Hinweise und Empfehlungen

für die Nachweise der anstehenden nächsten Nachweisrunde der KRITIS-Betreiber gemäß § 8 a Abs. 3 BSI-Gesetz

Quelle: kynny/iStock.com

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zieht nach dem Abschluss der ersten Nachweisrunde gemäß dem BSI-Gesetz ein positives Fazit. Mit Hinblick auf die noch in diesem Jahr anstehende nächste Nachweisrunde möchte es den Betreibern Kritischer Infrastrukturen (KRITIS-Betreiber) in dem Beitrag Hinweise und Empfehlungen geben, mit denen sich der Nachweisprozess in Zukunft noch reibungsloser gestalten lässt. Zentraler Bestandteil des Textes ist u. a. die Festlegung des Geltungsbereiches, die am Beispiel einer (fiktiven) Kläranlage nachvollzogen wird.

von: Christine Hofer & Frank Peterhänsel (beide: Bundesamt für Sicherheit in der Informationstechnik)

In diesem Jahr stehen die nächsten Audits für die nachweispflichtigen Betreiber des Sektors Wasser/Abwasser an. Das Bundesamt für Sicherheit in der Informationstechnik hat die Erfahrungen aus den ersten Nachweisen bereits auf verschiedenen Veranstaltungen vorgestellt. In diesem Zusammenhang haben Betreiber und Prüfer sehr oft den Wunsch geäußert, dass das BSI für die kommenden Nachweise 2020 verstärkt operative Hinweise geben möge, um den gesamten Nachweisprozess für alle Beteiligten reibungsloser zu gestalten. Das BSI greift diesen Wunsch gerne auf und möchte an dieser Stelle die Anforderungen an die Nachweise und eingereichten Unterlagen konkretisieren. Die nachfolgenden Ausführungen sollen den beteiligten Akteuren als Hilfestellung bei der Nachweiserbringung dienen.

Prüfvorbereitung

Zahlreiche Betreiber haben gegenüber dem BSI geäußert, dass in der Phase der Vorbereitung auf eine Prüfung zur Erfüllung der Anforderungen gem. § 8 a (3) BSIG häufig Klärungsbedarf mit den prüfenden Stellen bestand. So wiesen z. B. die vertraglichen Vereinbarungen mit den prüfenden Stellen Spielraum für Interpretationen hinsichtlich der mit dem Audit verbundenen Aufgaben auf. Daraus resultierte des Öfteren eine verspätete Einreichung der Nachweise. Es ist aus Sicht des BSI daher unbedingt ratsam, den Aufgabenumfang mit dem Ziel, die Umsetzung des § 8 a (1) BSIG zu auditieren, exakt vertraglich zu beschreiben.

Ein wichtiger Punkt für das BSI bei der Nachweisprüfung stellen zudem die ethischen Grundsätze dar. So verstößt z. B. ein Audit durch nur eine Person nach Ansicht des BSI gegen diese Grundsätze und kann zu Nacharbeiten und letztlich auch zu Mehraufwänden für die Betreiber führen.

Regelmäßigen Anlass zu Nachforderungen beim Betreiber geben die fehlenden Nachweise über die „zusätzliche Prüfverfahrenskompetenz“ der Prüfstellen. Hier gilt es zu beachten, dass diese „zusätzliche Prüfverfahrenskompetenz“ sowohl für einen Mitarbeiter der prüfenden Stelle als auch für einen der Prüfer nachzuweisen ist. Als Nachweis gilt beispielsweise die Bescheinigung über die Teilnahme an einer entsprechenden Schulung oder aber eine Selbsterklärung, in der das Vorhandensein der vom BSI geforderten Kenntnisse und Fähigkeiten versichert wird. Hierfür können die vom BSI zum Download bereitgestellten Formulare verwendet werden.

Weitere Rückmeldungen betrafen die Festlegung des Geltungsbereiches. Aus Sicht des BSI ist der Geltungsbereich dann nachvollziehbar, wenn erkennbar ist, dass er sich auf die registrierten Anlagen bezieht. Hier gilt: Die im Nachweis genannten Anlagen müssen identisch sein mit den registrierten. Ein besonderes Augenmerk sollte dabei auf den Namen der Anlage und ihren Standort gelegt werden. Der Geltungsbereich muss neben einer textuellen Beschreibung auch in Form einer grafischen Übersicht eingereicht werden. Zu beachten ist dabei insbesondere, dass daraus die für die kritische Dienstleistung relevanten Anlagen und ihre IT-Struktur (Netzplan) hervorgehen muss. Unter Netzplan ist dabei natürlich nicht ein Rohrleitungsplan o. Ä. zu verstehen, sondern eine Übersicht über die IT-Systeme und ihre Vernetzung. Auch Schnittstellen zu externen Systemen oder Dienstleistern müssen daraus erkennbar sein. Das BSI hat in diesem Zusammenhang in der Vergangenheit häufig Legenden zur grafischen Darstellung nachgefordert. Betreiber müssen dabei beachten, dass betriebsinterne Abkürzungen sowie farbliche und grafische Ausgestaltungen aus sich selbst heraus nicht eindeutig im Rahmen der Prüfung durch das BSI interpretiert werden können.

Quelle: BSI

Abb. 1: *Schritte zur Nachweiserbringung*

Die grafische Darstellung des Geltungsbereiches muss hierbei keine technischen Details wie IP-Adressen oder Hostnamen enthalten. Sowohl diese Darstellung als auch die textliche Beschreibung sollte umfassend und verständlich sein; so ist beispielsweise auf betriebsinternes Vokabular zu verzichten bzw. dieses zu definieren.

Die Qual der Wahl: Das Festlegen einer Prüfgrundlage

Zwar ist die Wahl der Prüfgrundlage grundsätzlich frei – diese muss jedoch geeignet sein, die Anforderungen im Sinne des § 8 a (1) BSIG zu erfüllen. Der Nachweis darüber obliegt dem Betreiber bzw. der prüfenden Stelle. Die meisten Betreiber im Sektor Wasser wählen als Prüfgrundlage den IT-Sicherheitsstandard Wasser/Abwasser (B3S) oder eine ISO-Zertifizierung (ISO 27001/2). Zu beachten ist, dass bei einem Audit nach ISO aufgrund der Systematik mit ggf. längeren Vorlaufzeiten zu rechnen ist. Dies ist insbesondere dann der Fall, wenn während eines Stage-1-Audits potenzielle Hauptabweichungen oder diverse Nebenabweichungen gefunden werden, da das Stage-2-Audit in der Regel erst nach Beseitigung der Abweichungen erfolgt. Diese mögliche Verzögerung wird im Rahmen der zeitlichen Planung des Audits häufig nicht berücksichtigt.

FESTLEGUNG DES GELTUNGSBEREICHES AM BEISPIEL EINER (FIKTIVEN) KLÄRANLAGE

Verfahrenstechnische Abgrenzung

Laut dem BSI-Gesetz (BSIG) sind grundsätzlich nur die IT-Systeme relevant, die zur Erbringung der kritischen Dienstleistung erforderlich sind. Um diese zu identifizieren, ist in einem ersten Schritt festzustellen und entsprechend zu beschreiben, welche der vorhandenen Anlagenkomponenten zur deren Erbringung erforderlich sind und eingesetzt werden. Bei einer dreistufigen Kläranlage wären z. B. folgende Anlagenteile als relevant aufzuführen:

- Zulauf,
- Rechen,
- Sandfang,
- Vorklärung,
- Belebung,
- Nachklärung und
- Ablauf.

Damit ist der verfahrenstechnische Geltungsbereich zunächst ausreichend definiert. Dass z. B. die Schlammbehandlung nicht aufgeführt ist, ist darin begründet, dass diese an sich nicht für die Reinigung des Abwassers – sprich: die Erbringung der kritischen Dienstleistung – erforderlich ist.

IT-technische Bewertung und Abgrenzung

Zum Betrieb der genannten verfahrenstechnischen Anlagenkomponenten werden typischerweise Aktoren, Sensoren und Automatisierungskomponenten (z. B. SPSen) eingesetzt, die tatsächlich den Betrieb der Anlagenkomponenten überwachen und deren Steuerung übernehmen. Diese IT-Komponenten und -Systeme sind zudem typischerweise miteinander vernetzt, sei es über (Kabel-) Leitungen oder über Funkverbindungen. Zudem findet man in der Regel eine der Automatisierungsebene übergeordnete IT-Instanz, z. B. ein Prozessleitsystem, welches auf komfortable Weise Eingriffe in das Betriebsgeschehen erlaubt. Alle diese IT-Systeme zählen ohne Ausnahme zum unmittelbaren Geltungsbereich für die Kritische Infrastruktur.

In der Praxis findet sich jedoch häufig die Situation, dass auch von anderen IT-Systemen auf die zum unmittelbaren Geltungsbereich zählenden IT-Systeme zugegriffen werden kann, etwa für Wartungszwecke. Denkbar ist auch, dass dasselbe Prozessleitsystem, welches die Kläranlage steuert, auch für die Steuerung der Schlammbehandlung eingesetzt wird. Grundsätzlich bleibt es dem Betreiber überlassen, zu entscheiden, ob er in diesen Fällen den Geltungsbereich ausweitet. Dies hat die Konsequenz, dass für den erweiterten Geltungsbereich ebenfalls die Anforderungen des BSIG erfüllt und nachgewiesen werden müssen. Alternativ kann der Betreiber auch entsprechende Abgrenzungsmechanismen (wie Firewalls etc.) nachweisen, die die geforderte IT-sicherheitstechnische Trennung sicherstellen. Hier ist in jedem Fall eine individuelle und situationsspezifische Bewertung durchzuführen. Auch diese ist entsprechend zu dokumentieren.

Festlegung des eigentlichen Geltungsbereichs

Folgende Empfehlung hat sich bewährt: Solange es definierte und technisch eindeutig zu identifizierende Schnittstellen zu anderen IT-Systemen gibt, ist eine Beschränkung auf den unmittelbaren Geltungsbereich sinnvoll und machbar. In Fällen, in denen etwa ein einziges Prozessleitsystem weitere Anlagenteile außerhalb des eigentlichen Geltungsbereiches des

Eine zusätzliche Hilfestellung finden Betreiber in der Empfehlung für Verbundunternehmen und den Hinweisen zur Nutzung eines bestehenden ISO-27001-Zertifikates als Bestandteil eines Nachweises gemäß § 8a (3) BSIG.

Die eigentliche Prüfdurchführung

Für die Durchführung der Prüfung selbst kann das BSI aus der Erfahrung der bisher geprüften Nachweise einen stetig wiederkehrenden Anlass für Nachforderungen bei Betreibern benennen: Stichproben. Es sind in diesem Zusammenhang alle registrierten Anlagen im Geltungsbereich vor Ort zu prüfen! Stichproben bei der Anlagenauswahl und eine reine Dokumentenprüfung sind nicht ausreichend.

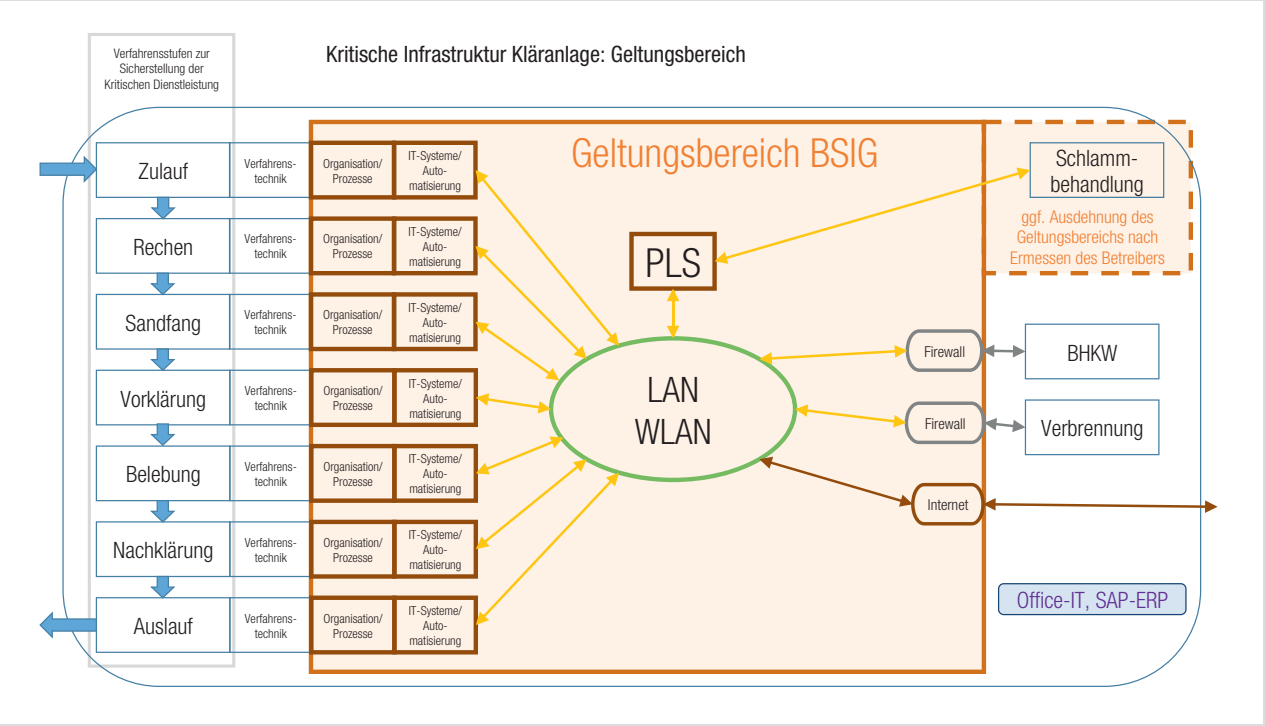
Innerhalb einer Anlage kann die Prüfthemenauswahl stichprobenartig erfolgen. Hierbei müssen mindestens alle kritischen Prozesse umfasst sein. Die Stichprobenauswahl soll risikoorientiert anhand von Eintrittswahrscheinlichkeiten und den potenziellen Folgen eines Ausfalls der kritischen Dienstleistung für die betroffene Bevölkerung erfolgen. Die Stichprobenauswahl ist dem BSI gegenüber zu begründen

Festgestellte Mängel und Restrisikobetrachtung

Das Prüfergebnis mit den festgestellten und bewerteten Mängeln bildet die Grundlage, um die Resilienz der beim Betreiber eingesetzten IT-Infrastruktur zu beurteilen. Der Betreiber erhält hierdurch eine Orientierung, wie in seinen Kritischen Infrastrukturen die IT-Sicherheit weiter erhöht werden kann und welchen Risiken noch zu begegnen ist. Dementsprechend legt das BSI besonderen Wert auf die Feststellung, Bewertung und Beseitigung der Mängel und der damit einhergehenden potenziellen Beeinträchtigung der kritischen Dienstleistung. Dafür müssen alle diejenigen Mängel aufgelistet und bewertet werden, die ein entsprechendes Risiko darstellen. Im gleichen Zusammenhang sollen den festgelegten Mängeln die ergriffenen Maßnahmen gegenübergestellt werden, um dem Risiko – in Bezug auf die Erbringung der kritischen Dienstleistung – zu begegnen.

Betreiber sollten zur Dokumentation die Empfehlung des BSI zum Aufbau einer Mängelliste verwenden. So kann sichergestellt werden, dass alle formalen Anforderungen eingehalten werden.

Besonders zu begründen ist der Umgang mit Mängeln, mit deren Behebung nicht umgehend begonnen werden kann. Einfache Hinweise, dass mit der Beseitigung „alsbald begon-



BSIG steuert oder überwacht – in diesem Beispiel etwa die Schlammbehandlung –, wird die technische Abgrenzung, wenn überhaupt möglich, zu erheblichen Mehraufwänden führen.

In jedem Fall sind sämtliche IT-Komponenten, auch des erweiterten Geltungsbereiches, entsprechend zu identifizieren und für diese die erforderlichen Nachweise zu erbringen.

Dr. Ludger Terhart
EMSCHERGENOSSENSCHAFT/
LIPPEVERBAND

nen wird“, oder „wird beim nächsten Wirtschaftsplan berücksichtigt“, reichen nicht aus. Zudem sollten Mängel aus der 1. Nachweisrunde nach Möglichkeit behoben sein.

Betreiber, Prüfer und das BSI haben wertvolle Erfahrungen bei der Begleitung von Umsetzungsmaßnahmen zur Mängelbeseitigung gesammelt. IT-Sicherheit ist ein lebendiger Prozess, der nicht nur zur Nachweiserbringung in den Fokus rücken sollte. Es ist daher aus Sicht des BSI zu erwarten, dass erkennbar ein PDCA-Zyklus etabliert, gelebt und weiterentwickelt wird.

Eine ausschließlich kaufmännische Betrachtung der Risiken hinsichtlich Eintrittswahrscheinlichkeit und Schadenshöhe ist nicht ausreichend. Es muss zwingend auf die Auswirkungen der betroffenen Bevölkerung bei einer Störung oder Ausfall der kritischen Dienstleistung eingegangen werden. Dies

BRANCHENSPEZIFISCHER SICHERHEITSSTANDARD WASSER/ABWASSER, VERSION 2 (B3S WA V2)

Im Februar dieses Jahres hat das BSI die Eignungsfeststellung für die Version 2 des „Branchenspezifischen Sicherheitsstandard Wasser/Abwasser“ erteilt und damit bestätigt, dass auch der B3S WA V2 den Mindestanforderungen für die Erfüllung der gesetzlichen Vorgaben nach § 8 a Abs. 1 BSI-Gesetz für den KRITIS-Sektor Wasser entspricht. Die Struktur der ersten Version des B3S WA (auf Basis der IT-Sicherheitskataloge) wurde bei der zweiten Version beibehalten. In der Version 2 finden sich folgende Änderungen und Ergänzungen:

- Es wurden zusätzlich Hinweise auf das IT-Grundschutz-Kompendium aufgenommen und die Maßnahmen der ersten Version im Hinblick auf die derzeitige Gefährdungslage für die Wasserwirtschaft bewertet und aktualisiert.
- Die Anforderungen und die zugehörigen Umsetzungshinweise aus dem IT-Grundschutz-Kompendium, die in den IT-Grundschutzkatalogen noch nicht enthalten waren, wurden ergänzt.
- Die Maßnahmen aus der Schicht „IND“ wurden geprüft und bei Relevanz übernommen.
- Es wurde ein weiterer Anwendungsfall definiert, um die Anforderungen des Objektschutzes an die IT-Infrastruktur zu berücksichtigen und Maßnahmen zum Schutz der Infrastruktur zu integrieren.
- Das Thema „Restrisikobewertung“ wurde aufgenommen, da es als sinnvoll angesehen wird, das Restrisiko, das nach Durchführung der Mindestmaßnahmen zum Erreichen des Stands der Technik verbleibt, auszuweisen.

Die Veröffentlichung des Updates des IT-Sicherheitsleitfadens auf den B3S WA V2 ist für Anfang März geplant.

Kirsten Wagner
DVGW-Hauptgeschäftsstelle | Wasserversorgung

stellt dann die Messgröße dar, um Maßnahmen bezüglich Wirtschaftlichkeit und Zielerreichungsgrad zu beurteilen. Risiken im Geltungsbereich des § 8 a (1) BSIG können nicht akzeptiert werden, solange wirtschaftlich zumutbare und nach dem Stand der Technik umsetzbare Maßnahmen zur Reduktion des Risikos möglich sind. Restrisiken können nach entsprechender Würdigung und Einordnung durch Prüfer und Betreiber außerhalb des Geltungsbereiches akzeptiert werden.

Die Einreichung der Nachweisformulare

Bei der Bearbeitung der Nachweisformulare kann das BSI einige Hinweise geben, welche die Zahl an Rückfragen reduziert und den Gesamtprozess der Nachweiserfüllung vereinfacht. So sollten Betreiber die BSI-Formulare (Formblätter) für die Nachweiserbringung verwenden. Dies erleichtert den Abgleich mit den entsprechenden Vorgaben und hilft dabei, Rückfragen zu minimieren. Darüber hinaus sind die Formblätter vollständig auszufüllen. Das Formblatt KI ist durch den Betreiber, alle anderen durch die prüfende Stelle zu unterschreiben.

Fazit und Ausblick

Basierend aus den Erfahrungen mit der ersten Nachweisrunde zieht das BSI ein positives Fazit. Auf Basis der vorliegenden Nachweise ist eine Tendenz zu qualitativ verständlicheren Nachweisen erkennbar. Anfängliche Unsicherheiten bei prüfenden Stellen, Rückfragen und Anmerkungen seitens der Betreiber fließen in FAQs ein, die das BSI zur Verfügung stellt.

Das BSI möchte mit den Betreibern im Austausch bleiben und gemeinsam mit diesen sowie den angeschlossenen Verbänden an Hinweisen und Hilfestellungen für einen gelungenen Nachweisprozess arbeiten! ■

Weiterführende Weblinks

Orientierungshilfe zu Nachweisen: www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Nachweise/Orientierungshilfe/Orientierungshilfe_node.html

Selbsterklärung prüfende Stelle: www.bsi.bund.de/dok/13491490

Selbsterklärung prüfende Person: www.bsi.bund.de/dok/13491522

Nutzung des branchenspezifischen Sicherheitsstandards in Verbundunternehmen: www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Kritis/B3S_WA_Analyse_Empfehlungen_pdf.html

FAQ BSI ISO: www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_8aBSIG_ISO27001/faq_bsi_8a_ISO27001_node.html;

www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Maengelliste_PEA_Final.html

Die Autoren

Christine Hofer ist Leiterin des Referats WG 12 „KRITIS-Sektoren Energie und Wasser sowie kerntechnische Anlagen“ beim Bundesamt für Sicherheit in der Informationstechnik in Bonn.

Frank Peterhänsel ist Referent im Referat WG 12 „KRITIS-Sektoren Energie und Wasser sowie kerntechnische Anlagen“ beim Bundesamt für Sicherheit in der Informationstechnik in Bonn.

Kontakt:
Christine Hofer
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185–189
53175 Bonn
Tel.: 0228 999582-5776
E-Mail: christine.hofer@bsi.bund.de
Internet: www.bsi.bund.de

Die neue VOB 2019

Geht es in Deutschland um die Bauvergabe, ist die VOB das einschlägige Grundlagenwerk. Die neue VOB Gesamtausgabe 2019 ist im Oktober erschienen.

Änderungen in Teil A

In Teil A liegt der Schwerpunkt im Unterschwellenbereich. Bereits im Zuge der Vergaberechtsreform 2016 wurden einige wesentliche Änderungen vorgenommen, um den erwünschten inhaltlichen Gleichlauf zwischen den verschiedenen Abschnitten der VOB/A herzustellen beziehungsweise zu wahren.

Änderungen in Teil C

In VOB Teil C wurden insgesamt 14 ATV fachtechnisch überarbeitet, bei drei ATV wurde der Titel geändert. 40 ATV wurden redaktionell überarbeitet und an den neuesten Stand der Technik und der Normung angepasst.

VOB Gesamtausgabe 2019

Vergabe- und Vertragsordnung für Bauleistungen – Teil A (DIN 1960), Teil B (DIN 1961), Teil C (ATV)

Hrsg.: DIN, DVA (Beuth Verlag)
Ausgabe 10/2019
1.146 Seiten, DIN A5, gebunden (Leinen)
Art.-Nr.: 310711, Preis: 54,00 €*

VOB Zusatzband 2019

„Kleine" VOB

Der VOB Zusatzband 2019 enthält traditionell Originalauszüge aus der VOB Teil A (DIN 1960) und VOB Teil B (DIN 1961). Zusätzlich stellt die Ausgabe 2019 die folgenden Dokumente in der jeweils neuesten Fassung bereit:

- Gesetz gegen Wettbewerbsbeschränkungen (GWB Teil 4)
- Vergabeverordnung (VgV)
- Vergabeverordnung Verteidigung und Sicherheit (VSVgV)
- Sektorenverordnung (SektVO)
- Konzessionsvergabeverordnung (KonzVgV)
- Vergabestatistikverordnung (Verg StatVO)
- Vergabe- und Vertragsordnung für Leistungen (VOL/A, 1. Abschnitt)
- Vergabe- und Vertragsordnung für Leistungen (VOL/B)

Neu 2019:
Unterschwellenvergabeverordnung (UVgO)

VOB Zusatzband 2019

Vergabe- und Vertragsordnung für Bauleistungen

Hrsg.: DIN (Beuth Verlag)
Ausgabe 10/2019
530 Seiten, DIN A5, broschiert
Art.-Nr.: 310712
Preis: 24,80 €*

*Alle Preise zzgl. Versandkosten

Kompetenz: Energie & Wasser. | wvgw

wvgw Wirtschafts- und Verlagsgesellschaft Gas und Wasser mbH · Josef-Wirmer-Straße 3 · 53123 Bonn
Telefon: 0228-9191-40 · Fax: 0228-9191-499 · E-Mail: info@wvgw.de · shop.wvgw.de