www.dwa.de

DWA
Klare Konzepte. Saubere Umwelt.

DWA-Handbuch

IT-Sicherheitsleitfaden des Branchenstandards Wasser/Abwasser

August 2017

DVGW

Die Deutsche Vereinigung für Wasserwirtschaft, Abwasser und Abfall e. V. (DWA) setzt sich intensiv für die Entwicklung einer sicheren und nachhaltigen Wasser- und Abfallwirtschaft ein. Als politisch und wirtschaftlich unabhängige Organisation arbeitet sie fachlich auf den Gebieten Wasserwirtschaft, Abwasser, Abfall und Bodenschutz.

In Europa ist die DWA die mitgliederstärkste Vereinigung auf diesem Gebiet und nimmt durch ihre fachliche Kompetenz bezüglich Regelsetzung, Bildung und Information sowohl der Fachleute als auch der Öffentlichkeit eine besondere Stellung ein. Die rund 14 000 Mitglieder repräsentieren die Fachleute und Führungskräfte aus Kommunen, Hochschulen, Ingenieurbüros, Behörden und Unternehmen.

Impressum

Herausgeber und Vertrieb:
DWA Deutsche Vereinigung für
Wasserwirtschaft, Abwasser und Abfall e. V.
Theodor-Heuss-Allee 17
53773 Hennef, Deutschland
Tel.: +49 2242 872-333
Fax: +49 2242 872-100
E-Mail: info@dwa.de
Internet: www.dwa.de

Satz:
Christiane Krieg, DWA

Inhalt

1 Der IT-Sicherheitsleitfaden

1.1 Grundlagen

Der Branchenspezifische Sicherheitsstandard (kurz: B3S) Wasser/Abwasser stellt den Betreibern Kritischer Infrastrukturen im Sinne der BSI-Kritisverordnung im Sektor Wasser ein Regelwerk zur Verfügung, mit dessen Hilfe Sie die im BSI-Gesetz genannten Anforderungen an die betrieblich relevanten IT-Systeme umsetzen und den geforderten Nachweis, den Stand der Technik erreicht zu haben, führen können.

Den grundsätzlichen Rahmen gibt dabei das Merkblatt „IT-Sicherheit – Branchenstandard Wasser/Abwasser“ DVGW W 1060 (M) bzw. Merkblatt DWA-M 1060 vor. Die Merkblätter sind inhaltsgleich. Der IT-Sicherheitsleitfaden stellt die konkrete Ausprägung der von den Betreibern Kritischer Infrastrukturen durchzuführenden Maßnahmen zur Erreichung eines dem Stand der Technik entsprechenden Zustands, der für den Betrieb der Infrastrukturen eingesetzten IT-Systeme, dar (siehe auch Anhang 4.1 „Struktur der Dokumente des branchenspezifischen Sicherheitsstandards“).

Mit den IT-Grundschutz-Katalogen des BSI (im Folgenden kurz „BSI-Grundschutz“ genannt) steht ein anerkannter und bewährter Standard für die Sicherheit von IT-Infrastrukturen zur Verfügung. Der BSI-Grundschutz stellt eine Implementierung insbesondere der Norm ISO/IEC 27001 dar. Im Gegensatz zur Norm werden allerdings nicht nur die allgemeinen Anforderungen an ein Informationssicherheitsmanagement beschrieben, sondern ganz konkret ein Maßnahmenkatalog zur Verfügung gestellt, aus dem ersichtlich ist, bei welcher Gefährdung welche dieser Maßnahmen sinnvoll umgesetzt werden sollten.

Der IT-Sicherheitsleitfaden basiert vollständig auf dem BSI-Grundschutz unter Hinzuziehung des ICS-Security-Kompendiums des BSI[1]. Es werden die für die Anlagen der Branche relevanten Gefährdungen und die entsprechenden Maßnahmen aus dem BSI-Grundschutz referenziert. Die Liste der Gefährdungen wie auch die Auswahl der entsprechenden Maßnahmen wurden durch Fachleute aus den Bereichen Trinkwasserversorgung und Abwasserentsorgung gemeinsam erarbeitet. Diese Auswahl stellt somit den branchenspezifischen Ausschnitt aus dem BSI-Grundschutz dar.

Der IT-Sicherheitsleitfaden gibt die Gefährdungen und Maßnahmen nicht abschließend wieder, sondern stellt die „Best Practices“ für den Sektor Wasser dar. Aufgrund der Tatsache, dass er sich ausschließlich des BSI-Grundschutzes bedient, steht den Betreibern jederzeit die Möglichkeit offen, in der konkret gegebenen Situation abweichend vom IT-Sicherheitsleitfaden zum Beispiel ergänzende Maßnahmen aus dem BSI-Grundschutz aufzunehmen oder Maßnahmen durch andere, besser geeignete zu ersetzen.

1.2 Struktur

Der IT-Sicherheitsleitfaden geht in Anlehnung an die von der AWWA beschriebene Vorgehensweise[2], von sogenannten „Anwendungsfällen“ aus. Diese Anwendungsfälle beschreiben grundsätzliche Infrastrukturkonfigurationen der IT-Systeme zum Betrieb der Anlagen, organisatorische Gegebenheiten sowie grundlegende Prozesse im betrieblichen Alltag, wie etwa Wartung und Nutzung der IT-Systeme. Ausgehend von den Anwendungsfällen werden die damit verbundenen Gefährdungen identifiziert und die nach BSI-Grundschutz empfohlenen Maßnahmen benannt, soweit für die Anlagen zur Trinkwasserversorgung und Abwasserentsorgung angemessen.

1) Download unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security_kompendium_pdf.pdf?__blob=publicationFile&v=2

2) Process Control System Security Guidance for the Water Sector, American Water Works Association (Hrsg.), Washington DC, 2014.

Der BSI-Grundschutz gliedert sich grundsätzlich in „Bausteine“, in denen die unterschiedlichen Aspekte der Informationssicherheit thematisch gebündelt werden, wie etwa Infrastruktur, IT-Systeme, Anwendungen. Innerhalb eines Bausteins werden die typischen Gefährdungen benannt und diesen geeignete Maßnahmen zugeordnet. Das Grundschema sieht damit wie folgt aus:

BSI-Grundschutz: Bausteine → Gefährdungen → Maßnahmen.

Im IT-Sicherheitsleitfaden wird die Ebene der Bausteine nicht explizit angesprochen. Vielmehr erfolgt die Zuordnung der Gefährdungen und zugehörigen Maßnahmen auf der Ebene der Anwendungsfälle. Damit stellt sich das Grundschema im IT-Sicherheitsleitfaden wie folgt dar:

IT-Sicherheitsleitfaden: Anwendungsfälle → Gefährdungen → Maßnahmen.

Dabei können einem Anwendungsfall durchaus Gefährdungen und entsprechende Maßnahmen aus verschiedenen Bausteinen zugeordnet sein. Der IT-Sicherheitsleitfaden ist intern allerdings so aufgebaut, dass die Zuordnung der Gefährdungen zu den Anwendungsfällen stets über die Bausteinzuordnung erfolgt. Die Bausteinreferenzschicht wird vor dem Anwender insofern verborgen, als er keine Bausteinauswahl treffen muss. Somit sieht die implementierte, vollständige Struktur wie folgt aus:

IT-Sicherheitsleitfaden (intern): Anwendungsfälle → Bausteine → Gefährdungen → Maßnahmen.

Die Zuordnungsketten Bausteine → Gefährdungen → Maßnahmen entsprechen dabei ausnahmslos nur solchen Kombinationen, die in den Kreuzreferenztabellen des BSI-Grundschutzes[3] enthalten sind. Auch die Einstufung in Maßnahmen, die in jedem Fall umgesetzt werden sollten und solche, die bei Kritischen Infrastrukturen zusätzlich umzusetzen sind, ist den Kreuzreferenztabellen entnommen („Siegel(stufe)“, „Qualifizierungsstufe“). Auf diese Weise wird sichergestellt, dass der IT-Sicherheitsleitfaden konsistent mit dem BSI-Grundschutz bleibt. Den Bausteinen wurde für die Zwecke des IT-Sicherheitsleitfadens und im Vorgriff auf die Modernisierung des BSI-Grundschutzes ein weiteres Attribut mitgegeben, welches kennzeichnet, ob sich der Baustein auf technische oder aber auf Managementaspekte bezieht. Diese Aufteilung soll helfen, bei den Gefährdungen und Maßnahmen mögliche Zuständigkeiten im Unternehmen/in der Organisation schnell zuordnen zu können.

Der IT-Sicherheitsleitfaden basiert auf dem aktuellen Stand des BSI-Grundschutzes. Neben den Kreuzreferenztabellen werden die Baustein-, Gefährdungs- und Maßnahmenkataloge verwendet, ebenso wie die „Zuordnungstabelle ISO 27001 sowie ISO 27002 und IT-Grundschutz“[4]. Auf allen Ebenen wird zudem die aktuelle Fassung der Beschreibungen auf den Internetseiten des BSI referenziert, sodass stets die Aktualität gewährleistet ist.

1.3 Inhalte

Der IT-Sicherheitsleitfaden stellt unabhängig von einer spezifischen Implementierung (sei es als Datenbank- oder Webanwendung, sei es als eine Sammlung von Tabellen) die für die Erreichung des nach dem Stand der Technik geforderten IT-Sicherheitsniveaus benötigten Informationen zur Verfügung. Aufgrund der Konzeption bietet er zudem ein methodisches Verfahren für einen bestmöglichen Einsatz (siehe Abschnitt 2 „Empfehlungen zur Anwendung des IT-Sicherheitsleitfadens“). Wie bereits im Unterabschnitt 1.2 „Struktur“ beschrieben, sind die wesentlichen Objekte des IT-Sicherheitsleitfadens die Anwendungsfälle, die Gefährdungen und die Maßnahmen. Diese werden nachfolgend beschrieben.

3) Download unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Check/kreuzreferenz_tabellen_zip.zip

4) Download unter:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf

1.3.1 Anwendungsfälle

Im IT-Sicherheitsleitfaden werden derzeit sechs Kategorien mit insgesamt 21 Anwendungsfällen unterschieden. Für jeden Anwendungsfall werden folgende Daten geführt:

Die **Kategorie** zu der der Anwendungsfall gehört, ein eindeutiges **Kürzel**, der **Name** des Anwendungsfalls und eine **Beschreibung**, ggf. weitere **Erläuterungen**, die wesentlichen **Sicherheitsaspekte** und die **Relevanz** des Anwendungsfalls für jeden einzelnen Anlagentyp nach BSI-Kritisverordnung [5]. Insbesondere Letzteres soll Betreibern helfen, sich bereits zu Beginn auf die relevanten Anwendungsfälle zu konzentrieren. Ferner ist bei einigen Anwendungsfällen zusätzlich eine **Prinzipskizze** verfügbar, die schematisch die Beschreibung des Anwendungsfalls ergänzt (siehe auch Anhang 4.2 „Prinzipskizzen").

Anwendungsfälle bilden den Einstieg in den IT-Sicherheitsleitfaden. Sie wurden so gewählt, dass sie unabhängig von der Größe einer Anlage sind. Auch werden keine Voraussetzungen in Bezug auf eine Einstufung einer Anlage als Kritische Infrastruktur gemacht. Für eine einzelne Anlage trifft in der Regel nur ein Teil der Anwendungsfälle je Kategorie zu, da die Anwendungsfälle innerhalb einer Kategorie meistens aufeinander aufbauen. Ein Beispiel:

In der Kategorie „SPS/PLS Programmierung und Wartung" werden drei Anwendungsfälle unterschieden:

- Lokale SPS Programmierung und Wartung,
- SPS Programmierung und Wartung von zentraler Stelle auf der Anlage,
- SPS Programmierung und Wartung über Fernzugriff (von anderem Standort aus).

Es ist zwar nicht ausgeschlossen, dass auf einer Anlage alle drei Szenarien anzutreffen sind, doch dürften in der Mehrzahl der Fälle nur ein oder zwei Anwendungsfälle innerhalb einer Kategorie zutreffen.

1.3.2 Gefährdungen

Den einzelnen Anwendungsfällen sind entsprechende Gefährdungen zugeordnet. Dabei kann ein und dieselbe Gefährdung mehreren Anwendungsfällen zugeordnet sein. Einem einzelnen Anwendungsfall sind in der Regel zwischen 20 und maximal 40 Gefährdungen zugeordnet. Nach Auswahl der zutreffenden Anwendungsfälle sind damit auch die zu betrachtenden Gefährdungen ermittelt. Die Liste der Gefährdungen enthält folgende Daten:

- Informationen zum jeweiligen Baustein: Das **Kürzel** des Bausteins im BSI-Grundschutz, die **Bezeichnung**, die **Ebene** (Technik, Management), zu der der Baustein gehört und der zugehörige **Link** zur BSI-Seite.
- Informationen zur jeweiligen Gefährdung: Das **Kürzel** der Gefährdung nach BSI-Grundschutz die **Bezeichnung** und der **Link** zur entsprechenden Seite beim BSI mit der Beschreibung der Gefährdung.

Der aus der Auswahl der Anwendungsfälle resultierende Katalog der relevanten Gefährdungen ist Grundlage für alle weiteren Schritte bei der Anwendung des IT-Sicherheitsleitfadens. Die Tatsache, dass dieselbe Gefährdung in verschiedenen Bausteinen mit verschiedenen Maßnahmen verknüpft sein kann, kann dazu führen, dass „scheinbar" Gefährdungen mehrfach genannt werden. Vor dem grundsätzlich sinnvollen Entfernen solcher Mehrfachnennungen, ist zu prüfen, ob auch derselbe Baustein genannt wird. In diesen Fällen, also derselbe Baustein mit derselben Gefährdung, können

5) Bereich Trinkwasserversorgung: Trinkwassergewinnungsanlage, Wasserwerk, Trinkwasseraufbereitungsanlage, Wasserverteilsysteme; Leitzentrale.
Bereich Abwasserentsorgung: Kanalisation, Kläranlage, Leitzentrale.

Doppelnennungen aus der Liste der Gefährdungen gestrichen werden. Je nach Implementierung sollte diese Aufgabe durch die entsprechenden Tools erledigt werden.

1.3.3 Maßnahmen

Das Ziel des IT-Sicherheitsleitfadens ist es, den Betreibern eine Liste der Maßnahmen an die Hand zu geben, die bei entsprechender Umsetzung den Stand der Technik in Bezug auf die IT-Sicherheit für den Anlagenbetrieb schaffen. Dabei werden diese Maßnahmen über die Auswahl der relevanten Anwendungsfälle und den damit verbundenen Gefährdungen identifiziert und entsprechend ausgewiesen. Maßnahmen stellen Handlungsanweisungen dar, in denen auch die verantwortlichen Rollen benannt werden. Auf Basis der Liste der Maßnahmen kann eine entsprechende Umsetzung geplant, durchgeführt und schließlich auch auditiert werden.

Im IT-Sicherheitsleitfaden werden zwei verschiedene Maßnahmenkategorien unterschieden. Diese bestimmen das B3S-Level[6] in folgender Weise:

Maßnahmen der Kategorie A (Alle) decken die Mindestanforderungen an IT-Sicherheit ab. Sie sollten unabhängig davon, ob eine Anlage Kritische Infrastruktur ist oder nicht, von allen Anlagenbetreibern umgesetzt werden. Mit Umsetzung der Maßnahmen des Levels A wird jedoch dann und nur dann der Stand der Technik erreicht, wenn im gegebenen Fall keine Maßnahmen des Levels K (Kritische Infrastruktur) in der Maßnahmenliste stehen. Ansonsten ist der Stand der Technik nur zu erreichen, wenn auch die Maßnahmen des Levels K umgesetzt werden. Demnach sind bei Anlagen, die als Kritische Infrastruktur eingestuft sind, sowohl die A- als auch die K-Maßnahmen umzusetzen. Bezogen auf den BSI-Grundschutz entsprechen die Maßnahmen des B3S-Levels A den mit Siegel A eingestuften Maßnahmen, alle übrigen Siegelwerte werden bei den im IT-Sicherheitsleitfaden aufgeführten Maßnahmen mit dem B3S-Level K eingestuft.

Zu den Maßnahmen werden folgende Daten im IT-Sicherheitsleitfaden geführt:

Das **Kürzel** der Maßnahme gemäß BSI-Grundschutz, die **Bezeichnung**, der **Link** auf die entsprechende BSI-Internetseite, das **B3S-Level** und die **Phase** entsprechend der Zuordnung von Gefährdung und Maßnahme im jeweiligen Baustein (aus der Kreuzreferenztabelle).

Die Liste der Maßnahmen kann in Verbindung mit den Informationen zu den Bausteinen und den Gefährdungen nach unterschiedlichen Kriterien sortiert und aufbereitet werden. Beispielsweise:

- Aufteilung der Maßnahmen in solche, die das Management betreffen und solche, die sich auf die Technik beziehen.
- Sortierung nach Themen (Bausteinen).
- Sortierung nach B3S-Level, etwa zum Zwecke der Priorisierung (z. B.: A-Maßnahmen mit höchster Priorität, K-Maßnahmen nachfolgend).
- Sortierung nach Gefährdungen.
- Sortierung nach Phasen.

Die Liste der Maßnahmen kann auch als Checkliste für ein Audit verwendet werden.

6) B3S = **B**ranchen**s**pezifischer **S**icherheits**s**tandard.

1.4 Erweiterbarkeit

Der IT-Sicherheitsleitfaden kann auf allen drei Ebenen (Anwendungsfälle, Gefährdungen, Maßnahmen) individuell durch den Anwender erweitert werden. Bei Erweiterungen ist allerdings die Systematik des IT-Sicherheitsleitfadens streng zu beachten. Dies bedeutet unter anderem, dass die Integritätsregeln unter allen Umständen einzuhalten sind, etwa dass ausschließlich Baustein-Gefährdung-Maßnahme-Kombinationen zulässig sind, die in den Kreuzreferenztabellen des BSI-Grundschutzes enthalten sind. Ebenso sind ausschließlich solche Gefährdungen und Maßnahmen zu verwenden, die in den entsprechenden Katalogen des BSI-Grundschutzes enthalten sind und nicht als „entfallen" gekennzeichnet wurden. Auf diese Art und Weise ist sichergestellt, dass die Erweiterungen zu keiner Abweichung vom Stand der Technik führen. Andernfalls muss der Betreiber auch noch nachweisen, dass er mit den zusätzlichen Maßnahmen immer noch den Stand der Technik erreicht.

Die Erweiterungen sollen eine individuelle Anpassung für den Betreiber ermöglichen, der dann in den Folgejahren auf den für seine Anlagen angepassten Inhalten aufsetzen kann. Allerdings ist es dann auch seine Verantwortung, die Fortschreibungen des IT-Sicherheitsleitfadens entsprechend in die individuell angepasste Version zu übernehmen. Dieses wird er im Rahmen der jeweiligen Audits nachweisen müssen.

2 Empfehlungen zur Anwendung des IT-Sicherheitsleitfadens

Nachfolgend wird die empfohlene Anwendung des IT-Sicherheitsleitfadens vorgestellt. Diese orientiert sich an den oben beschriebenen Prinzipien und Strukturen des IT-Sicherheitsleitfadens. Die Beschreibung erfolgt dabei „tool-neutral", setzt also nicht den Einsatz eines bestimmten Tools für den IT-Sicherheitsleitfaden voraus.

2.1 Grundsätzliches Vorgehen

Vorausgesetzt wird, dass die im Merkblatt beschriebenen Anforderungen beachtet und erfüllt werden. Entsprechende Hinweise finden sich im Folgenden an gegebener Stelle.

Der IT-Sicherheitsleitfaden kann in nahezu allen Phasen der Umsetzung der Anforderungen des IT-Sicherheitsgesetzes bei der Herstellung des Stands der Technik der für den Betrieb erforderlichen IT-Systeme unterstützen. Dabei werden grundsätzlich folgende Phasen unterschieden:

1. **Objektauswahl**
   - Infrastruktur-/Anlagenauswahl und -abgrenzung
   - Identifikation der relevanten IT-Systeme/-Komponenten
2. **Anwendungsfallauswahl**
   - Bestimmung der Anwendungsfälle
   - Überprüfung, ggf. Änderung/Ergänzung der Liste der Anwendungsfälle
3. **Gefährdungsbestimmung**
   - Überprüfung, ggf. Änderung/Ergänzung der Liste der Gefährdungen
   - Zuordnung der relevanten IT-Systeme/-Komponenten zu den Gefährdungen

4. **Risikobewertung**
   - Abgrenzung zur allgemeinen Risikobetrachtung
   - Risikoanalyse auf Basis der Gefährdungen
   - Risikobewertung mit Priorisierung der zugrunde liegenden Gefährdungen

5. **Maßnahmenermittlung**
   - Ermittlung der sich aus der Liste der Gefährdungen ergebenden Maßnahmen
   - Überprüfung der Liste der Maßnahmen und ggf. Änderung/Ergänzung
   - Zuweisung der relevanten IT-Systeme/-Komponenten zu den Maßnahmen

6. **Maßnahmenumsetzung**
   - Umsetzungsplanung (Ressourcen, Termine, Organisation etc.)
   - Durchführung
   - Wirksamkeitsprüfung
   - Dokumentation

7. **Auditierung**
   - Vorbereitung Audit (Nachweise, Checklisten etc.)

In Abschnitt 3 werden die Prozesse in Form von einfachen Prozessdiagrammen dargestellt, aus denen ersichtlich ist, welche Schritte in welcher Reihenfolge und mit welchen Ergebnissen in den Phasen 1 bis 5 abgearbeitet werden sollten.

2.2 Gegenstand des Einsatzes des IT-Sicherheitsleitfadens

Der Grundprozess der Trinkwasserversorgung beginnt mit der Wassergewinnung aus Oberflächen-, Quell- und/oder Grundwasser. Dort wo erforderlich, wird das gewonnene Wasser zur Einhaltung der Forderungen der Trinkwasserverordnung (TrinkwV) einer Aufbereitung unterzogen und desinfiziert. Im Anschluss daran wird das Trinkwasser über das Wasserverteilungssystem – bestehend aus Transport-, Haupt- und Versorgungs- sowie Anschlussleitungen – bis zum Kunden geliefert. Absperr- und Regelarmaturen, z. B. Schieber, Klappen und Ventile, sind ebenso Bestandteile des Wasserverteilungssystems wie Mess- und Zähleinrichtungen und Hydranten. Daneben umfasst das Wasserverteilungssystem auch (Hoch-)Behälter sowie Druckerhöhungs- bzw. Druckminderanlagen.

Bei der Trinkwasserversorgung und Abwasserentsorgung handelt es sich grundsätzlich um einen mechanisch-hydraulischen Grundprozess, für dessen Funktionieren zunächst keine IT-Systeme erforderlich sind. Aufgrund der Heterogenität von Anlagen sowie Ver- und Entsorgungs(infra)strukturen reicht die Bandbreite der Steuerungstechnik von autonomen dezentralen Systemen bis zu zentralen Prozessleitsystemen. Bei zentralen Systemen besteht häufig eine dezentrale autonome Rückfallebene; teilweise bis hin zur rein mechanisch-elektrischen Steuerung/Bedienung.

2.3 Vorgehen im Detail

Das nachfolgend beschriebene Vorgehen empfiehlt sich nicht nur für Kritische Infrastrukturen, sondern grundsätzlich für alle Anlagen der Trinkwasserversorgung und der Abwasserentsorgung.