IT-Sicherheitsniveau kritischer Infrastruktur unterhalb der KritisV

Zuletzt erfolgen Hackerangriffe auch auf deutsche Infrastruktur mit hoher Anzahl und Erfolgsquote. Betroffen sind Krankenhäuser und Kliniken, Kommunen, Stadtwerke, Energieversorger etc. Vor allem bei den Krankenhäusern und Kliniken sind teilweise bis heute, mehr als 12 Monate später, Einschränkungen im Betrieb vorhanden. In Deutschland werden verschiedene Sektoren und Branchen beispielsweise die Energie- und Wasserversorgung, der Verkehr, aber auch die medizinische Versorgung zur Kritischen Infrastruktur gezählt. Der Sektor Wasser wird dabei unterschieden in die Öffentliche Wasserversorgung - Gewinnung, Aufbereitung, Verteilung, Steuerung und Überwachung - und Öffentliche Abwasserbeseitigung - Siedlungsentwässerung, Abwasserbehandlung und Gewässereinleitung, Steuerung und Überwachung. Diese müssen bei Überschreiten der Grenzwerte, die sich an 500 000 Einwohnerwerten orientieren, die Vorgaben der KritisV erfüllen und alle zwei Jahre das Nachweisverfahren gegenüber dem BSI durchlaufen. Im Folgenden werden Pilotprojektergebnisse vorgestellt, welche erstmals das IT-Sicherheitsniveau von Kläranlagen unterhalb der Schwellwerte der KritisV untersucht haben.

Sebastian Kerger, Daniel Löwen, Rainer Stecken und Björn Boos

1 Hintergrund

Die Bedrohung durch Cyberangriffe wächst von Jahr zu Jahr - auch für kritische Infrastrukturen - an [1]. Nicht nur zuletzt durch die Warnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) vor einer erhöhten Bedrohungslage in der Cybersicherheit in Deutschland [2] wächst das Bewusstsein für Informationssicherheit. Vor diesem Hintergrund wurde im Jahr 2021 das Projekt subKRITIS: „Bestandsaufnahme des Informationssicherheitsniveaus von kleinen und mittelgroßen Kläranlagen in NRW unterhalb des Grenzwertes der KritisV - subKritis“ durchgeführt. Die Pflicht zur Informationssicherheit ist für kritische Infrastrukturen seit dem 25.07.2015 durch das Informationssicherheitsgesetz rechtlich festgeschrieben [3]. Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG) und die daran gebundene Verordnung zur Bestimmung Kritischer Infrastrukturen (KritisV) des Bundesministeriums des Innern für das Bundesamt für Sicherheit in der Informationstechnik (BSI) haben Schwellenwerte aufgenommen, die aus dem Katastrophen- und Bevölkerungsschutz kommen. Kritisch ist, was mindestens 500 000 Einwohner betrifft [4]. Alle kritischen Infrastrukturen, die diesen abgeleiteten Schwellenwert überschreiten, wurden zu Maßnahmen zur Steigerung der Informationssicherheit verpflichtet. Somit gilt für Kläranlagen, die unterhalb dieses Schwellenwertes liegen, dass sie zur kritischen Infrastruktur gehören, aber keine Maßnahmen zur Informationssicherheit vorgeschrieben sind. Daraus resultierend war es das Ziel des Pilotprojektes, wie das IT-Sicherheitsniveau dieser Kläranlagen zu bewerten ist.

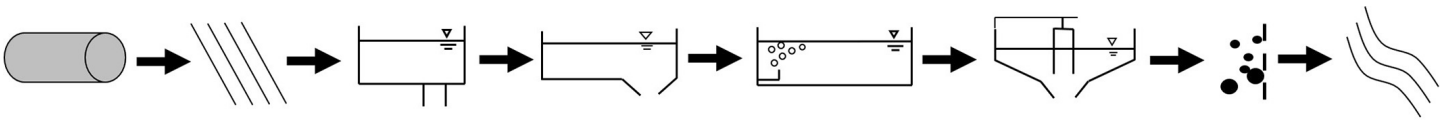
Kompakt

- Eine gute Ausgangslage der Informationssicherheit wurde auf den Kläranlagen festgestellt.
- Die Informationssicherheit sollte durch kurzfristige Maßnahmen und langfristig durch die Umsetzung des B3S WA erhöht werden.
- Eine Priorisierung von Kläranlagen nur nach Ausbaugröße erscheint nicht sinnvoll.

2 Bestandsaufnahme

Zum Stand vom 31.12.2018 gibt es in Nordrhein-Westfalen 599 Kläranlagen von denen 10 oberhalb des KRITIS-Schwellenwertes liegen [5]. Im Projekt wurden insgesamt 13 Kläranlagen in Ostwestfalen begutachtet. Diese sind den Größenklassen 3 bis 5 zuzuordnen und liegen unterhalb der KritisV. Für die Bestandsaufnahme wurde eine Besichtigung und ein Interview durchgeführt. Dabei wird zunächst eine unabhängige Bewertung auf der wasserwirtschaftlichen Seite und auf der IT-technischen Seite durchgeführt. Auf der wasserwirtschaftlichen Seite werden die möglichen Folgen eines Angriffes, die aus dem abwassertechnischen Aufbau der Kläranlagen entstehen können, betrachtet. Als mögliche Schäden werden betrachtet.

- Monetäre Schäden für den Betreiber,
- Umweltschäden und
- Sachschäden



Zulauf	Rechen	Sand-/Fettfang	Vorklärung	Belebung	Nachklärung	Filtration
Verstellung Schieber	Verstellung Schieber	Ausfall Räumer	Ausfall Räumer	Ausfall Belüftung	Ausfall Räumer	Ausfall Fällmittel Dosierung
Manipulation Messonden	Manipulation Messonden	Aktivierung Notumlauf	Aufteilung auf Becken	Manipulation der Belüftungsregelung	Veränderung Rücklaufschlammabzug	Veränderung Rückspülung

© Kerger et al.

Bild 1: Beispielhafte Angriffsszenarien mit möglichen Einwirkungen auf die Verfahrensstufen einer Kläranlage

Im Wesentlichen werden drei Angriffsmöglichkeiten als relevant betrachtet: Physischer Angriff, Cyberangriff und ein Stromausfall. Für jeden dieser Aspekte wurde an den jeweils relevanten Verfahrensstufen eine Bewertung durchgeführt. Mögliche Einflussnahmen auf Kläranlagen sind in **Bild 1** dargestellt. Auf der IT-technischen Seite wird betrachtet, welche Schwachstellen auf den Kläranlagen vorhanden sind, die ein Eindringen in die steuerungsrelevanten Systeme der Kläranlage ermöglichen könnten.

Zur Beurteilung des IT-Sicherheitsniveaus der Kläranlagen wird der Branchenspezifische Sicherheitsstandard Wasser/Abwasser (kurz: B3S WA) [6], wegen seines normativen Charakters und seiner ubiquitären Einsatzmöglichkeit in der Wasserwirtschaft angewendet. Der B3S WA basiert auf der durch § 8a Abs. 3 BSIG [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 kleinere Unternehmen zu schaffen. Der Standard wird alle zwei Jahre weiterentwickelt, um den sich ständig ändernden Herausforderungen zeitnah angepasst zu sein. Zudem hat der Standard von Anfang an Maßnahmen bzw. Anforderungen in zwei Gruppen unterteilt:

- Allgemeine 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.

Auf jeder Kläranlage wurde ein Interview auf Grundlage des B3S WA durchgeführt. **Bild 2** zeigt den vereinfachten Prozessablauf der Durchführung. Zu Beginn der Anwendung des B3S WA werden die Werte der Anlage(n), bspw. Pumpen, identifiziert und aufgelistet bzw. dokumentiert. Die Hauptfrage, die es anschließend zu beantworten gilt, ist „was muss gesichert werden?“. Dementsprechend werden die Anlagen, die es abzusichern gilt, definiert. Für Kläranlagen ist die Bündelung der Assets zu einer Anlage einfach zu leisten. Die Anlage besteht in aller Regel aus allen Werten innerhalb des Schutzzaunes. Im nächsten Schritt erfolgt die Bestimmung der Anwendungsfälle, indem angeschaut wird, wie mit den jeweiligen Anlagen gearbeitet wird. Der B3S WA v2 umfasst 23 Anwendungsfälle, aus denen sich unmittelbar vordefinierte Gefährdungen bzw. Risiken sowie die ihnen entgegenwirkenden Maßnahmen ergeben. Die Risiken lassen sich allerdings nicht mit geschlossenen Fragen, die mit ja oder nein zu beantworten wären, bewerten. Dementsprechend müssen in die Beurteilung der Fragen immer die genauen örtlichen Gegebenheiten einfließen.

Da der B3S WA dem BSI-Grundschutzkompendium [7] unterliegt, soll an dieser Stelle erwähnt werden, dass das Grundschutzkompendium Maßnahmen in sogenannten Bausteinen [8] bzw. Schichten zusammenfasst. Die Antworten aus den gestellten Fragen und ausgewerteten Tabellen ergeben, dass die meisten Fragen aus dem B3S WA im Rahmen dieser Untersuchung aus den Schichten Netze und Kommunikation, Organisation und Personal, Betrieb und IT-Systeme kommen. Die Risiko-Minimierung innerhalb dieser Schichten und damit auch die Risiko-Minimierung von Angriffen über entsprechende Netzverbindungen ist am besten durch korrekte Konfigurationen und qualifiziertes Personal zu gewährleisten.

3 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. Ein informationstechnischer Mangel ist als Gefährdung zu verstehen, dem nicht vollständig durch geeignete Maßnahmen entgegengewirkt wird. Massive Konsequenzen für den Betrieb einer Kläranlage sowie daraus resultierende Ablaufwerte und Konsequenzen für nachfolgende Gewässer sind zu erwarten, wenn durch einen IT-Angriff schreibender Zugriff auf die Steuerung oder Leitstellensoftware erlangt wird. Dann kann auf alle Systeme, Komponenten, Bauteile o. ä. zugegriffen werden, welche sonst nur über die Leitstelle steuerbar sind.

Ob einzelne Anlagen-Prozesse veränderbar sind, ist individuell unterschiedlich. So werden an einigen Kläranlagen noch viele Schieber rein händisch oder Dosierungen über konstante Volumenströme eingestellt. 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 einem Kontrollgang auffällt.

3.1 Abwasserwirtschaftliche Auswirkungen

Zur Bewertung der möglichen abwasserwirtschaftlichen Auswirkungen auf die 13 Kläranlagen wurden verschiedenen

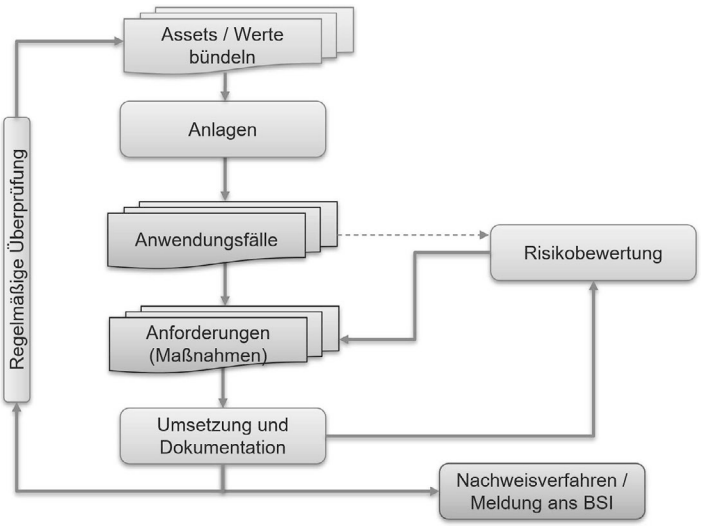


Bild 2: Vereinfachte Prozessdarstellung des branchenspezifischen Sicherheitsstandards

Angriffsszenarien in der Software SIMBA#WATER 4.3 modelliert und simuliert. Als Szenarien wurden drei Zeiträume für die Fehlererkennung und -behebung gewählt:

1) Bereitschaftsstörung: 4 h
2) Angriff zwischen Kontrollgängen (Wochenenden): 24 h
3) Versteckter Eingriff: 7 Tage

In diesen Szenarien wurden veränderte Betriebsweisen für alle Verfahren modelliert, welche entweder physisch oder durch einen Cyberangriff auslösbar sind. Dies erfolgte zunächst einzeln und später zusammengefasst in einem Extremfall Szenario.

Die Ergebnisse zeigten, dass es bei allen Kläranlagen innerhalb eines Tages zu Grenzwertüberschreitungen im Ablauf kommen kann. Bei einem Extremfall-Szenario liegen bei ~30 % der Kläranlagen die Zeitspannen bis zu Grenzwertüberschreitungen unter 4 Stunden. 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 (analog zum Ausfall der zugehörigen Pumpen, Ausfall der Räumer oder Herabfahren eines Dekanters) 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.

3.2 Wasserwirtschaftliche Relevanz

Weitergehend wurde ein Stoffstrommodell aufgebaut. Ziel dieses Modells war es, die wasserwirtschaftliche Relevanz eines Cyberangriffes zu bestimmen. Durch ein Teil- oder Vollversagen der Kläranlagen resultiert eine Gefährdung für die im Anschluss vorhandenen Vorfluter, Naturräume und wasserwirtschaftlichen Infrastruktur. In diesem Modell wurden beispielhaft die Umweltkonzentration von Stickstoff und Phosphor modelliert, welche sich in den Fließgewässern bei verminderter Reinigungsleistung der Kläranlagen im Untersuchungsgebiet einstellt.

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 diesem Projekt nur Qualitätsnormen als Grenzwerte zur Entstehung von Schäden verwendet. Mit Hilfe weiterer Untersuchungen könnte zudem gezeigt werden, 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. Mit diesem Wissen könnten für jede Kläranlage Risikoanalysen erstellt werden, welche das Schadensmaß eines Angriffes quantifizieren. Als Betrachtung kämen dafür die Anzahl geschädigter Personen, geschützte Naturräume oder Trinkwassergewinnungsanlagen in Frage.

3.3 Priorisierung von Kläranlagen

Die Priorisierung 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 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 Kläranlagen basierend auf Kenndaten schützenswerter sind als andere. Auch die Größe der Kläranlagen spielt keine übergeordnete Rolle, sondern die individuellen Rahmenbedingungen sind 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 im Gegensatz zur KritisV in der Priorisierung mehr Wert auf den Anteil des Kläranlagenabflusses am Gewässer und auf relevante Nutzungsarten im Gewässer - wie die Trinkwasserversorgung - gelegt werden.

3.4 Übertragbarkeit der Ergebnisse

Insgesamt gibt die Untersuchung im subKRITIS-Projekt eine erste Stichprobenanalyse mit gutem Einblick in kommunale Kläranlagen unterschiedlicher Größe. Auf Grund der Vielfalt der kommunalen Kläranlagen ist dieses Vorhaben aber nicht als

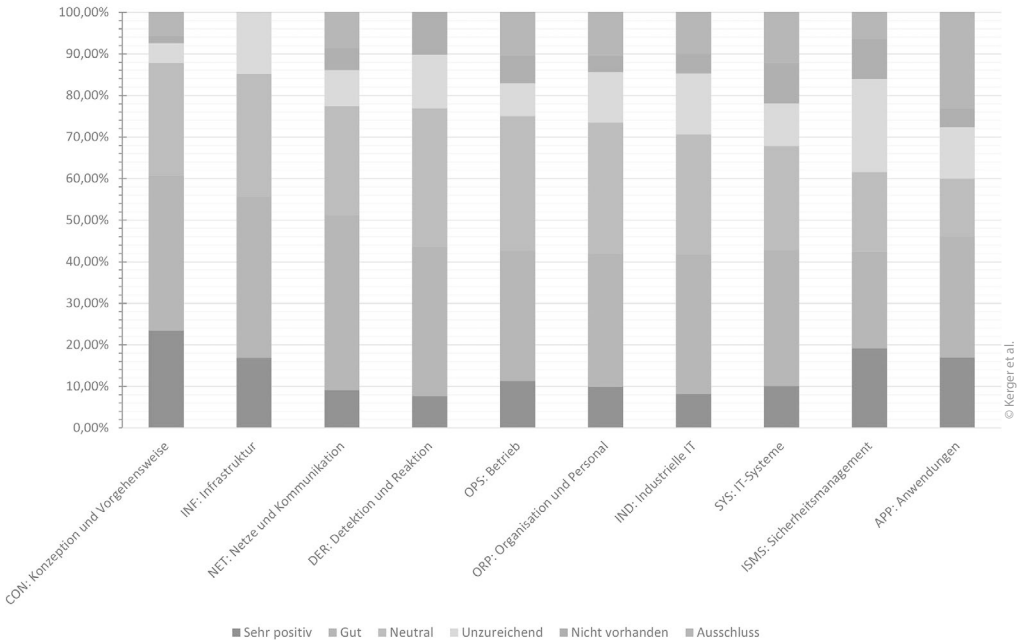


Bild 3: Antworten auf den B3S WA nach Schichten normiert nach abnehmender Zahl positiver Antworten bzw. Schicht

repräsentativ für ganz NRW anzusehen. Für eine repräsentative Aussage für alle Kläranlagen muss die Stichprobenanzahl erhöht werden. Dafür wäre ein regionaler Vergleich und ein Vergleich der Organisation (durch beispielsweise Wasserverbände) relevant, um regionale oder organisatorische Strukturen und Muster zu unterscheiden. Zudem wurden beispielsweise bisher keine Kläranlagen mit Membranverfahren betrachtet.

4 IT-Sicherheitsniveau

4.1 Auswertung des Informationssicherheitsniveaus

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

Eine normierte Auswertung der Antworten des B3S WA nach Schichten ist **Bild 3** zu entnehmen. Diese zeigt auf, wo die Stärken und Schwächen im Bereich der Kläranlagen liegen. Spezifische Auswertungen für die drei untersuchten Größenklassen erscheinen nicht sinnvoll, weil die jeweilige Gesamtzahl zu gering ist. Vor allem in den Schichten „Konzeption und Vorgehensweise“ sowie „Infrastruktur“ sind bereits über 60 % der Antworten „sehr positiv“ oder „gut“ ausgefallen. Die Schichten „Anwendungen“ und „Sicherheitsmanagement“ fallen dem gegenüber ab.

Die technische Auswertung der Simulationsergebnisse einerseits und der Befragungsergebnisse nach dem B3S WA andererseits finden in Excel statt. Die Datenstrukturen unterscheiden sich in beiden Fällen stark. Deshalb werden zwei Tabellen verwendet. Eine Tabelle erlaubt die Auswirkung auszuwerten. Die andere Tabelle wird dazu genutzt, aus den wasserwirtschaftlichen Folgen, die für eine Anlage betrachtet werden, zu ermitteln bezüglich welcher Informationssicherheits-Anforderungen etwas verbessert werden muss, damit diese Folgen gar nicht erst eintreten.

Aus dieser Zusammenführung war es möglich, den teilnehmenden Kläranlagen priorisierte Anforderungslisten mitzugeben, die dem BSI-Grundschutzkompendium 2019 entnommen sind und den Anlagenbetreibern zur Umsetzung empfohlen wurden. Diese Anforderungen haben sich aus den jeweiligen Anwendungsfällen für die Anlagen ergeben und sind die anlagenspezifischen Empfehlungen zur Verbesserung der Sicherheit für jeden Betreiber. Es hilft den Anlagenbetreibern zu priorisieren, was vorrangig umgesetzt werden muss, und reduziert so den zwingend zu leistenden Aufwand. Dies bedeutet 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.

4.2 Empfehlungen zur IT-Sicherheit

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

Natürlich müssen Steuerungen parametriert und hier und da auch Anpassungen an der Leitstellensoftware vorgenommen werden. Allerdings können grundsätzlich Steuerungen, die nicht aus dem Internet erreichbar sind, auch nicht von dort kompromittiert werden. Was sich so trivial anhört, ist die beste Methode zum Schutz kritischer Infrastrukturen. Und in der Tat gehen viele Unternehmen der kritischen Infrastruktur so vor, zu der ebenfalls Energieversorger zählen.

Ein großes Problem der Umsetzung sind fehlende Kapazitäten auf Seiten der Betreiber. Insbesondere kleine Betreiber haben zu wenig Personal, um eine ausreichende IT-Sicherheitskompetenz aufzubauen. Daher sollten IT-Sicherheits-Kooperationen zwischen Unternehmen aufgebaut werden. Zu demselben Schluss sind auch Schramm und Zimmermann [9] gekommen. Im Rahmen des Projektes wurden Vorträge vor den Kanal- und Kläranlagennachbarschaften des DWA NRW gehalten, in dessen Nachgang mehrere Betreiber ihren Kooperationswillen bekräftigt haben.

5 Ausblick

Im Rahmen der Bestandsaufnahme wurde kurz-, mittel- und langfristiger Handlungsbedarf zur Herstellung einer sicheren IT-Infrastruktur identifiziert. Mit Blick auf aktuelle Veränderungen bezüglich europäischer Richtlinien bzw. Verordnungen wie bspw. der NIS2-Richtlinie und der damit verbundenen Wandlung in nationales Recht ergibt sich weiterer Handlungsbedarf in puncto Informationssicherheit. Aufbauend auf diesen Veränderungen wird erwartet, dass zukünftig mehr Kläranlagen zu Informationssicherheitsmaßnahmen verpflichtet werden. Durch die Betrachtung der wasserwirtschaftlichen Relevanz von Kläranlagen zeigt sich ebenfalls deutlich, dass auch kleinere Kläranlagen einen großen Handlungsbedarf aufweisen.

Langfristig wird allen Kläranlagenbetreibern empfohlen, mit einer Umsetzung des B3S WA zu beginnen [10]. 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. Kurzfristig können erste anlagenspezifische Maßnahmen durchgeführt werden, um einen Grundstein zur Erhöhung der Informationssicherheit zu legen. Dazu gehören beispielsweise regelmäßige Schulungen, Trennung von IT und Prozess- bzw. Steuerungstechnik, regelmäßige Prüfung von Zugriffs- und Benutzermanagement oder regelmäßige Prüfung auf Updates der Softwarekomponenten.

Sebastian Kerger, Daniel Löwen, Rainer Stecken and Björn Boos

IT security level of critical Infrastructure below the KritisV

Recently, hacker attacks are also taking place on German infrastructure with high numbers and success rates. Hospitals and clinics, municipalities, public utilities, energy providers, etc. are affected. Particularly in the case of hospitals and clinics, there are still restrictions on operations in some cases today, more than 12 months afterwards. In Germany, various sectors and industries, such as energy and water supply, transport, but also medical care, are counted as critical infrastructure. The water sector is divided into public water supply - extraction, treatment, distribution, control and monitoring - and public wastewater disposal - urban drainage, wastewater treatment and water discharge, control and monitoring. These must meet the requirements of the KritisV if the threshold values, which are based on 500 000 population equivalents, are exceeded, and must undergo the verification procedure vis-à-vis the BSI every 2 years. In the following, pilot project results are presented, which for the first time examined the IT security level of wastewater treatment plants below the threshold value of KritisV.

Dank

Dieses Projekt wurde durch die Bezirksregierung Detmold und das Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen unter der Kennziffer: IT-01/20-BO gefördert. Als Zuwendungsempfänger fungierten die Stadtwerke Bad Oeynhausen.

Autoren

Sebastian Kerger, M. Sc.
Daniel Löwen, M. Sc.
Forschungsinstitut für Wasserwirtschaft und Klimazukunft
an der RWTH Aachen (FiW) e. V.
Kackertstraße 15-17
52072 Aachen
kerger@fiw.rwth-aachen.de
loewen@fiw.rwth-aachen.de

Rainer Stecken, ISO 27001 Lead Auditor
Björn Boos, B. A.
DVGW Service & Consult GmbH
Josef-Wirmer-Straße 1-3
53123 Bonn
rainer.stecken@dvgw-sc.de

Literatur

[1] Spinnler, T.: Kliniken im Visier der Hacker. 28.06.2021. (www.tagesschau.de/wirtschaft/technologie/cybersicherheit-infrastruktur-hacker-kliniken-cybercrime-101.html; Abruf 25.03.2022).
[2] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Cyber-Sicherheitslage im Zusammenhang mit dem russischen Angriff auf die Ukraine. 16.03.2022 (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Ukraine-Krise/ukraine-krise_node.html; Abruf 20.03.2022).
[3] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) vom 14. August 2009 (BGBl. I S. 2821), zuletzt geändert durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982).
[4] Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV) vom 22. April 2016 (BGBl. I S. 958), zuletzt geändert durch Artikel 1 der Verordnung vom 6. September 2021 (BGBl. I S. 4163).
[5] Landesbetrieb Information und Technik Nordrhein-Westfalen (Hrsg.): Elwas-web. (www.elwasweb.nrw.de; Abruf 05.07.2021).
[6] DWA; DVGW (Hrsg.): IT-Sicherheitsleitfaden (https://v2.b3s-wa.de; Abruf 25.03.2022).
[7] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Informationssicherheit mit System - Der IT-Grundschutz des BSI. Bonn, 2020.
[8] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Bausteine. 2022. (www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html; Abruf 25.03.2022).
[9] Schramm, E.; Zimmermann, M.: Cybersicherheit in der Siedlungswasserwirtschaft, insbesondere bei kleinen Unternehmen. In: Korrespondenz Abwasser Abfall 69. (2022), Nr. 2, S. 122-126.
[10] DVGW (Hrsg.): Wassersektor vor Cyberangriffen schützen - Update des IT-Sicherheitsleitfadens veröffentlicht - Cloud-Nutzung, Internet of Things und Angriffserkennung neu im Fokus. (www.dvgw.de/der-dvgw/aktuelles/presse/presseinformationen/dvgw-presseinformation-vom-07042022-it-sicherheitsleitfaden-update; Abruf 25.03.2022).