Research. Transfer. Sustainabilty.

IT Security of Wastewater Treatment Plants in NRW below the KritisV

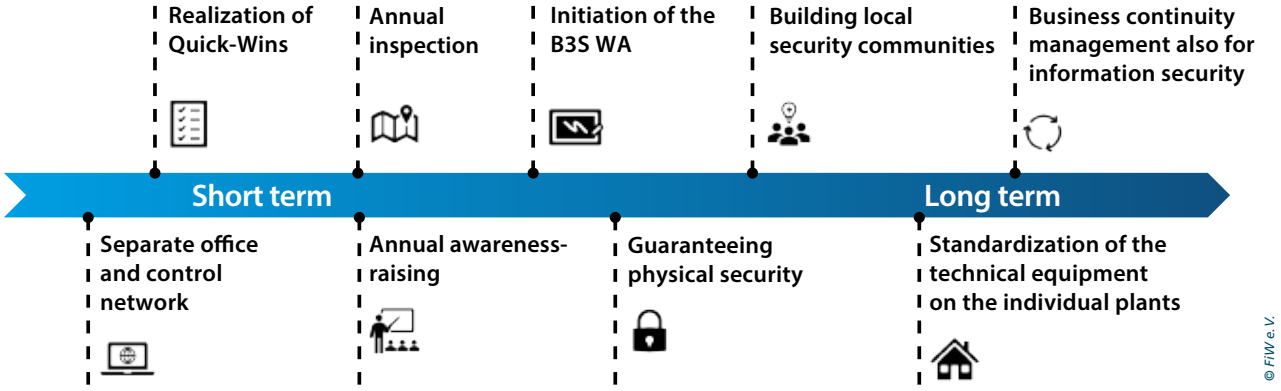
subKRITIS – Assessment of the IT security level of small and medium-sized wastewater treatment plants in North Rhine-Westphalia below the KritisV (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) threshold

Manipulable digital interface on a wastewater treatment plant.

The threat of cyber attacks is growing from year to year. Wastewater treatment plants below the KritisV threshold have not yet been obliged to implement any information security measures. How vulnerable these plants are to an increasing number of cyberattacks was previously unknown.

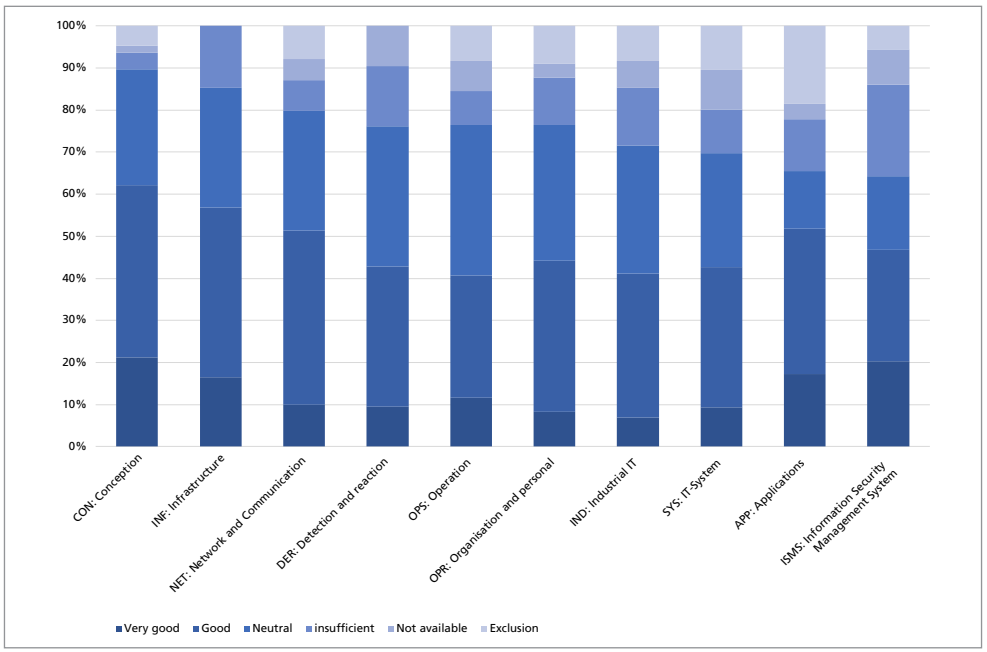
To assess the information security level of small and medium-sized wastewater treatment plants in NRW below the KritisV threshold, 13 wastewater treatment plants in East Westphalia were examined. Interviews were conducted based on the industry-specific security standard for water/wastewater (B3S WA). Furthermore, the effects of different attack scenarios were estimated using modeling and simulations.

The relevance of the risks for the water management sector essentially depends on whether the IT defects can have a direct controlling effect on plant control systems or the control center software. An IT attack on the control system or control center software can have massive consequences for the operation of a wastewater treatment plant, the associated discharge values and, as a result, for the waterbodies. Various attack scenarios were modeled and simulated in the SIMBA#WATER 4.3 software to evaluate the potential impact on wastewater management. In these scenarios, changed operating modes were modeled for all processes, which can be triggered either physically or by a cyber attack. The attacks were initially carried out individually and later summarized in a worst-case scenario. In a worst-case scenario, the time periods until the limit value is exceeded in the effluent are less than 4 hours for approx. 30 % of the wastewater treatment



© FiW e. V.

Recommended timeline for the implementation of measures in the short and long term.



© DVGW S&C

Answers to the B3S WA normalized by layers according to decreasing number positive answers.

plants. A comparison of the processes that are most likely to cause limit values to exceed shows that the failure of aeration and the failure of return sludge discharge are the most critical areas at all wastewater treatment plants. In addition to the increased discharge values, the critical areas for triggering flooding or discharge of wastewater can also be identified. Pumping stations are the most critical areas for this. The aim of this model was to determine the water management relevance of a cyberattack.

A partial or complete failure of the wastewater treatment plants results in a threat to the receiving waters, natural areas and water management infrastructure in the surrounding area. In an additional model, the environmental concentrations of nitrogen and phosphorus were modeled as examples, which occur in the watercourses when the purification performance of the wastewater treatment plants in the study area is reduced. If several plants fall victim to an attack at the same time, both the pollutant loads and the volume flows in the course of the flow path add up. With the help of further investigations, it could also be shown which temporal and water-specific factors ultimately lead to the actual occurrence of this damage. With this knowledge, risk analyses could be drawn up for each wastewater treatment plant, quantifying the extent of damage caused by an attack.

Unprotected gate, which can only be physically moved by handwheel without electrical connection.

Manipulable measuring device that can influence the sewage treatment plant control.

It is not possible to guarantee complete protection in information security, but it is possible to make attackers' plans as unattractive as possible with comparatively little effort. From a technical point of view, this can be achieved by setting up cleanly segmented networks and good protection against unwanted external access and, from an organizational point of view, by improving the knowledge of employees.

The subKRITIS project thus provides an initial sample analysis with a good insight into the information security of municipal wastewater treatment plants of different sizes. Overall, it can be stated that there is an interest in information security among the managers and employees of the wastewater treatment plants, that there is a willingness for continuous improvement and that many measures have already been taken to improve information security.

Project overview

PROJECT TITLE

subKRITIS – Assessment of the IT security level of small and medium-sized wastewater treatment plants in North Rhine-Westphalia below the KritisV (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz) threshold

PROJECT PERIOD

01/2021 – 12/2021

PROJECT PARTNER

DVGW Service & Consult GmbH

FUNDING / PRINCIPAL

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

Bezirksregierung Detmold

Bad Oeynhausen

CONTACT

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

As a member of the JRF research community, FiW is funded by the state of North Rhine-Westphalia.
The FiW is a member of the Zuse-Gemeinschaft.

Status
June 2023