Achtsamkeit

Einmal mehr hingucken – und auf „Dennoch-Ereignisse“ vorbereitet sein

Was die Wasserwirtschaftsunternehmen zur Minimierung von Cyberrisiken und zur Minimierung der Folgen erfolgreicher Cyberangriffe tun müssen – und tun sollten

Stand 24.3.2022

KDW
Kompetenzzentrum
Digitale Wasserwirtschaft

Warum diese Handreichung

Alle Strukturen der Wasserwirtschaft, die Teil der Daseinsvorsorge sind, müssen bestmöglich vor Cyberangriffen und Cyberausfällen geschützt werden, damit die 24/7 Leistungsfähigkeit aufrecht erhalten wird.

Was hierzu umzusetzen ist bzw. umgesetzt werden sollte, ist für die Branchen Wasser und Abwasser in den Merkblättern DWA-M 1060 bzw. DVGW-W 1060 beschrieben. Die Merkblätter und der damit in Verbindung stehende IT-Sicherheitsleitfaden der regelsetzenden Branchenverbände richten sich an **alle** Wasserwirtschafts-Unternehmen. Für die Unternehmen, die die Schwellenwerte der BSI KRITIS-V überschreiten, gelten dabei weitergehende Anforderungen und Maßnahmen als für die übrigen.

Aber: Die Basis-Maßnahmen (Maßnahmen der Kategorie A) gelten für alle. Wir raten deshalb dringend, den IT-Sicherheitsleitfaden der Branchenverbände anzuwenden.

Der aktuelle Branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA 2021) ist vom BSI wieder als geeignet anerkannt worden und steht in Kürze bei den regelsetzenden Verbänden DVGW und DWA bereit.

Damit der Branchenstandard eine zügige und bessere Durchdringung in der Fläche erreicht, werden wir als Kompetenzzentrum Digitale Wasserwirtschaft gGmbH in Zusammenarbeit mit dem DVGW und DWA in den nächsten Wochen (Stand 21.03.2022) Cybersicherheits-Tage und ggf. Weiteres anbieten.

Zum Kompetenzzentrum Digitale Wasserwirtschaft

Wir sind eine gemeinnützige GmbH. Unsere Gesellschafter sind das Ministerium für Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen, die sondergesetzlichen Wasserverbände in NRW, die Stadtentwässerungsbetriebe Köln, die Rheinisch-Westfälische Wasserwerksgesellschaft mbH und die Gelsenwasser AG.

Wie ist die aktuelle Sicherheits-Lage und wo kann ich mich aktuell informieren

Nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gibt es aktuell (Stand 18.3.2022) als Teil des Ukraine-Angriffs bzw. in Zusammenhang bisher keine besonderen Cyber-Auffälligkeiten beobachtet worden. Diese Lageeinschätzung kann sich aber täglich ändern (s. unten – wo kann ich mich informieren).

Trotzdem gilt für alle Wasserwirtschaftsunternehmen besonders achtsam zu sein.

Aktuelle Informationen zur Lage finden Sie u.a. an nachfolgenden Stellen. Die Mitgliedschaft in der Allianz für Cybersicherheit bzw. für größere Unternehmen im UP KRITIS beim BSI wird dringend empfohlen.

Informationen branchenübergreifend	
Allianz für Cybersicherheit	https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Home/home_node.html
Bundesamt für Sicherheit in der Informationstechnik	https://www.bsi.bund.de/DE/Home/home_node.html (Auf der Startseite unter „Meldungen“ und unter „Sicherheitsinformationen“)
Informationen für die Wasserwirtschaft, Fragen stellen, Diskutieren	
Kompetenzzentrum Digitale Wasserwirtschaft gGmbH	https://www.kompetenzzentrum-digitale-wasserwirtschaft.de/ Links auf die zentralen Informationen von BSI, Allianz für Cybersicherheit und aus anderen Quellen
Community Wasserwirtschaft	www.community.kdw-nrw.de Diskussionsforum rund um die Digitalisierung für die Wasserwirtschaft. Einmalige Registrierung ist erforderlich. Lassen Sie sich davon nicht abschrecken, es ermöglicht die Diskussion „im geschlossenen Raum der Wasserwirtschaftsbranche“. Im Space „Zur Sicherheitslage“ können Sie Fragen stellen und Hinweise an die Kollegen:Innen geben.
Fachverbände DWA und DVGW	Ansprechpartner DWA, Ansprechpartner DVGW
	IT-Sicherheitsleitfaden

Was sollte ich jetzt (zusätzlich) tun

Auf den „Dennoch-Fall“ vorbereiten

Ein erfolgreicher Angriff auf den operativen Betrieb von Wasserversorgungsanlagen, Kläranlagen, Kanalnetzbetrieben, Hochwasserschutzanlagen ist komplex und schwierig, aber nicht unmöglich. Deshalb sollte sich jeder Betrieb auf diesen „Dennoch-Fall“ vorbereiten, genauso wie er sich selbstverständlich auf die Möglichkeit eines Stromausfalles, einer Extrem-Wetterlage oder eines sonstigen Umweltereignissen mit Folgen für den ordnungsgemäßen Betrieb vorbereitet.

Was heißt das konkret bezogen auf die Sicherheit von **Information Technology (IT) und Operation Technology (OT)**?

1. **Legen Sie regelmäßig, durchaus in enger Taktung, Backups an, auch offline!**
   - Überprüfen Sie, ob aktuelle Backups bzw. Datensicherung aller relevanten Unternehmensdaten, sowohl bezogen auf Verwaltungsdaten als auch bezogen auf Betriebsdaten, vorhanden sind.
   - Testen Sie erstellte Backups, auch um sicherzustellen, ob eine Wiederherstellung aus diesen Daten heraus möglich ist.
   - Legen Sie Backups auch „offline“ an und lagern Sie die Datenträger nach dem Backup-Vorgang im Tresor. Backups, die über das Datennetz erreichbar sind, sind erreichbar.
2. **Prüfen Sie Ihre Notfallpläne**
   - Decken Ihre Notfallpläne auch den „Cyber-Notfall“ ab? Können Sie die Mitarbeiter:Innen im Notfall auch „offline“ erreichen; sowohl die Mitarbeiter:Innen, die im Notfall den Betrieb „händisch“ aufrechterhalten müssen als auch die Mitarbeiter:Innen und ggf. Dienstleister, die die IT und/oder OT wieder anfahren können.
   - Bauen Sie sich ein „zweites Netz“ auf. Gemeint ist hier nicht ein technologisches Netz, sondern ein Netzwerk von Kompetenzträger:Innen, die im Notfall mithelfen können. Wissen Sie, wen Sie

zu Hilfe rufen können, wenn die eigenen Kapazitäten und Kompetenzen für den noch nie erlebten, vermutlich auch nicht geübten, Dennoch-Fall nicht ausreichen? (s. hierzu auch unten: Wer kann helfen?)

Cyberrisiken vermindern

Alle sogenannten A-Maßnahmen, die im IT-Sicherheitsleitfaden des B3S WA 2021 genannt sind, sollten umgesetzt werden. Die nachfolgend genannten Maßnahmen sind in diesem Kontext im Sinne von SOFORT-Maßnahmen aufgrund der aktuellen Lage zu verstehen, alle weiteren Maßnahmen sind ebenfalls als allgemeine Regeln der Technik umzusetzen.

3. **Führen Sie Updates regelmäßig und zügig durch**
    - Stellen Sie sicher, dass alle Updates - insbesondere Sicherheits-Updates - für **Betriebssysteme** und **relevante Softwarekomponenten** regelmäßig und zügig nach Veröffentlichung durchgeführt werden, auch auf Mobile Devices wie Smartphones und an HomeOffice-Arbeitsplätzen. Dies gilt ausnahmslos für alle Devices, die dauerhaft oder gelegentlich Verbindung zum Internet haben. Beispielsweise sollten nach einem Patch-Tuesday von Microsoft (2.ter Dienstag im Monat) sollten nicht mehr als drei Tage verstreichen, bis alle Systeme mit den Patches versehen sind.
    - Im Moment werden täglich mehr als 300.000 neue Schadprogramme bekannt. **Updates der Virenschutzlösungen** müssen deshalb aktuell und automatisiert vorgenommen werden. Bitte beachten Sie zudem die aktuellen Warnungen des BSI (-- wo kann ich mich informieren).
    - Berücksichtigen Sie bei den Updates unbedingt auch die Netzwerkkomponenten, wie z.B. **Router, Switches** etc.
    - Überprüfen Sie im Bereich der OT die Update-Regeln für Steuerungsgeräte und IoT (Internet of Things, zum Beispiel Sensoren mit Datenübertragung über Funkstrecken) und stellen Sie sicher, dass vom Hersteller freigegebene oder vom BSI empfohlene Updates auch zeitnah eingespielt werden; auch auf Geräten, die keine permanente Verbindung zum Internet haben. Wenn dazu eine Internet-Verbindung, die ansonsten nicht besteht, erforderlich ist, sollten Sie diese über Multi-Faktor absichern und sofort wieder abschalten, wenn das Update abgeschlossen ist.

4. **Trennen Sie die IT- und OT-Netze**
    - Richten Sie für die OT ein eigenes und von der IT getrenntes Netzwerk ein. Das kann in Form eines virtuellen Netzwerks erfolgen, welches durchaus dasselbe physikalische Netz nutzt, wie die IT.
    - Wenn Sie ein WLAN im OT-Bereich nutzen, ist dieses mit den stärksten Sicherheitsmaßnahmen abzusichern.
    - Es sind zudem persönliche User-Accounts zu nutzen. Ein nicht personalisierter Zugang oder ein Zugang über die IT zu den OT-Systemen ist nicht zulässig.

5. **Sichern Sie die Zugriffsmöglichkeiten auf das Internet ab!**
    - Internetverbindungen sollten aus den OT-Systemen nur explizit aus definierten Gründen heraus erfolgen. Sie sind nach der vorgesehenen Nutzung sofort wieder zu schließen.
    - Erschweren Sie Angreifern den Zugriff auf Konten und Verwaltungsoberflächen.
    - Setzen Sie im Idealfall überall die Multi-Faktor Authentifikation oder zumindest komplexe Passwörter ein. Passwörter sollten mindestens 12-stellig sein, für Admin-Konten auch länger und komplexer.

- Stellen Sie sicher, dass die Admin-Konten nicht für alltägliche Routine-Arbeiten verwendet werden.
- Passwörter müssen sich von System zu System unterscheiden. Passwörter aus dem dienstlichen Umfeld dürfen NIE im privaten Umfeld verwendet werden.

6. Machen Sie die Türen zu!

Diese Hinweise wirken überflüssig, bilden aber durchaus in einigen Fällen erlebte Realität ab und können deshalb nicht oft genug wiederholt werden.

- Machen Sie die Türen zu, lassen Sie Schlüssel nicht auf Schlössern stecken, seien Sie informiert, welche Dritten sich wo auf dem Gelände bewegen. Ein USB-Stick ist schnell eingesteckt, ein Steuerungskasten ist schnell aufgebrochen. Vertrauen ist gut, aber Kontrolle ist tatsächlich besser.

7. Seien Sie achtsam und achten Sie darauf, dass es auch alle Kollegen:Innen sind

2-Faktor-Authenitifzierung ist unbequem, Phishing-Mails sind immer schwerer zu erkennen, komplexe Passwörter nicht zu merken, und wenn ich mal nicht da bin, muss doch der Kollege an den Rechner kommen. So nachvollziehbar die Argumente sind, so richtig ist es auch, dass der „Faktor Mensch“ das schwächste Glied in der Sicherheitskette ist.

- Sensibilisieren Sie immer wieder für die Gefahr von Phishing-Mails
- Bieten Sie sichere, gleichzeitig komfortable Lösungen wie Passwort-Tresore an.

Den Betrieb dauerhaft cyber-sicherer aufstellen

- Beachten Sie den (aktualisierten) Branchenstandard B3S WA und arbeiten Sie den IT-Sicherheitsleitfaden angemessen, entsprechend der Anforderungen an Ihr Unternehmen, durch, allein oder mit einem Dienstleister. Wenn Sie dazu Fragen haben oder eine „Zweit-Meinung“ benötigen, können Sie sich an die Fachverbände wenden. Vielleicht vereinbaren Sie auch ein gegenseitiges Sparring mit einem anderen Unternehmen. Manchmal verändert sich der Blickwinkel auf die eigenen Maßnahmen, wenn man mit einem sachkundigen, interessierten Dritten seines Vertrauens durchs Unternehmen geht.
- Treten Sie der Allianz für Cybersicherheit bei; dort bekommen Sie zügige Informationen und vieles Mehr. Große Unternehmen sollten dem UP KRITIS beitreten.
- Machen Sie mit beim Kompetenzzentrum Digitale Wasserwirtschaft. Nehmen Sie an den (kostenfreien, meist virtuellen) Veranstaltungen und Workshops teil und sprechen Sie uns an, wenn Sie eine Veranstaltung, einen Workshop, einen Erfahrungsaustausch vermissen. Wir sehen, was wir da machen können.
- Organisieren Sie Schulungen für Ihre Mitarbeiter:Innen. Dazu gibt es inzwischen viele Angebote, auch solche, die bei „wenig Zeit“ machbar sind. Wir werden uns umsehen und in der „community“ Informationen dazu zusammenstellen.
- Organisieren Sie sich das „dritte und vierte Auge“, indem Sie ein anderes Unternehmen als „Sparring-Partner“ dazu nehmen oder regionale Erfahrungsaustausche organisieren. Wir, als KDW, unterstützen dabei gerne. Kommen Sie auf uns zu.