Forschung. Transfer. Nachhaltigkeit.

IT-Sicherheit von Kläranlagen in NRW unterhalb der KritisV

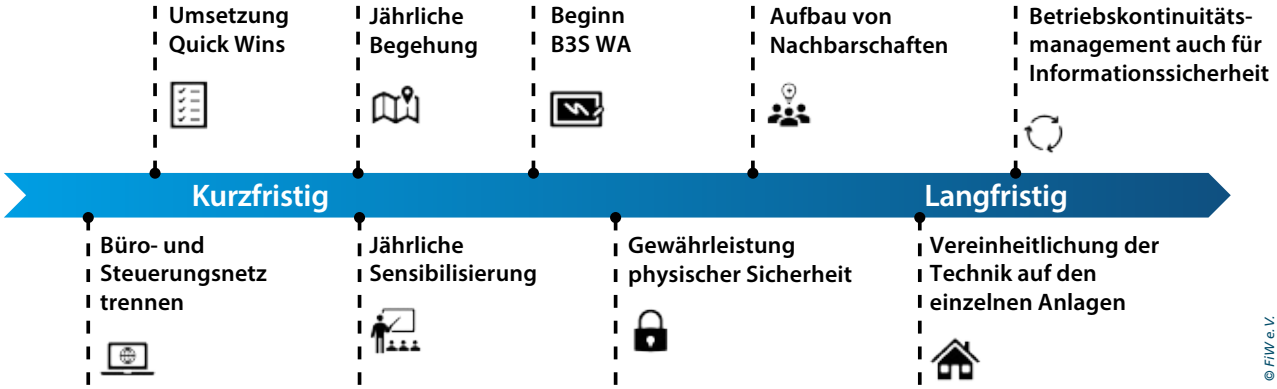
subKRITIS – Bestandsaufnahme des IT-Sicherheitsniveaus von kleinen und mittelgroßen Kläranlagen in NRW unterhalb des Grenzwertes der KritisV

Manipulierbare digitale Oberfläche auf einer Kläranlage.

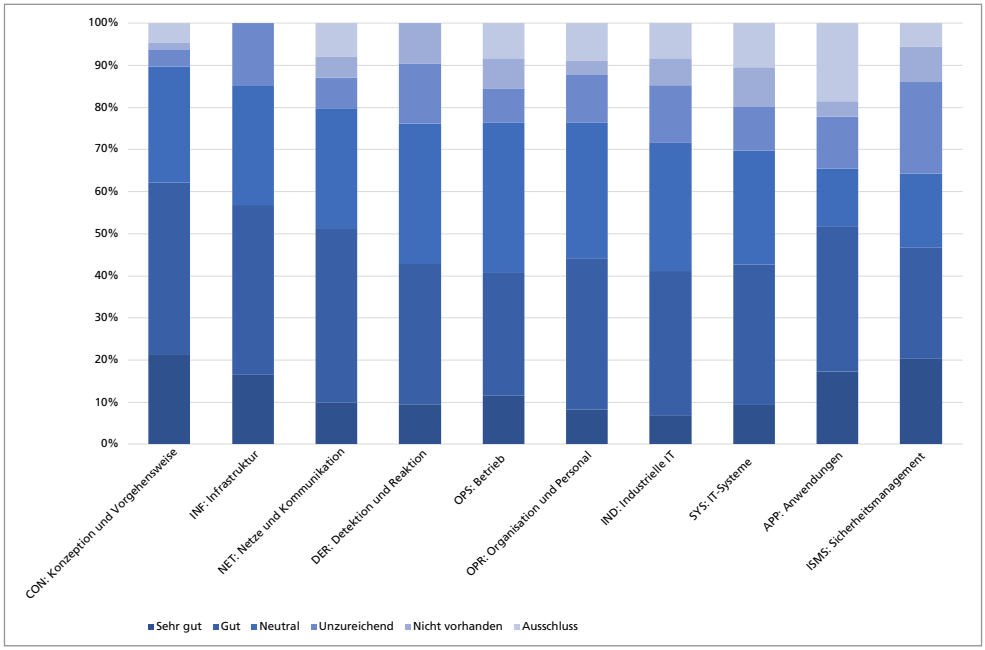
Die Bedrohung durch Cyberangriffe wächst von Jahr zu Jahr an. Kläranlagen unterhalb des Schwellenwertes der KritisV sind bisher zu keinen Maßnahmen zur Informationssicherheit verpflichtet. Wie verwundbar diese Anlagen gegenüber einer steigenden Zahl von Cyberangriffen sind, war bisher unbekannt.

Zur Bestandsaufnahme des Informationssicherheitsniveaus von kleinen und mittelgroßen Kläranlagen in NRW unterhalb des Grenzwertes der KritisV wurden 13 Kläranlagen in Ostwestfalen begutachtet. Dafür wurden Interviews basierend auf dem Branchenspezifischen Sicherheitsstandard Wasser/Abwasser (B3S WA) durchgeführt. Weiterhin wurden durch Modellierungen und Simulationen die Auswirkungen unterschiedlicher Angriffsszenarien abgeschätzt.

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. Ein IT-Angriff auf die Steuerung oder Leitstellensoftware kann massive Konsequenzen für den Betrieb einer Kläranlage, den damit verbundenen Ablaufwerten und resultierend für das Gewässer haben. Zur Bewertung der möglichen abwasserwirtschaftlichen Auswirkungen wurden verschiedene Angriffsszenarien in der Software SIMBA#WATER 4.3 modelliert und simuliert. In diesen Szenarien wurden veränderte Betriebsweisen für alle Verfahren modelliert, welche entweder physisch oder durch einen Cyberangriff auslösbar sind. Die Angriffe erfolgten zunächst einzeln und später zusammengefasst in einem „worst-case" Szenario. Bei einem „worst-case" Szenario liegen bei ca. 30 % der Kläranlagen die Zeitspannen bis zur Grenzwertüberschreitung im Ablauf unter 4 Stunden.



Empfohlener Zeitplan für die kurz- und langfristige Maßnahmen-Umsetzung.



Antworten auf den B3S WA nach Schichten normiert nach abnehmender Zahl positiver Antworten bzw. Schicht.

Werden die Verfahren verglichen, bei denen es am ehesten zu den Grenzwertüberschreitungen kommt, zeigt sich, dass der Ausfall der Belüftung und der Ausfall des Rücklaufschlamm-Abzuges die kritischsten Bereiche auf allen Kläranlagen darstellen. Neben den erhöhten Ablaufwerten lassen sich auch die kritischen Bereiche für die Auslösung von Überflutungen oder Abschlägen aufzeigen. Pumpwerke stellen hierfür die kritischsten Bereiche dar. Ziel dieses Modells war es die wasserwirtschaftliche Relevanz eines Cyberangriffs zu bestimmen.

Durch ein Teil- oder Vollversagen der Kläranlagen resultiert eine Gefährdung für die im Anschluss vorhandenen Vorfluter, Naturräume und wasserwirtschaftliche Infrastruktur.

In diesem Modell wurden beispielhaft die Umweltkonzentrationen von Stickstoff und Phosphor modelliert, welche sich in den Fließgewässern bei verminderter Reinigungsleistung der Kläranlagen im Untersuchungsgebiet einstellen. Werden mehrere Anlagen gleichzeitig Opfer eines Angriffes, summieren sich sowohl die Schadstofffrachten als auch die Volumenströme im Verlauf des Fließweges. Mit Hilfe weiterer Untersuchungen könnte zudem gezeigt werden, welche zeitlichen und gewässerspezifischen Faktoren letztendlich zum konkreten Eintritt dieser Schäden führen. Mit diesem Wissen könnten für jede Kläranlage Risikoanalysen erstellt werden, welche das Schadensmaß eines Angriffes quantifizieren.

Ungeschützter Schieber, welcher physisch nur mit Handrad ohne elektrischen Anschluss bewegt werden kann.

Manipulierbare Messeinrichtung, welche die Kläranalgensteuerung beeinflussen kann.

Einen vollständigen Schutz in der Informationssicherheit zu gewährleisten ist nicht möglich, jedoch ist es bereits mit vergleichsweisem geringem Aufwand möglich, Angreifern ihr Vorhaben so unattraktiv wie möglich zu gestalten. Aus technischer Sicht ist dies durch sauberes Aufsetzen segmentierter Netze und guten Schutz gegen ungewollten äußeren Zugriff zu erreichen und aus organisatorischer Sicht durch eine Verbesserung des Wissens der Mitarbeiter.

Das subKRITIS-Projekt gibt somit eine erste Stichprobenanalyse mit gutem Einblick in die Informationssicherheit kommunaler Kläranlagen unterschiedlicher Größe. Insgesamt kann festgehalten werden, dass das Interesse an Informationssicherheit bei den Verantwortlichen und Beschäftigten der Kläranlagen gegeben, und Wille zur stetigen Verbesserung vorhanden ist und bereits viele Maßnahmen zur Verbesserung der Informationssicherheit ergriffen wurden.

Projektübersicht

PROJEKTTITEL

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

LAUFZEIT

01/2021 – 12/2021

PROJEKTPARTNER

DVGW Service & Consult GmbH

FÖRDERMITTELGEBER / AUFTRAGGEBER

Ministerium für Umwelt, Naturschutz und Verkehr des Landes Nordrhein-Westfalen

Bezirksregierung Detmold

Bad Oeynhausen

ANSPRECHPARTNER

Forschungsinstitut für Wasserwirtschaft und Klimazukunft
an der RWTH Aachen e. V.
Kackertstraße 15 – 17 / 52072 Aachen

Sebastian Kerger, M. Sc.
T +49 241 80 2 68 23 / kerger@fiw.rwth-aachen.de

Dr.-Ing. Kristoffer Ooms
T +49 241 80 2 68 22 / ooms@fiw.rwth-aachen.de

www.fiw.rwth-aachen.de

Mitglied der Johannes-Rau-Forschungsgemeinschaft und der Zuse-Gemeinschaft

Stand
Juni 2023