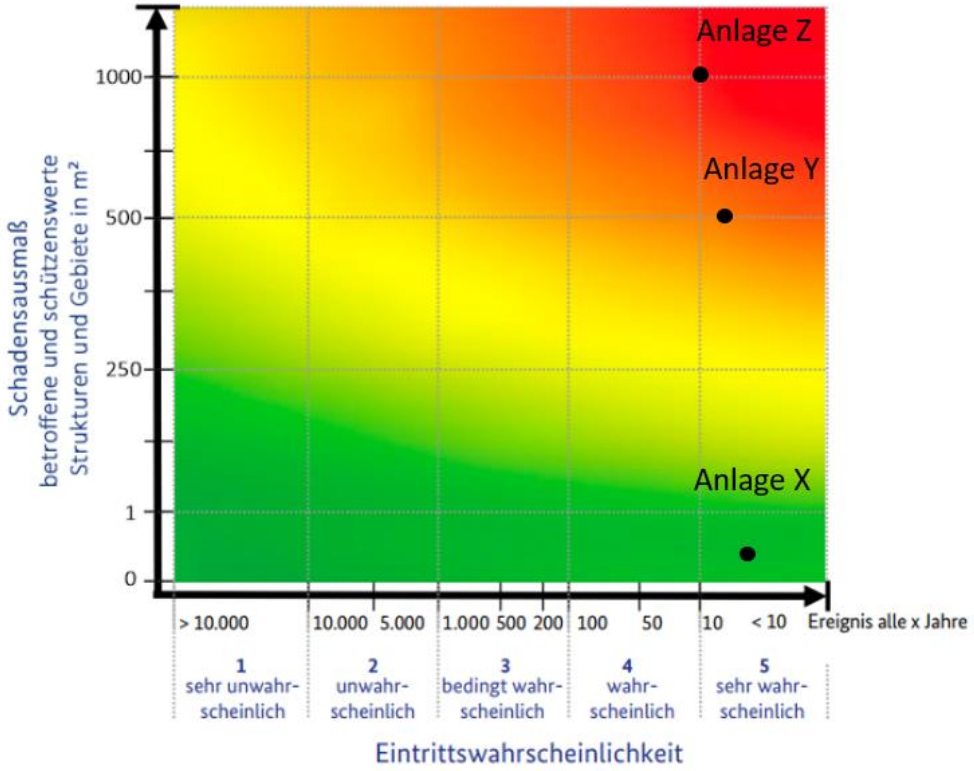


Abbildung 4-12: Beispiel einer Risikomatrix für das resultierende Risiko von schützenswerten Gebieten bei einem Cyberangriff auf eine Kläranlage (Vgl. *(Wienand & Hasch, 2019)*).

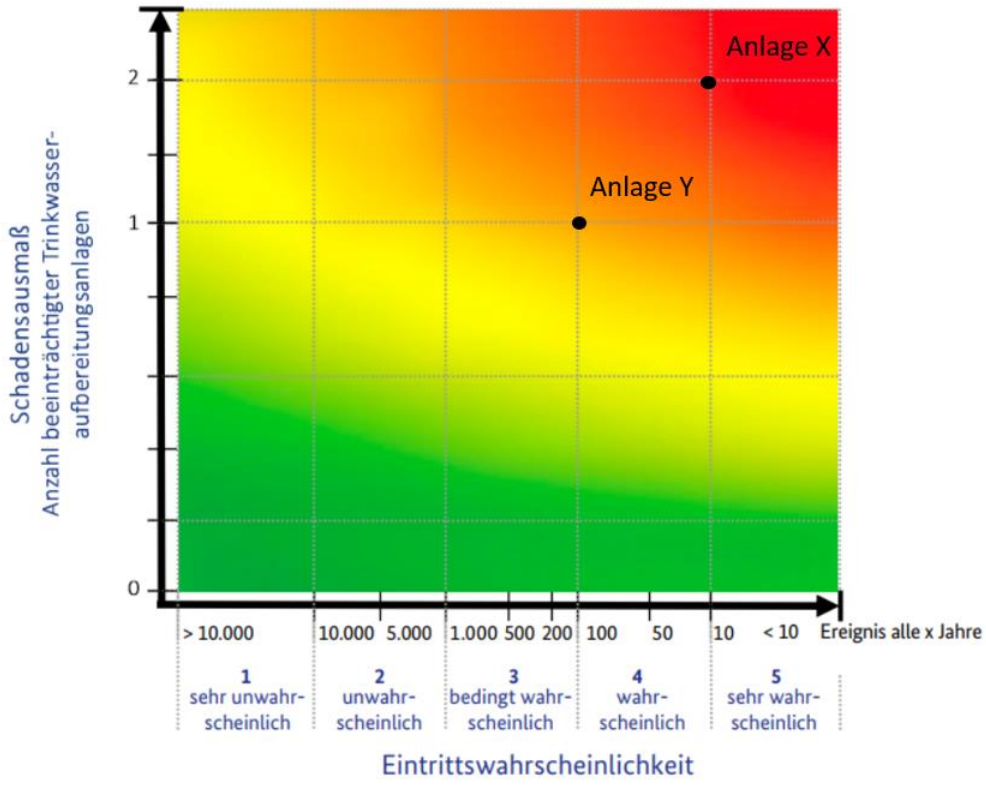


Abbildung 4-13: Beispiel einer Risikomatrix für das resultierende Risiko von Trinkwasseraufbereitungsanlagen bei einem Cyberangriff auf eine Kläranlage (Vgl. *(Wienand & Hasch, 2019)*).

4.3. 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.

4.3.1. Priorisierung von Anlagenteilen

Die Priorisierung von Anlagenteilen wurde bereits in Kapitel 3.5 in Abbildung 3-30 und Abbildung 3-31 aufgezeigt. Die Ergebnisse der Simulationsauswertung sind nach absteigender Wichtigkeit in Tabelle 4-2 dargestellt.

Tabelle 4-2: Abgestufte Priorisierung von Anlagenteilen.

Schadensfall Erhöhte Ablaufwerte/ eingeschränkte Abwasserreinigung	Schadensfall Überflutungen/ Abschläge
Ausfall RLS-Abzug	Zulaufpumpwerk
Ausfall Belüftung	Zwischenpumpwerk
Aufteilung auf Belebungsbecken	Zulaufschieber
Aufteilung auf Nachklärbecken	Schieberstellungen Verteilerbauwerke
Regelungstechnik Belüftung	Rückstau vom Rechen
Regelungstechnik RLS-Abzug	
Kohlenstoff Dosierung	
Ausfall Rührwerke	
Umfahren von Stufen	
Herabfahren von Dekantern	

An dieser Stelle sei darauf hingewiesen, dass die Wichtigkeit auf der individuellen Kläranlage abweichen kann. Lediglich die beiden fett gedruckten Bereiche sind immer von hoher Relevanz. Bei der individuellen Betrachtung sind immer die Teile 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). Zu unkontrollierten Austritten gehören auch Angriffe auf das Kanalnetz, welche bereits vor der Kläranlage geschehen können. Daher sollte auch möglichen Pumpen- und Schieberstellungen in Kanalnetzen große Aufmerksamkeit geschenkt werden.

4.3.2. Priorisierung einzelner Anlagen

Auf Basis der Betrachtung der SIMBA Simulation konnten folgende Erkenntnisse zur individuellen abwasserwirtschaftlichen Priorisierung gewonnen werden:

- Größere Kläranlagen bieten mehr Angriffspunkte für Veränderungen der abwasserwirtschaftlichen Prozesse, fordern so aber auch mehr Know-How für Veränderungen. Gleichzeitig können so aber auch einfacher versteckte Veränderungen durchgeführt werden.
- Kleinere Kläranlagen sind genauso anfällig wie größere Kläranlagen für Schäden die durch Angriffe ausgelöst werden können. Somit ist die Größe nur unter abwasserwirtschaftlichen Aspekten nicht die maßgebendste Größe.
- Wenn Kläranlagen höher ausgelastet sind, weisen sie eine höhere Anfälligkeit für entstehende Schäden auf.

- Die hydraulische Verweilzeit auf einer Kläranlage ist ein guter Indikator dafür, wie lange auf einer Kläranlage Zeit verbleibt, bis es nach einem Angriff zu einem Schaden kommt. Inwiefern diese bei einem Angriff verkürzt werden kann, ist vom individuellen Aufbau abhängig.

Als Fazit kann aus diesen Schlussfolgerungen gezogen werden, dass aus den bisherigen limitierten Daten aus abwasserwirtschaftlicher Sicht keine Priorisierung der Kläranlagen erfolgen kann, da die Anfälligkeit der Abwasserreinigung gegenüber Angriffen maßgeblich vom individuellen 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. Resultierend aus der Risikoabschätzung lassen sich folgende Empfehlungen und Priorisierungen ableiten:

- Ein erhöhter Sicherheitsbedarf resultiert auch unter Berücksichtigung des nachfolgenden Vorfluters, bspw. wenn es sich um einen Vorfluter mit geringem Durchfluss bzw. hohem Anteil des Kläranlagenabflusses am Gewässer handelt.
- Nach relevanter wasserwirtschaftlicher Nutzungsart im Abstrom:
    - Trinkwasser
    - FFH-Gebiete
    - Stauanlagen und Talsperren
    - Industrie: Bspw. Kühl- und Prozesswasser
    - Gewerbe: Bspw. Fischzucht
    - Erholung
    - ….

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.

4.4. Zusammenfassende Auswertung

Die wasserwirtschaftliche Relevanzanalyse kann in zwei Teile aufgeteilt werden. 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 IT-Sicherheit 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. Auf wasserwirtschaftlicher Seite zeigten die Modellierungen, dass für den Schutz der Umwelt und Gewässernutzungen eine Priorisierung von großen Anlagen im Untersuchungsraum sinnvoll erscheint. 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.

5. Empfehlungen IT-Sicherheit für Kläranlagen

Im Datenschutz wird der Begriff der Technisch-Organisatorischen Maßnahmen (TOMs) genutzt. Der Begriff beschreibt eigentlich gut, wie Informationssicherheit zu erreichen ist. Zu 100 % ist das nicht zu schaffen, aber es kann mit vergleichsweise geringem Aufwand den potentiellen Angreifern unattraktiv gemacht werden. 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 Verbessertes Wissen bzw. die Sensibilisierung der Mitarbeiter. Organisatorisch aber 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. Ausgearbeitete Notfallpläne und Business Continuity Management (kurz: BCM) sind hierbei zu nennen. Wenn diese zudem getestet und erprobt werden, steigert dies den Sicherheitsleitgedanken.

In den jeweiligen Protokollen für einzelne Anlagen haben wir individuelle Listen von Maßnahmen abgelegt, die dem BSI-Grundschutzkompendium 2019 entnommen sind und den Anlagenbetreibern die Umsetzung empfohlen. Diese Maßnahmen haben sich aus den jeweiligen Anwendungsfällen für die Anlagen ergeben und sind die anlagenspezifischen Empfehlungen zur Verbesserung der Sicherheit für jeden Betreiber.

5.1. Entwicklung von IT-Schutzkonzepten

Steuerungen, die nicht aus dem Internet erreichbar sind, können 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 ja auch die 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
- mit Intrusion Detection Systemen (IDS, Angriffserkennungssysteme) lassen sich nicht zulässige Netzteilnehmer sehr einfach sichtbar machen.

Natürlich müssen Steuerungen parametriert und hier und da auch Anpassungen an Leitstellensoftware vorgenommen werden. Dies geschieht häufig durch Externe. Viel sicherer wird ein Zugang zum Netz, wenn er nicht dauerhaft geschaltet ist. Wann immer es möglich ist, sollte z.B. über eine Einwahlnummer die Stromversorgung für den Zugriff eingeschaltet werden (z.B. eine AVM FRITZ!box). Dies kann zum Beispiel über die Telefonanlage der Kläranlage oder über eine GSM Schaltsteckdose geschehen, die eine SIM-Karte enthält und übers Mobilfunknetz aktiviert wird. Die Verbindung zum Zugriffspunkt muss immer eine Virtual

Private Network (VPN)-Verbindung sein, bei der beide Seiten identifiziert sind. Es wird also eine gegenseitig verschlüsselte Verbindung aufgebaut (Fachausdruck ist Mutual TLS = Gegenseitige Transportverschlüsselung – Transport Layer Security). Indem beide Seiten mit Parametern ausgestattet sind, die die konfigurierende Person der Verbindung festgelegt hat, ist eine solche Verbindung sehr sicher. Das Schalten des Zugriffspunktes über eine getrennte und natürlich vertraulich behandelte Zusatzverbindung und eine sicher konfigurierte Verbindung sind gemeinsam ein exzellenter Schutz gegen Angriffe.

Diese Trennung und die Art der Zugriffsgewährung sind auch bei sehr kleinen Anlagen zu realisieren, weil sie kostengünstig ist. Das VPN kann durchaus auch durch den Zugriff über **Team**Viewer™ mit einer korrekt konfigurierten Verbindung gebildet werden, bei der sichergestellt sein muss, dass nur die benötigten Netzwerkports offen sind. Der externe Zugriff sollte zeitgesteuert nach nicht zu langer Zeit automatisch geschlossen werden, indem der Strom für den Router wieder abgeschaltet wird. Für den Zugriff von außen muss ein Laptop verwendet werden, der vor Aufbau der Verbindung aktuell virengeprüft wird. Er sollte grundsätzlich nicht zu anderen Zwecken verwendet werden, um nicht durch anderweitige Nutzung das Infektionsrisiko zu erhöhen.

Beispiel für ein quelloffenes *IDS* ist *SNORT*®, für das auch das BSI Regeln bereitstellt. Es gibt viele IDS Systeme deshalb sei *SNORT*® nur als Beispiel erwähnt. Wird also der Zugriff aufs Steuerungsnetz wie zuvor beschrieben extern an- und ausgeschaltet und läuft im Netz selbst ein IDS System, so lässt sich jeder Zugriff aufs Netz zuverlässig erkennen, weil das Ein- und Ausschalten des Zugriffspunktes sichtbar gemacht wird.

Wenn ein Zugriff von außen unbedingt erforderlich ist, muss auch die Frage beantwortet werden, ob das ein schreibender Zugriff sein muss. Ein rein lesender Zugriff würde über eine so genannte Datendiode realisiert werden können, die Daten nur von innen nach außen passieren lässt, nicht umgekehrt. Datendioden gibt es auch für industrielle Umgebungen (Rail-Montage). Sie sind allerdings vergleichsweise teuer.

Darüber hinaus ist bei der Installation und Nutzung getrennt arbeitender Steuerungs- und Büronetze penibel darauf zu achten, dass die Netze wirklich vollständig getrennt sind. Hier ist Vertrauen gut, Kontrolle aber aus der Auditorerfahrung heraus deutlich besser. Es sollte unbedingt aus dem Steuerungsnetz heraus mindestens einmal jährlich mit einem Intrusion Detection System geprüft werden, dass unter keinen Umständen eine Verbindung zum Office-System besteht.

Die größte Gefahr für Computer sitzt vor dem Bildschirm. Jeder kennt diesen Satz. Auch wenn er nur eingeschränkt wahr ist, ist aber auch der beste Verteidiger eines Netzes der jeweilige Anwender, der schnell merkt, wenn irgendetwas nicht stimmt. Die diesbezüglichen Fähigkeiten

der Mitarbeiter hängen stark von der Ausbildung / Weiterbildung ab. Computersicherheit gehört wie Arbeitssicherheit, Umgang mit Gefahrstoffen, Fahrsicherheit etc. ins jährliche Schulungsprogramm. Es hat sich bewährt, Computersicherheitsschulungen so anzubieten, dass sie auch für die private Nutzung neue Kenntnisse mitbringen. Dadurch werden die Lerninhalte kontinuierlich angewendet und geübt. Zudem erhöht sich die Sicherheit der Netze, die für Home-Office Nutzung genutzt werden.

Pläne des Steuerungsnetzes aktuell zu halten, scheint häufig gerade auf kleineren Anlagen nicht notwendig zu sein, weil die Mitarbeiter sich ja auskennen. Wenn es aber Probleme gibt, weil ein Netz kompromittiert wurde oder einfach der Blitz eingeschlagen ist, hilft ein aktueller Netz- oder Netzstrukturplan ungemein (bspw. fordert das IT-Grundschutzkompendium Edition 2022 NET.1.1.A13. Netzplanung. „*Jede Netzimplementierung MUSS geeignet, vollständig und nachvollziehbar geplant werden.*“). Er versetzt auch anlagenfremde Personen in die Lage, schnell Unterstützung leisten zu können. Und den Plan fortzuschreiben führt für den Schreiber selbst dazu, das Wissen über die eigene Anlage immer wieder fortzuentwickeln. Dazu kann man sich den Internetplan für das eigene Wohnviertel vorgestellen. Wenn der Provider den Internetplan nicht aktuell hält, wird das Netz nicht funktionieren. Und selbst beim Blick auf Anlagen der GK 3 sieht man, dass die inzwischen mit aller Sensorik und den Steuerungen schon ähnlich komplex geworden sind. Es sei hier noch einmal darauf hingewiesen, dass im Projekt einige gute Pläne gezeigt wurden, die die jeweiligen Dienstleister erstellt hatten. Betreiber kritischer Infrastruktur und Energieversorger sind zum Bereitstellen aktueller Netzstrukturpläne verpflichtet.

Das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) verlangt in § 8a (1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen. Es umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.

Gemeint sind damit Intrusion Detection Systeme, die also Eindringlinge aufspüren können (Siehe weiter oben in diesem Kapitel). Nicht verpflichtete Unternehmen müssen solche Systeme nicht dauerhaft betreiben. Der periodische Einsatz ist trotzdem sinnvoll. Diese Systeme könnten z.B. in DWA Nachbarschaften oder auf Kreisebene gemeinsam beschafft und reihum auf den Anlagen betrieben werden. So ist verifiziert, dass in jeder Steuerungsumgebung tatsächlich nur zulässige Geräte laufen. Außerdem unterstützen solche Geräte u.U. bei der Dokumentation der Anlagen, indem sie Listen der gefundenen

Steuerungen exportieren können. Auch der korrekt konfigurierte Remote-Zugriff kann mit solchen Systemen nachgewiesen werden.

Der branchenspezifische Sicherheitsstandard Wasser/Abwasser wurde entwickelt, um unabhängig von der jeweiligen Anlagengröße ein Instrument zur Sicherstellung der Informationssicherheit verfügbar zu haben. Er enthält die wichtigen Komponenten der Risikobewertung für die Assets vor und nach Maßnahmen und der kontinuierlichen Verbesserung, indem er jährlich durchgearbeitet wird. Das kann natürlich durch externe Dienstleister geschehen, aber auch in Nachbarschaften untereinander. Auch der Zusammenschluss mehrerer Kläranlagen, die sich externe Unterstützung teilen, kann zu kostengünstigen Managementsystemen für Informationssicherheit führen.

Zuletzt sollten die Dienstleister eng eingebunden sein, wie kommunale Rechenzentren, größere Abteilungen in den größeren Städten oder leistungsstarke Hauselektriker. Bei allen ist das Know-How vorhanden, wie die Informationssicherheit gesteigert werden kann.

5.2. Ableitung von fachpolitischen Ansätzen

Im Rahmen des Projektes wurde deutlich, dass auf Kläranlagen noch wenig bis kein Bewusstsein für die Art und gegenwärtige akute Lage von Cyberangriffen vorhanden ist. Zudem ist oft auch nicht bewusst, welch erheblicher Schaden aus einem Angriff entstehen kann, der auch für eine Kommune (sehr) teuer werden kann. Dazu kommt ein ökologischer und volkswirtschaftlicher Schaden aufgrund des Versagens der Abwasserbehandlung. Im Rahmen des Ukrainekrieges steigt das Bewusstsein für die eigene Angreifbarkeit allerdings stark an.

Unter Beachtung der aktuellen politischen Diskussionen und Veränderungen - auch auf europäischer Ebene mit der NIS-2 Richtlinie - ist dauerhaft von einer Senkung der zur Einhaltung von Informationssicherheitsmaßnahmen verpflichteten Organisationen auszugehen, wodurch auch kleinere Kläranlagen zukünftig einen Standard des Schutzniveaus erfüllen müssen. Ganz unabhängig davon ist es sinnvoll, bei allen Beteiligten das Wissen darüber zu verbessern, wie Informationssicherheit ausgebaut werden kann. Dieses Wissen und die damit einhergehenden geänderten Verhaltensweisen müssen in den Alltag einfließen. Aus den gewonnenen Erkenntnissen des Projektes wird eine erste fachpolitische Agenda formuliert, die zu einer Verbesserung des Schutzniveaus von Kläranlagen beiträgt. In Abbildung 5-1 sind im Zeitstrahl kurz- und langfristige Maßnahmen dargestellt, welche zur Erhöhung des Schutzniveaus beitragen. Im Folgenden werden diese der Reihe nach vorgestellt.

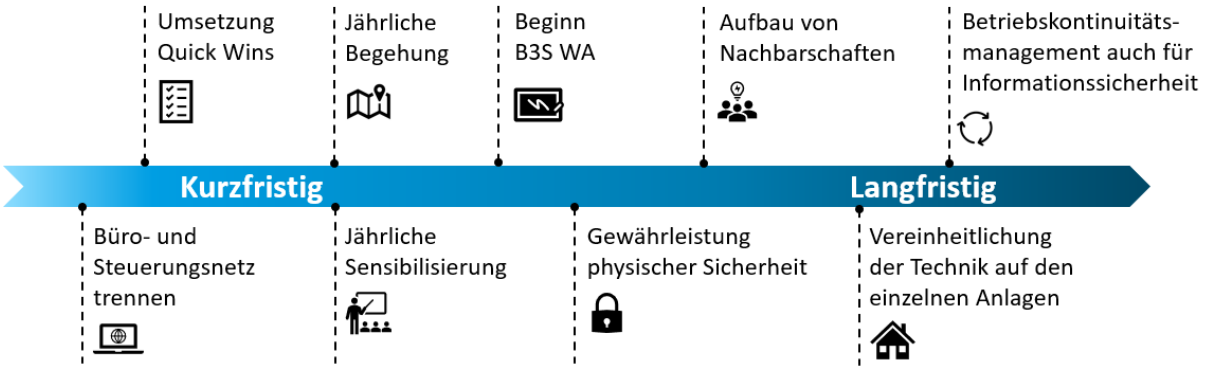


Abbildung 5-1: Empfohlener Zeitplan für die kurz- und langfristige Maßnahmen-Umsetzung. (eigene Darstlelung)

Büro- und Steuerungsnetz trennen

Es ist möglichst schnell anzustreben den Zugang zum Steuerungsnetz der Kläranlagen aus dem Netz zu nehmen, erschweren oder mit zwei Faktoren abzusichern (Quick-Wins). Mögliche Vorgehensweisen sind in Kapitel 4.1 beschrieben. Die regelmäßige Überprüfung des tatsächlichen Trennungszustandes durch Intrusion Detection Systems ist sinnvoll. Eine weitere Möglichkeit ist die Absicherung des Zugangs nach *Zero-Trust* Prinzipien. Zero Trust bedeutet, wie der Name schon nahelegt, dass keinem Computer und keinem Netz vertraut wird. Um dennoch kommunizieren zu können und die Kontrolle über den Datenfluss zu behalten, werden möglichst viele Faktoren geprüft, bevor eine Verbindung überhaupt aufgebaut werden kann. Dies kann das zugreifende Gerät sein, welches bekannt und auf Sicherheit hin untersucht sein muss. Wenn es der Organisation gehört und der Virenschutz tagesaktuell ist, darf es für den Zugriff verwendet werden. Dann wird der Benutzer nach Nutzername, Passwort und beispielsweise einem Token geprüft. Weitere Kriterien können der Ort, von dem aus der Zugriff erfolgt, und / oder die Tageszeit sein. Oder es muss auf Empfängerseite eine Meldung vorliegen, bevor von außen zugegriffen werden kann. Dieses Prinzip ist militärischen Ursprungs (wie fast die gesamte Internettechnik) und wird seit 2007 von der Cloud Security Alliance unter den Stichworten Software Defined Perimeter oder Zero Trust Network verwaltet.

Cyber-Sicherheit Sofortmaßnahmen – Checklisten

Als erste Maßnahme wird die Einführung von Checklisten empfohlen, welche Cyber-Sicherheit Sofortmaßnahmen enthalten. Ziel ist erste Quick-Win Maßnahmen schnell und unkompliziert auf den Kläranlagen umzusetzen. Hierzu hat das subKRITIS-Konsortium einen ersten Entwurf einer Checkliste erarbeitet, siehe Tabelle 0-2 im Anhang. Dazu sollte die Liste auf mehreren Kläranlagen ausprobiert und aktualisiert werden und die Ergebnisse mit den Kläranlagenbetreibern besprochen werden. Anschließend kann dann die Checkliste durch das

KDW veröffentlicht und durch MULNV / BezReg gezielt verteilt werden. Langfristig sollte eine Umsetzung in DWA-Arbeitsblättern erfolgen. Es muss allerdings klar festgehalten werden, dass Checklisten zwar kurzfristig das Sicherheitsniveau anheben können, langfristig aber nur die Umsetzung eines periodisch durchlaufenen Informationssicherheitsmanagementsystems, z.B. auf Basis des B3S WA, das erforderliche Sicherheitsniveau gewährleisten kann. Bereits erkannte Maßnahmen, welche in die Checklisten aufgenommen werden können, sind die Folgenden (ohne Anspruch auf Vollständigkeit):

- Steuerungs- und Büronetz trennen,
- Ports nach außen schließen, routerseitig und per IEEE **802.1X** (Ein Standard zur Authentifizierung in Rechnernetzen),
- Alarmierung redundant auslegen, einem kompromittierten Leitsystem ist nicht zu trauen, deshalb eine zweite Alarmierungsebene etablieren,
- Tokens statt Passwörtern, z.B. Authentifizierung (Zugriff) per RFID nutzen, Multi-Faktor-Authentisierung für administrative Accounts einführen,
- Anlagen-Zugänglichkeit gesichert durch: Zaun (intakt, tw. beschädigt), Tor (dauerhaft geschlossen, tw. offen, automatisierte Öffnung), keine Zugangsbeschränkungen,
- Regelmäßige Überprüfung von Notstromaggregaten (bspw. Blackout-Tests)
- Kraftstoff-Reserven für Notstromaggregat hinreichend und auf Resilienz gegen Dieselpest geprüft,
- Zugänglichkeit und Verfügbarkeit von Schlüsselschaltern prüfen,
- Zugänglichkeit und Bedienung von Messinstrumenten sicherstellen,
- Definieren und vorab einbinden von Notfallkontakten: THW - Notstromversorgung, Dienstleister (Service Level Agreement), Feuerwehr, …

Jährliche Sensibilisierung (Workshops)

Die aktuelle Untersuchung ist ein guter Startpunkt zur Schärfung des Bewusstseins für Informationssicherheitsbelange. Zur kontinuierlichen Weiterbildung und Sensibilisierung für die Cyber-Sicherheit ist die Durchführung von jährlichen Workshops wichtig, die Wissen so vermitteln sollten, dass es auch im privaten Bereich der Mitarbeiter regelmäßig genutzt wird. Dabei könnten zusätzliche Formate wie bspw. Lernvideos, E-Learning-Systeme, usw. genutzt werden. Vorab sollte dafür eine Umfrage hinsichtlich der letzten Erfahrung möglicher IT-Angriffe oder Probleme erfolgen. Durch Anwendungsfälle auf Kläranlagen kann die Relevanz

für das Personal/ Meister:in/ Betreiber gesteigert werden. Die Workshops sollten unter anderem mit den folgenden Inhalten gefüllt werden:

- Ergebnisdarstellung von Erfahrungen auf anderen Kläranlagen,
- Darstellung aktueller Angriffe auf Industrie und andere kritische Infrastruktur,
- Aufzeigen von neuen Entwicklungen oder Problemstellungen und
- Hinweise auf Checklisten / Standards / Sofortmaßnahmen/ mögliche zukünftige finanzielle Anreize.

Die Durchführung kann auf verschiedenen Ebenen erfolgen, um auch alle verschiedenen Verantwortlichen zu erreichen. Dazu gehören beispielsweise: KDW, Städtetag, VKU (Verband kommunaler Unternehmen), BEW (Bildungszentrum für die Ver- und Entsorgungswirtschaft), DWA, …

Jährliche Begehung

Um eine Betriebsblindheit für Schwachstellen auf den Kläranlagen zu umgehen, ist eine jährliche Begehung mit externen Partnern sinnvoll. Diese können Dienstleister oder auch ein etabliertes Nachbarschaftskollegium sein. Auf dieser kann dann unter anderem auf die Punkte der Checklisten geachtet werden. Dabei ist eine Begehung und Bewertung analog zum Projekt subKRITIS auf Basis des B3S WA anzustreben, weil dadurch auch ein Managementsystem für Informationssicherheit und die jährliche erneute Risikobewertung etabliert werden. Bei den Inhalten können dann die Themen der Cybersicherheit, Stromausfall und physische Eingriffe zusammengebracht werden. Die Ergebnisse der Begehung sollten gründlich dokumentiert werden. Zusätzlich zu den bisherigen Inhalten ist die Aufnahme eines Penetrationstests / Intrusion-Detection Tests zu empfehlen. Es ist sehr empfehlenswert, wenn dies als verpflichtende Maßnahme analog zur Unterweisung für Arbeitssicherheit o.ä. in den Betriebsablauf verankert wird.

Gewährleistung physischer Sicherheit

Physische Sicherheit der Anlagen wirkt sich nicht auf Cyber-Angriffe aus, verhindert aber die lokale Beeinflussung der Anlagen und unterstützt den Bewusstseinswandel aller Mitarbeiter. Hierher zählt alles, vom Zaun, über nicht steckende Anlagenschlüssel bis zur grundsätzlichen Verwendung von Badges zur Freischaltung von Steuerungen.

Aufbau von Nachbarschaften

Besonders im ostwestfälischen Raum zeigt sich, dass durch nicht vorhanden sein von Abwasserverbänden oder ähnlichen Einrichtungen viele Kommunen auf sich alleine gestellt sind. Daraus ergibt sich das Problem, dass nicht jede Kläranlage Personal haben kann, welches sich mit dem aktuellen Stand der Cybersicherheit auskennt. Von daher sollte

beginnend mit einem Austausch zwischen den Kläranlagen zum Thema Cybersicherheit eine Zusammenarbeit zu diesem Thema entstehen. Mögliche Arbeitsebenen dafür wären beispielsweise die bestehenden DWA-Kläranlagennachbarschaften oder die Kläranlagen-Meisterebene. Es kann alternativ aber auch eine Zusammenarbeit auf Kreis- oder Bezirksregierungsebene entstehen.

Vereinheitlichung der Technik auf den einzelnen Anlagen

Während der vorliegenden Untersuchung wurde festgestellt, dass sich auf etlichen Anlagen viele verschiedene Steuerungen der unterschiedlichsten Hersteller fanden. Das führt dazu, dass die Mitarbeiter der Anlagen Know-How für ganz verschiedene Technik erwerben müssen oder unterschiedliche Dienstleister die verschiedenen Techniken warten. Große Anlagenbetreiber versuchen dies bewusst zu vermeiden, weil es nicht wünschenswerte Komplexität ins Spiel bringt. Ursache ist regelmäßig, dass über vorgeschriebene Ausschreibungen solche Hardware eingebaut wird. Aus technischer Sicht ist das eindeutig ein Fehler und es sollte darüber nachgedacht werden, wie dies zu vermeiden ist. Einheitliche Technik wird häufig verhindert, weil die Kriterien bei Ausschreibungen den günstigsten Preis verlangen. Das ist für eine einzelne Ausschreibung vielleicht sinnvoll, kann bei den Folgekosten durch Komplexität aber verheerend wirken. Ggfs. ist über finanzielle Anreize in Form von Zuschüssen im Zusammenhang entsprechender Fördermittel bei Neuplanungen/Anschaffungen in / im BZ, Ministerium nachzudenken, um eine solche Situation zu vermeiden. Adressaten sind aber auch Dienstleister, die sich um einheitliche Technik bemühen sollten.

Betriebskontinuitätsmanagement für Cyber-Sicherheit

Aus der deutschen Wikipedia: „Betriebskontinuitätsmanagement (BKM; englisch: business continuity management (BCM)) bezeichnet in der Betriebswirtschaftslehre die Entwicklung von Strategien, Plänen und Handlungen, um Tätigkeiten oder Prozesse – deren Unterbrechung der Organisation ernsthafte Schäden oder vernichtende Verluste zufügen würden (etwa Betriebsstörungen) – zu schützen bzw. alternative Abläufe zu ermöglichen. Auf Kläranlagen geht es um die Vermeidung der Überschreitung erklärter Werte und genau hier sollte einerseits die Sensorik sicherstellen, dass die Anlagenverantwortlichen frühzeitig fatale Trends erkennen können und es Pläne gibt, wie solcher Entwicklung unmittelbar entgegengewirkt werden kann. Dies nicht nur mit Blick auf wasserwirtschaftliche Parameter, sondern auch mit Blick auf eine ausgefallene IT. Möglichkeiten sind Ersatzrechner/Steuerungen, die schnell und jederzeit beschafft werden können, Virtualisierungsumgebungen, die schnelle Wiederaufnahme der Dienste ermöglichen etc. Im Rahmen dieser Planungen ist unbedingt der Personaleinsatz zu berücksichtigen. Wer spielt welche Rolle und wie ist die Verfügbarkeit für jede Funktion, die zur Wiederherstellung einer voll funktionsfähigen Anlage benötigt wird, sichergestellt.

Zusammenfassend kann daher die Aussage getroffen werden, dass die Betreiber, unabhängig der Größenklasse der zu verantwortenden Kläranlage, die Umsetzung der Maßnahmen des vorhandenen Standards für die Wasserwirtschaft (B3S WA) mittelfristig beginnen sollten. Die Umsetzung des branchenspezifischen Sicherheitsstandards setzt die Implementierung eines ISMS voraus, in dem u.a. die aufgeführten Punkte bzw. Maßnahmen umzusetzen, zu bewerten und zu dokumentieren sind. In einem regelmäßigen Zyklus erfolgen langfristig erneute Überprüfungen und (Risiko-)Bewertungen der Anlagenkomponenten sowie der Informationssicherheit der Anlage, um so ein sich stetig wachsendes Sicherheitsniveau anzustreben.

5.3. Zusammenfassende Darstellung

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

1. *Trennung von IT und Prozesstechnik. Das ist auf den meisten Anlagen bereits 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 IT-Sicherheitsbewusstseins. 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, verliert man bestenfalls einige Stunden, die die Daten nicht aktuell sind.

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. Es 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 anlagen-übergreifenden 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 für Informationssicherheit wecken immer externe Begehrlichkeiten. Die Wasserwirtschaft benötigt sie aber auch.

6. Ausblick

Vor dem Hintergrund der fortschreitenden Digitalisierung und Automatisierung in der Wasserwirtschaft gewinnt die Sicherheit bestehender Informationssysteme zur Steuerung der wasserwirtschaftlichen Infrastruktur zunehmend an Wichtigkeit. Dies insbesondere mit Blick auf die Diskrepanz zwischen dem Willen zu Transparenz, nämlich dem Bürger Zugang zu Anlageninformationen zu geben, und der Missbrauchsmöglichkeit, die sich aus dieser Transparenz für Angreifer ergibt, indem sie einfach an Informationen über lohnende Ziele kommen (Stichwort ELWAS). IT-Systeme bieten prinzipiell einen Angriffspunkt für Manipulation, wenn sie nicht ausreichend geschützt werden. Ein Cyberangriff auf Kläranlagen mit daraus resultierender Funktionsuntüchtigkeit der Anlagen könnte folgenschwere Auswirkungen auf den Vorfluter haben, wenn in Folge der Funktionsuntüchtigkeit der Kläranlage ungeklärtes Abwasser in den Vorfluter abgeschlagen werden muss. Ein solches Versagen dieser Anlagen zieht möglicherweise, zusätzlich zu den negativen Umweltfolgen, strafrechtliche Konsequenzen für den Betreiber nach sich.

Durch das IT-Sicherheitsgesetz und die KritisV wird der Schutz von kritischer Infrastruktur verschiedener Sektoren, darunter die Wasserversorgung und die Abwasserbehandlung gesetzlich vorgeschrieben. Die gesetzliche Verpflichtung zur Einhaltung des Stands der Technik betrifft allerdings nur Betreiber mit einer Zahl angeschlossener Einwohnerwerte von über 500.000 EW. Da die Sicherheit gegenüber Ausfällen bedingt durch Cyberattacken aber auch für kleine bis mittelgroße Betreiber und deren Kunden essenziell ist, erfolgte eine Bestandsaufnahme des Stands der IT-Sicherheit für diese Betreiber.

Im Rahmen der Bestandsaufnahme wurde kurz-, mittel- und langfristiger Handlungsbedarf zur Herstellung einer sicheren IT-Infrastruktur identifiziert.

Bei Anwendung des B3S WA muss ein *Informationssicherheitsmanagementsystem* (ISMS) implementiert sowie die Erreichung eines bestimmten Standes der Technik in einem regelmäßigen Zyklus, vergleichbar mit einer Arbeitssicherheitsunterweisung, angestrebt werden (wozu eigentlich die Erfüllung der Maßnahmen für kritische Infrastrukturen aus dem B3S WA zusätzlich erforderlich ist). 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. Darüber hinaus steht den Betreibern nach Implementierung eines ISMS nach dem B3S WA die Möglichkeit zur Verfügung, sich für das Nachweisverfahren durch Anmeldung beim BSI zu melden, um somit sich die Einhaltung des Stands der Technik und einen Grad der Sicherheit nachweisen zu lassen.

Die Ausführung und Kontrolle der Notstromversorgung ist auf einigen Kläranlagen verbesserungswürdig. Die Notstromversorgung ist auch für physische oder Cyberangriffe von großer Bedeutung und deshalb sollten alle Angriffsfälle kombiniert betrachtet werden.

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 Kontrolluntersuchungen 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).

Den am Projekt teilnehmenden Kläranlagen wurde jeweils ein Einzelbericht zur Verfügung gestellt in dem das jeweilige Vorgehen auf der Kläranlage vorgestellt wurde. Zudem wurden Empfehlungen mit Prioritätenlisten ausgesprochen mit welchen Maßnahmen die IT-Sicherheit erhöht werden kann und wo das Risiko auf wasserwirtschaftlicher Seite liegt und welche verbundenen Maßnahmen ergriffen werden können.

Welche Kläranlagen einen erhöhten Sicherheitsbedarf haben, resultiert aus der Berücksichtigung des nachfolgenden Vorfluters. Denn bei Betrachtung der Kläranlagen zeigte sich, dass die Größe der Kläranlagen keine übergeordnete Rolle spielt, sondern der individuelle Aufbau ist der maßgebende Faktor für die Anfälligkeit einer Anlage. Ein erhöhter Schutzbedarf besteht, wenn es sich um einen Vorfluter mit geringem Durchfluss bzw. hohem Anteil des Kläranlagenzuflusses am Gewässer handelt. Zudem sollte eine Kläranlage prioritär geschützt werden, wenn es relevante wasserwirtschaftliche Nutzungen im Abstrom gibt. Dazu

gehören wasserabhängige Naturschutzräume und Trinkwassergewinnungsanlagen insbesondere bei Rohwasserentnahme aus Oberflächengewässern oder durch Uferfiltration.

Aktuelle Veränderungen bezüglich europäischer Richtlinien bzw. Verordnungen wie bspw. der NIS2-Richtlinie und der damit verbundenen Wandlung in nationales Recht, 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 NIS2-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 IT-Sicherheit 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.

Ausblick auf weitere Forschung

Die bisherige Betrachtung bezieht sich auf 13 Kläranlagen und damit auf 2 % der Kläranlagen in NRW. Um die gewonnen Kenntnisse auszubauen und zu bestätigen, ist eine Erweiterung der Untersuchungen auf weitere Kläranlagen notwendig. Dabei sollten noch kleinere Kläranlagen und auch bisher nicht erfasste Strukturen und Verfahren betrachtet werden. 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 in Deutschland auch die industrielle Abwasserbehandlung eine wesentliche Rolle in der Abwasserbehandlung. 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 IT-Sicherheit auf diesen Kläranlagen existiert. Eine Kontrolle und Ist-Aufnahme sind aufgrund der vielfältigen privaten Betreiber schwierig.

Die ersten Modellierungsergebnisse, welche den Einfluss von wenig bis nicht geklärtem Abwasser auf die Umwelt haben, 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, die sich damit befassen, welche zeitlichen und gewässerspezifischen Faktoren letztendlich zum konkreten Eintritt von ökologischen Schäden und einer erheblichen Beeinflussung der Trinkwassergewinnung führen. Darauf aufbauend kann eine 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

Adepu, S., & Mathur, A. (2016). An Investigation into the Response of a Water Treatment System to Cyber Attacks. *2016 IEEE 17th International Symposium on High Assurance Systems Engineering 17*, (S. 141-147).

Alexander, R. (2018). Anforderungen an Wasserversorger und Abwasserentsorger gemäß DVGW-Merkblatt W 1060 bzw. DWA-Merkblatt M 1060. *energie* | *wasser-praxis*, S. 34-37.

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

BMI. (2009). *Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITISStrategie).* Bundesministerium des Innern und für Heimat.

BSI. (2021). *Die Lage der IT-Sicherheit in Deutschland 2021.* Bundesministerium für Sicherheit in der Informationstechnik.

Clark, R., Hakim, S., & Panguluri, S. (2018). rotecting water and wastewater utilities from cyber-physical threats. *ater and Environment Journal*, S. 2-6.

Deutscher Bundestag. (2019). *Einleitung ungeklärter Abwässer in deutsche Gewässer.* Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Dr. Gero Clemens Hocker, Frank Sitta, Carina Konrad, weiterer Abgeordneter und der Fraktion der FDP. Von https://dserver.bundestag.de/btd/19/137/1913768.pdf abgerufen

DIN4261. (2008). Kleinkläranlagen. Von https://www.steinburg.de/fileadmin/download/buerger-service/dienststellen-ansprechpartner/dezernat-1/amt-fuer-umweltschutz/wasserwirtschaft/download/abwasser/DIN_4261_1.pdf abgerufen

DWA. (2018). *Branchenspezifischer Sicherheitsstandard zur IT-Sicherheit.* In: Branchenarbeitskreis "Datacenter & Hosting", Giese, G.; Bestenlehner, D.; Boyne, G.; Dorn, B.; Eggers, G.; Feichtner, M.; Fölsch, J.;Gerhards, H.; Kranawetter, M.; Nadzeyka, L.; Otten, D.; Saxena, S.; Schmidt, P.; Rauscher,V.; Wienholz, R.

DWA. (2019). *31. Leistungsnachweis kommunaler Kläranlagen.* Von https://de.dwa.de/files/_media/content/06_SERVICE/Zahlen%20%7C%20Fakten%20%7C%20Umfragen/Leistungsnachweis%202018_netz..pdf abgerufen

Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, K. (2020). A Review of Cybersecurity Incidents in the Water Sector. *Journal of Environmental Engineering*, S. 1-4.

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

Kaspersky Labs. (2021). *Was ist Social Engineering?* Von https://www.kaspersky.de/resource-center/definitions/social-engineering [Stand 18.12.2021] abgerufen

KFN. (2021). *Cyberangriffe gegen Unternehmen in Deutschland. Ergebnisse einer Folgebefragung 2020.* Kriminologisches Forschungsinstitut Niedersachsen E.V.

Landratsamt-Ostalbkreis. (05. 01 2022). *ostalbkreis.de*. Von Kleinkläranlagen: https://www.ostalbkreis.de/sixcms/detail.php?_topnav=36&_sub1=31788&_sub2=37427&_sub3=967&_sub4=95059&_sub5=-1&id=95065 abgerufen

Lloyd Owen, D. (2021). Cybercrime, cybersecurity and water utilities. *International Journal of Water Resources Development*(37), S. 1-4.

MKULNV. (2012). *Entwicklung und Stand der Abwasserbeseitigung in Nordrhein-Westfalen.* Düsseldorf: Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen (.

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

Panguluri, S., Patrick, E., & Patrick, W. (2011). Cyber Security: Protecting Water and Wastewater Infrastructure. *Handbook of Water and Wastewater Systems Protection*, S. 285-299.

Rudel, S., & Lechner, U. (2018). IT-Sicherheit für Kritische Infrastrukturen – State of the Art. *Ergebnisse des Förderschwerpunkts IT-Sicherheit für Kritische Infrastrukturen ITS|KRITIS des BMBF*, S. 8-16.

Sayfayn, N., & Madnick, S. (20. 12 2021). *Cybersafety Analysis of the Maroochy Shire Sewage Spill.* Von https://web.mit.edu/smadnick/www/wp/2017-09.pdf abgerufen

USF. (08. 06 2020). Von https://www.usf.uni-osnabrueck.de/forschung/angew_systemwissenschaft/great_er.html abgerufen

Verizon. (2021). *2021 Data Breach Investigations Report.*

Verizon. (17. Januar 2021). *Verizon.* Von Verizon: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ abgerufen

Wienand, I., & Hasch, M. (2019). Sicherheit der Trinkwasserversorgung Teil 1: Risikoanalyse. *Praxis im Bevölkerungsschutz*(15), S. 14-50.

Verizon Inc., „Data Breach Investigations Report 2021". 2021, Seite 81 Utilities nach NAICS Code 22 https://www.verizon.com/business/de-de/resources/reports/dbir/?cmp=paid_search:google:ves_international:gm:awareness&utm_medium=paid_search&utm_source=google&utm_campaign=GGL_BND_DE_Security_DBIR_BMM&utm_content=DE_Security_DBIR&utm_term=%2Bverizon%20%2Bdata%20%2Bbreach&gclid=EAIaIQobChMIzZjwpOHO9AIVjs13Ch3Q1gaqEAAYASAAEgJU6_D_BwE&gclsrc=aw.ds

Anhang

Anhang 1

Tabelle 0-1: Alle verwendeten Daten im GIS-Modell

Layer im Modell	Attribut	Datenquelle	Datensatz
DirectDischarge	Shapes	ELWAS-WEB	Objektdetails der Anlage
	Emission		
	Flow		
	Einleitungspunkt		Korrespondenz
HydroEdge	Shapes	GEOportal.NRW	Fließgewässer NRW
	Qmean	ELWAS-WEB	Regionalisierter Abflusskennwert
	MNQ		
	Depth		HWRM-RL Gefahrenkarten 2. Zyklus 2019
	Velocity Mean		
Dam	Shapes	ELWAS-WEB	Objektdetails der Anlage
	Width	GoogleEarth	
HydroLine	Shape	ELWAS-WEB	Korrespondenz
	Einleitungspunkt		
Gewässereinzugsgebiete	Shapes	GEOportal.NRW	Gewässereinzugsgebiete NRW
Regierungsbezirke			WMS NW Digitale Verwaltungsgrenzen
Trinkwasserschutzgebiete			festgesetzte Trinkwasserschutzgebiete NRW
FFH Gebiet			Gebiete für den Schutz der Natur
Naturschutzgebiet			

Anhang 2

Tabelle 0-2: Vorschlag für eine Checkliste – Checklisten können immer nur kleine Ausschnitte der Sicherheitsanforderungen abfragen. Wir empfehlen deshalb die Umsetzung des B3S WA (Version 3.0, Stand ab 24.03.2022)

1	Objektschutz	Ja	Nein	Bemerkungen / umgesetzte Maßnahme / identifizierter Handlungsbedarf
1.1	Ist das Anlagengelände vollständig umzäunt? Erfolgt eine regelmäßige Überprüfung des Zustandes der Umzäunung? [Perimeterschutz]			
1.2	Findet auf dem Gelände eine Videoüberwachung statt und ist diese DSGVO konform beschildert? Wird die Anlage durch einen Sicherheitsdienst(-leister) außerhalb der Präsenzzeit geprüft bzw. überwacht? [Freilandüberwachung an der Außengrenze und/oder innerhalb des Geländes]			
1.3	Sind Anlageteile bzw. Anlagengebäude alarmgesichert? Sind alle Türen, Tore sowie Fenster auf der Anlage stets verschlossen? Werden Türe, Tore und Fenster mittels Kontaktschalter bzw. Glasbruchsensoren überwacht? [Außenhautschutz/-überwachung]			
1.4	Werden Innenräume der Betriebsgebäude, bspw. mittels Bewegungsmeldern, überwacht? [Innenraumüberwachung / Einzelobjektschutz(-überwachung)]			
2	**Elektroinstallationen / Schaltschränke**	**Ja**	**Nein**	**Bemerkungen / umgesetzte Maßnahme / identifizierter Handlungsbedarf**
2.1	Erfolgt eine regelmäßige Prüfung der Betriebsmittel bzw. der Elektroinstallationen (Verteiler-/ Schaltschränke) gem. DGUV V3 ehemals BGV A3			
2.2	Stecken die Bedienschlüssel in den Schlüsselschaltern innerhalb der			

	verbauten Steuerungen und wenn ja warum?			
2.3	Sind in unmittelbarer Nähe der Elektroinstallationen bzw. Schaltschränken, die zum Öffnen notwendigen Elektrikerschlüssel (Doppelbartschlüssel) verfügbar und wenn ja warum?			
2.4	Sind die verlegten Kabel und Leitungen zu den Anlagen und Steuerungen vor Beschädigungen, bspw. durch Nagetierschäden, geschützt? *Geeignete Maßnahmen können bspw. Leitungsrohre oder auch das Ablängen von Kabel- und Leitungsüberlängen sein.*			
3	**Informationssicherheit**	**Ja**	**Nein**	**Bemerkungen / umgesetzte Maßnahme / identifizierter Handlungsbedarf**
3.1	Ist eine vollständige und aktuelle Betriebsdokumentation, insbesondere die Dokumentation der IT-Infrastruktur (bspw. Netzstrukturplan) und der darin implementierten Komponenten, vorhanden?			
3.2	Führen Sie regelmäßige Awareness-Schulungen der Mitarbeiter zum Thema Informationssicherheit durch?			
3.3	Erfolgt eine strikte Netzwerktrennung der Office-IT und der Steuerungstechnik?			
3.4	Verwenden Sie eine Möglichkeit, bspw. RDP oder TeamViewer, zur Fernwartung bzw. Fernsteuerung des Prozessleitrechners und wenn ja, wie ist diese Verbindung abgesichert?			
3.5	Ist eine Zutrittsregelung und -kontrolle implementiert?			
3.6	Ist ein Rollen- und Berechtigungskonzept etabliert?			
3.7	Sind Richtlinien in Bezug auf die Informationssicherheit bzw. die Nutzung der Geräte und Steuerungen vorhanden und wenn ja, welche?			
3.8	Ist eine Richtlinie oder Dienstanweisung vorhanden, die den Gebrauch von Passwörtern regelt?			
3.9	Werden administrative Accounts tatsächlich nur zu administrativen Zwecken verwendet?			

3.9	Ist eine regelmäßige Datensicherung von Daten und Systemen konzipiert, umgesetzt und wird getestet?			
3.10	Sind Regelungen für den Einsatz von Fremdpersonal vorhanden, wenn ja welche?			