Der neue B3S WA – Edition 2023 – ist da

Christian Cichowski (Wuppertal), Daniel Fricke (Bonn), Heiko Jepp (Düsseldorf), Rolf Tenner (Köln)

Zusammenfassung

Der Branchenspezifische Sicherheitsstandard Wasser/Abwasser (B3S WA) – Edition 2023 – liegt vor. Der bestehende Standard wurde auf Basis des BSI IT-Grundschutz-Kompendiums (Edition 2023) grundlegend überarbeitet. Mit den Änderungen im B3S WA Edition 2023 gehen auch die Überarbeitungen der inhaltsgleichen Merkblätter DVGW W 1060 (M) bzw. DWA-M 1060 „IT-Sicherheit – Branchenspezifischer Sicherheitsstandard Wasser/Abwasser“ einher.

Schlagwörter: Wirtschaft, IT-Sicherheit, kritische Infrastruktur, Sicherheitsstandard

DOI: 10.3242/kae2024.02.004

Abstract

The new B3S WA – 2023 edition – is here

The 2023 edition of the B3S WA sector-specific security standard for water/wastewater is now available. The old standard has been fundamentally revised based on the BSI IT-Grundschutz Compendium (2023 edition). Changes to the 2023 edition of the B3S WA are also accompanied by revisions to the identical leaflets DVGW W 1060 (M) and DWA-M 1060 IT security – industry-specific security standard for water/wastewater.

Keywords: Business, IT security, critical infrastructure, security standard

DVGW und DWA stellen neue Version des B3S WA bereit

Gemäß den Vorgaben im BSI-Gesetz[Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)] überprüft das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) alle zwei Jahre, ob der B3S WA (Branchenspezifischer Sicherheitsstandard Wasser/Abwasser) zur Gewährleistung der Anforderungen für die Kritischen Infrastrukturen der Sektoren Trinkwasserversorgung und Abwasserbeseitigung gemäß § 8a Absatz 1 BSIG geeignet ist. Für das inzwischen vierte Update des B3S WA (Edition 2023) läuft zum Zeitpunkt der Erstellung dieses Artikels die Eignungsfeststellung beim BSI. Die Eignungsfeststellung für den aktuell gültigen B3S WA (Version 2021) ist bis zum 22. Januar 2024 befristet.

Mit den Änderungen im B3S WA Edition 2023 gehen auch die Überarbeitungen der inhaltsgleichen Merkblätter DVGW W 1060 (M) bzw. DWA-M 1060 „IT-Sicherheit – Branchenspezifischer Sicherheitsstandard Wasser/Abwasser“ einher.

Sektor	Teilsektor
Energie	Stromversorgung
	Fernwärme und -kälteversorgung
	Kraftstoff- und Heizölversorgung
	Gasversorgung
Transport und Verkehr	Luftverkehr
	Schienenverkehr
	Schifffahrt
	Straßenverkehr
Finanz- und Versicherungswesen	Bankwesen
	Finanzmarktinfrastrukturen
Gesundheit	
Wasser und Abwasser	**Trinkwasserversorgung**
	Abwasserbeseitigung
Informationstechnik und Telekommunikation	
Weltraum	

Tabelle 1: Sektoren mit hoher Kritikalität

Gesetzeslage

Die in der EU beschlossene NIS-2-Richtlinie (NIS: Netzwerk- und Informationssicherheit) muss bis zum 17. Oktober 2024 in deutsches Recht überführt werden. Mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) werden an vielen Stellen Anforderungen erhöht und branchenübergreifend harmonisiert. Bisher wurden im Rahmen der BSI-KritisV [Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung – BSI-KritisV)] Anlagen im Bereich der Trinkwasserversorgung (> 22 Millionen Kubikmeter) bzw. der Abwasserbeseitigung (> 500 000 EW) als Grundlage der Einstufung genutzt. Dies wird nun angepasst und neu geordnet werden. Grundlage dafür ist die Einordnung der Unternehmen in Sektoren mit hoher Kritikalität [1] (Tabelle 1), in der die Trinkwasserversorgung und Abwasserbeseitigung aufgeführt sind. Das zweite Kriterium für die Einordung findet sich dann im zukünftigen § 28 BSIG, die Einteilung in „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“:

- Besonders wichtige Einrichtungen sind Unternehmen aus Anlage 1 (hohe Kritikalität) mit > 250 Beschäftigten oder > 50 Millionen Euro Umsatz.
- Wichtige Einrichtungen sind Unternehmen aus Anlage 1 (hohe Kritikalität) und 2 (sonstige kritische Sektoren) mit > 50 Beschäftigten oder > 10 Millionen Euro Umsatz.

Ebene	Kategorie	Anwendungsfall	Beschreibung	Einstufung
Ebene 1: Organisatorische und technische Verantwortung für IT-Sicherheit				Verpflichtend
	ORS – Organisation			
		ORS1	Verantwortung der Einrichtungsleitung für die IT-Sicherheit	
		ORS2	Zuständigkeiten innerhalb der Einrichtung für die IT-Sicherheit	
	INF – Infrastruktur			
		INF1	Sicherung der Infrastruktur	
	IDR – Angriffserkennung und Reaktion			
		IDR1	Verantwortung der Einrichtungsleitung für die Systeme zur Angriffserkennung	
		IDR2	Zuständigkeiten innerhalb der Einrichtung für die Systeme zur Angriffserkennung	
Ebene 2: IT-Sicherheit der IT-/OT-Infrastruktur				Verpflichtend
	ARC – Architektur der Kommunikationsinfrastruktur			
		ARC1 ARC2 ARC3	Lokales Netzwerk, ausschließlich genutzt zur Überwachung und Steuerung der Betriebsanlage Lokales Netzwerk, gemeinsam mit anderen IT-Systemen genutzt Fernzugriff auf die IT-/OT-Systeme des Anlagenbetriebs	
	ARS – Architektur der Systeminfrastruktur			Verpflichtend
		ARS1 ARS2 ARS3	Server- und Clienteinsatz Virtualisierung von IT-/OT-Komponenten Einsatz von IoT-Komponenten	
	POI – Ordnungsgemäßer Betrieb der Infrastruktur			
		POI1 POI2	Regulärer-IT-/OT-Betrieb IT-/OT-Betrieb teilweise oder vollständig durch Dritte	
Ebene 3: IT-Sicherheit bei der Nutzung der IT-/OT-Infrastruktur				Verpflichtend
	DEX – Datenaustausch			
		DEX1 DEX2	Senden von Daten an externe Systeme Empfangen von Daten von externe Systemen	
	SYA – Systemzugriff			
		SYA1 SYA2	Anlageninterner Zugriff auf die IT-/OT-Systeme des Anlagenbetriebs Fernzugriff auf die IT-/OT-Systeme des Anlagenbetriebs	
	PPM – PLC-Programmierung und Wartung			
		PPM1	Programmierung und Wartung der Automatisierungskomponenten	Verpflichtend

Tabelle 2: Struktur des B3S WA – Edition 2023

Damit wird die bisherige Sicht von Anlagen hin zu Unternehmen (Einrichtungen) verschoben. Die Anzahl der betroffenen Unternehmen steigt durch diesen Ansatz signifikant von ca. 80 Anlagen auf ca. 800 Unternehmen im Bereich des B3S WA.

Eine weitere Neuerung für Unternehmen in den KRITIS-Sektoren ist die Umsetzung der von der EU beschlossenen CER-Richtlinie (CER: Critical Entities Resilience) als KRITIS-Dachgesetz [2] in deutsches Recht. Auch hier liegt derzeit nur ein Referentenentwurf vor, die Umsetzung in den EU-Mitgliedsstaaten hat bis spätestens 17. Oktober 2024 zu erfolgen. Ohne in „vorauseilendem Gehorsam“ dem nicht finalen Referentenentwurf zu folgen, enthält der B3S WA schon jetzt einige Anforderungen in dem Anwendungsfall „INF1 – Sicherung der Infrastruktur“, die auf die Umsetzung des KRITIS-Dachgesetzes einzahlen werden.

Der neue B3S WA – Edition 2023 stellt sich vor

Die wohl auffälligste Änderung im neuen B3S WA sind die neuen Anwendungsfälle. Im Zuge der Überarbeitung hat sich das Gremium für eine komplette Renovierung der Anwendungsfälle, auch in Erwartung der Änderungen, die sich durch NIS2 ergeben, entschieden. In Tabelle 2 wird die Struktur verdeutlicht. Da durch die NIS2 ebenfalls viele neue Nutzer des B3S erwartet werden, wurde die grundlegende Überarbeitung der Struktur in dieser Version vollzogen, um diesen neuen Nutzern den sonst zu erwartenden Umbau in der nächsten Version zu ersparen. Die inhaltlichen Anpassungen sind nicht so umfassend, wie die Änderung der Struktur dies befürchten ließe. Für Nutzer der vorherigen Versionen des B3S WA gibt Tabelle 3 eine grobe Übersicht hinsichtlich der neuen Zuordnung.

Die verschiedenen Bereiche sind in Ebenen voneinander abgegrenzt. Die Kategorien gliedern sich dann weiter in die Anwendungsfälle, die in den Anwendungsfällen (mit Ausnahme von ARS) aufeinander aufbauen. Dadurch konnten diverse Dopplungen entfernt und die Anzahl der Anforderungen auf 200 reduziert werden. Weiterhin werden neben den Anforderungen (früher Maßnahmen) auch die Umsetzungshinweise (sofern verfügbar) angeboten.

Bei der Einstufung der Anwendungsfälle als „Verpflichtend“ sind, neben den Anwendungsfällen aus Ebene 1, vier weitere

Anwendungsfälle obligatorisch umzusetzen. So ist beispielsweise der Anwendungsfall „POI1 – regulärer IT-/OT-Betrieb“ verpflichtend, wohingegen der Anwendungsfall „POI2 – IT-/OT-Betrieb teilweise oder vollständig durch Dritte“ nur im Bedarfsfall hinzugezogen werden muss.

Beispiel einer praktischen Anwendung

In der Trinkwasserversorgung und Abwasserentsorgung ist es üblich, dass die Steuerungssysteme nicht nur vor Ort programmiert und gewartet werden, sondern zum Beispiel auch von einem zentralen Arbeitsplatz (Engineering-Platz).

Dieses typische Beispiel wird im B3S WA durch den verpflichtenden Anwendungsfall PPM1 „Programmierung und Wartung der Automatisierungskomponenten“, aus der Ebene 3 „IT-Sicherheit bei der Nutzung der IT-/OT-Sicherheit”, abgedeckt (Tabelle 2). Der Anwendungsfall PPM1 beschreibt alle Anforderungen (Tabelle 4), die für den Fall der Programmierung und Wartung zu erfüllen sind. Dieses schließt auch einen unmittelbaren Zugang zu der jeweiligen Automatisierungskomponente mit ein, wenn etwa ein Programmiergerät die Schnittstelle einer Speicherprogrammierbaren Steuerung (SPS) nutzt.

Um ein Mindestmaß an IT-Sicherheit zu gewährleisten, müssen Betreiber alle Anforderungen des Typs „A“ umsetzen. Für Betreiber kritischer Infrastrukturen im Sinne der BSI-KritisV gilt verpflichtend zusätzlich die Umsetzung der „K“-Anforderungen.

So ist es mittlerweile unabdingbar, das Netzwerk oder die Netzwerke der ICS-Infrastruktur (ICS: Industrial Control System) zu segmentieren. Hierbei werden unterschiedliche funktionale Bereiche definiert und aus Netzwerksicht getrennt. Die Kommunikation zwischen den jeweiligen Netzwerksegmenten wird dabei durch aktive Netzwerk- und Sicherheitskomponenten auf das für die Funktion der Anlage erforderliche Mindestmaß reduziert. So wird es einem potenziellen Angreifer erschwert, auf alle Segmente und damit komplette Systeme zugreifen zu können. Ein klassisches Beispiel hierfür ist das Trennen des OT-Netzwerks (OT: Operational Technology) von der Büro-IT. Konkrete Hilfestellung bietet in dem Fall auch der zugehörige Umsetzungshinweis IND.2.1.M6. In Abbildung 1 ist die beispielhafte Aufteilung der Netzwerke in Sicherheitszonen für eine kleinere Anlage dargestellt. Die erforderliche Kommunikation zwischen den Sicherheitszonen „OT“ und „IT“ wird hierbei über Firewall-Systeme gesteuert, wobei die OT-Firewall in der Verantwortung des OT-Betriebs liegen sollte. Je nach Kritikalität der Systeme können die Sicherheitszonen noch in weitere Teilzonen aufgeteilt werden.

Anwendungsfall Edition 2023	Anwendungsfälle Edition 2021/2021.2
ORS1	OM1 (teilweise)
ORS2	OM1 (teilweise)
IDR1	ID1 (teilweise)
IDR2	ID1 (teilweise)
INF1	nahezu unverändert
ARC1	AR1
ARC2	AR3
ARC3	AR2, AR6
ARS1	AR4
ARS2	AR7
ARS3	AR8
POI1	(teilweise) NM1, NM2, NM3
POI2	(teilweise) NM1, NM2, NM3
DEX1	PA1, PA2, zum Teil PA5, PA6
DEX2	PA3, PA5, PA6
SYA1	UA1, UA2
SYA2	UA3, UA4, UA5
PPM1	PLC1, PLC2, PLC3

Tabelle 3: Umsetzung Anwendungsfälle in neue Struktur

Anforderungs-ID	Bezeichnung	Umsetzungshinweis-ID	Typ
IND.1.A3	Schutz vor Schadprogrammen	IND.1.M3	A
IND.1.A9	Restriktiver Einsatz von Wechseldatenträgern und mobilen Endgeräten in ICS-Umgebungen	IND.1.M9	K
IND.2.1.A1	Einschränkung des Zugriffs auf Konfigurations- und Wartungsschnittstellen	IND.2.1.M1	K
IND.2.1.A11	Wartung der ICS-Komponenten	IND.2.1.M11	A
IND.2.1.A6	Netzsegmentierung	IND.2.1.M6	A
ORP.1.A3	Beaufsichtigung oder Begleitung von Fremdpersonen	nicht vorhanden	A
SYS.2.1.A1	Sichere Authentisierung von Benutzenden	nicht vorhanden	A
SYS.3.1.A14	Geeignete Aufbewahrung von Laptops	SYS.3.1.M14	K
SYS.3.1.A8	Sicherer Anschluss von Laptops an Datennetze	nicht vorhanden	K

Tabelle 4: Anforderungen und Umsetzungshinweise aus dem Anwendungsfall PPM1

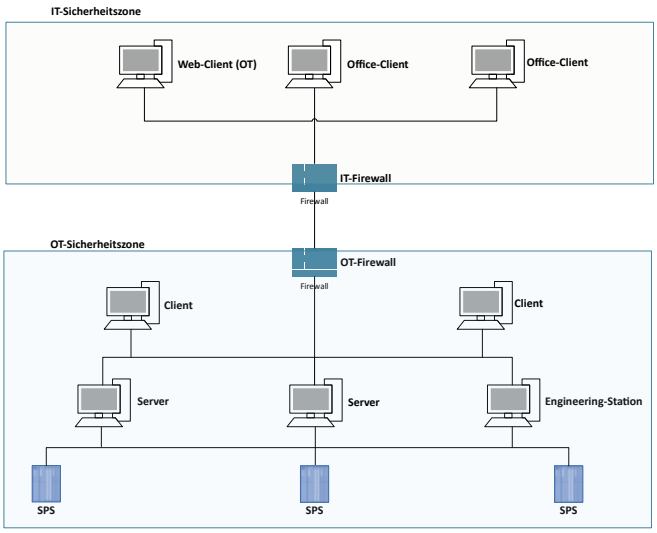

Abb. 1: Beispielhafte Segmentierung IT/OT

Hierbei ist zu beachten, dass eine direkte Kommunikation nur zwischen aneinander angrenzenden Zonen zulässig ist.

Blick in die Zukunft des B3S WA

Die Cybersicherheitslage wird für alle Betreiber zunehmend bedrohlicher. Daher ist zur Aufrechterhaltung der Informationssicherheit die Nutzung eines etablierten Sicherheitsstandards für kleine wie für große Betreiber sinnvoll. Diesen Anspruch will der B3S WA erfüllen und wird daher regelmäßig dem Stand der Technik angepasst. Er bietet den Betreibern in der Wasserwirtschaft nicht nur eine solide Basis für den Einstieg, sondern auch eine verlässliche Grundlage für den Ausbau eines eigenen ISMS (Informationssicherheitsmanagementsystem). Bei der Weiterentwicklung des B3S WA werden auch wie bisher die Verbesserungsvorschläge der KRITIS und Sub-KRITIS Betreiber berücksichtigt und mit den gesetzlichen Anforderungen abgeglichen.

Die Sicherheitsanforderungen aus dem KRITIS-Dachgesetz – soweit bereits bekannt – wurden in dem aktuellen B3S WA 2023 berücksichtigt. Mit dem im Oktober 2024 in Kraft tretenden NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) steht die nächste Entwicklungsstufe des B3S zur Eignungsfeststellung durch das BSI an. Die Grundsteine und die Systematik für eine transparente Integration der zu erwartenden NIS2UmsuCG-Anforderungen wurden in der Version 2023 durch das neue Schichtenmodell berücksichtigt.

Weiterhin wird auf Wunsch vieler Betreiber mithilfe der „Zuordnungs ISO zum IT-Grundschutz“ [3] des BSI auch eine Verlinkung zu den ISO/IEC 2700x Controls eingebaut. Damit haben die Betreiber einen qualitätsgesicherten Überblick, welche Controls bereits im Zuge der B3S WA-Umsetzung auch tatsächlich schon erledigt wurden.

Fazit

Die (wiederholte) Anerkennung des B3S WA durch das BSI ist ein großer Erfolg für die technische Selbstverwaltung der Branche. Dies zeigt, dass auch ohne einschlägige Regulierung mit einem pragmatischen Ansatz die gesetzlichen Anforderungen erfüllt werden können. Des Weiteren wird durch den zweistufigen Ansatz (A- und K-Anforderungen) die Hürde so niedrig gelegt, dass auch bisher noch nicht von der BSI-KritisV erfassten Betreibern ein einfacher und zielführender Einstieg in die Informationssicherheit für den OT-Bereich gelingt.

Der B3S WA als Grundlage für die Nachweisführung nach § 8a BSIG hat sich in den letzten Jahren bewährt. Der enge Austausch von Betreibern, Verbänden und BSI hat zu einem guten gegenseitigen Verständnis und deutlichen Verbesserungen der Prozesse rund um die Nachweisführung geführt.

Literatur

[1] Diskussionspapier des Bundesministeriums des Innern und für Heimat: Wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland (Stand: 27.09.2023), *https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-UmsetzungWirtschaft_DisP.pdf?__blob=publicationFile&v=2*

[2] Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen, *https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html*

[3] Zuordnungstabelle ISO zum IT-Grundschutz, *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Zuordnung_ISO_und_IT_Grundschutz_Edit_6.html?nn=128568*

Autoren

Christian Cichowski
Wupperverband
Untere Lichtenplatzer Straße 100, 42289 Wuppertal

Daniel Fricke
DVGW Service & Consult GmbH
Josef-Wirmer-Straße 1–3, 53123 Bonn

Dipl.-Ing. Heiko Jepp
Stadtwerke Düsseldorf AG
Höherweg 100, 40233 Düsseldorf

Dipl.-Ing. (FH) Rolf Tenner
Stadtentwässerungsbetriebe Köln, AöR
Ostmerheimer Straße 555, 51109 Köln