DVGW

DWA
Clear Concepts. Clean Environment.

Industry-specific Security Standard for Water/Wastewater Utilities

July 2018

Industry-specific Security Standard for Water/Wastewater Utilities

Recognised under the IT Security Act – Legal Certainty for Operators of Critical Infrastructures in the Water Supply/Wastewater Sector

The Act to Strengthen the Security of Federal Information Technology (*BSI-Gesetz*, *BSIG*) that has been amended by the IT Security Act, defines the IT security requirements to be met by operators of Critical Infrastructures, which include, among others, the water industry sector with the drinking water supply and wastewater disposal industry. The Act provides an opportunity for the industry concerned to develop an 'industry-specific security standard' (B3S for short) that defines the 'state-of-the-art', which is required by law, for the Critical Infrastructures of the industry. With the elaboration of Guidelines DVGW W 1060 and DWA M 1060 - "IT Security – Industry-specific Security Standard for Water Supply/Wastewater Utilities" and the associated IT Security Code of Practice, the water supply/wastewater industry has succeeded in preparing the first B3S to be approved by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik, BSI*). The knowledge of experts from both lines of business, the application of existing standards, flexibility with respect to individual circumstances, a structured implementation approach and content in conformance with the set of rules played a key role in the preparation of these documents.

By Uwe Marquardt (GELSENWASSER AG) & Dr. Ludger Terhart (Emschergenossenschaft (Lippeverband)

Unlike many other industries, the water industry sector can rely on two associations with a long history of preparing industry-specific sets of rules, i.e. the DVGW that pronounces the rules in the drinking water supply sector and the DWA that does likewise in the wastewater disposal sector. Against this background, the idea immediately suggested itself to entrust exactly these associations with the task of elaborating an industry-specific security standard in accordance with the BSI Act.

The DVGW and the DWA founded joint working groups for this purpose that studied the various aspects of such a B3S in relation to water supply and wastewater (B3S WA, for short). Some of the key requirements that had to be considered in drafting this standard included, for instance

- Conformity with the DVGW and DWA sets of rules
- Meeting the requirements of the BSI B3S orientation guide
- Flexible adaptability to technical developments
- Use of existing standards
- Comprehensibility (intelligibility) and applicability by all industry operators, in particular SMEs
- Conformity with existing standards (in particular DIN ISO/IEC 297001 et seqq.), for multi-utility companies
- Strict limitation to the realities and infrastructures of the industry
- Consideration of individual conditions in respect of specific system components and installed IT systems
- Appropriateness of the processes required for implementation
- Clear naming of controls to be taken

The procedure and structure of the B3S WA that the DVGW and DWA elaborated on the basis of the above-mentioned requirements and that are described further down below may serve as a blueprint for other industry-specific security standards as they are inherently free of industry-specific assumptions.

As shown in [1], the B3S WA rests on two pillars, i.e. its integration into and conformity with the set of rules in the form of a DVGW-DWA Guideline, and the associated IT Security Code of Practice that can be flexibly adapted to situations. The regulations on the procedure of furnishing proof of compliance with the state of the art complement these two pillars. The Guideline itself contains all fundamental provisions and has been deliberately designed for longer-term applicability, whereas the IT Security Code of Practice addresses all procedures and structures – e.g. possible hazards and the controls required to avert or mitigate them – that have to be quickly aligned to the 'state of the art'.

The Guideline is associated with technical risk management in accordance with DIN EN 15975-2, "Security of drinking water supply – Guidelines for risk and crisis management – Part 2: Risk management" (previously DVGW Guideline W 1001). Accordingly, it describes the classical elements of risk assessment and risk mitigation and defines the corresponding requirements in addition to discussing the fundamentals and goals of IT security, the B3S WA structure and the organisational requirements, including IT security and/or business continuity management. It does, however, not address security services requirements, which are discussed in DVGW Guideline W 1050 and DVGW Water Information Bulletin No. 80. DIN EN 15975-2 as well as DVGW Guideline W 1050 and DVGW Water Information Bulletin No 80 can be applied, *mutatis mutandis*, to wastewater disposal utilities.

Operators of drinking water supply and wastewater disposal utilities are inherently operators of Critical Infrastructures, even though the majority of the respective companies do not currently fall within the scope of the Critical Infrastructure Protection Ordinance (*BSI-Kritisverordnung, BSI-KritisV*). Since it cannot be assumed that all these companies dispose of appropriate IT organisations and profound technical knowledge, the IT Security Code of Practice abstracts from technical IT conditions and, following the procedure [2] described by the American Water Works Association (AWWA), describes generalised use cases in layman's terms. These use cases describe fundamental IT system configurations for infrastructures as well as organisational issues and fundamental processes that occur in day-to-day business such as, for instance, how to maintain and use IT systems.

The BSI IT-Grundschutz Catalogues (in the following "BSI Standards" for short) provide an approved, tried and trusted IT infrastructure security standard and a practical interpretation of the DIN EN/IEC standard 27001, in particular. In contrast to the DIN EN/IEC-standard, the BSI Standards do not, however, only define general information security management system (ISMS) requirements but also provide a concrete catalogue of controls specifying which controls should be reasonably taken in the presence of a particular hazard.

The IT Security Code of Practice is fully based on the BSI Standards and the ICS Security Compendium of the BSI [3]. Reference is made to both, the hazards that are relevant in the context of the described use cases and to the associated controls (see figure 1) defined in the BSI Standards.

Drinking water supply and wastewater disposal experts jointly prepared, in collaboration and coordination with the BSI, the list of hazards and DIN EN/IEC to take in each case. This list consequently represents an industry-specific excerpt from the BSI Standards.

The IT Security Code of Practice does not conclusively mention all hazards and controls but presents the 'best practices' for the water industry sector. Since it exclusively draws from the BSI Standards, operators are free at any time to include other hazards and controls of the BSI Standards or, alternatively, substitute them by better-suited controls in a concrete situation, this way complementing the IT Security Code of Practice. It has been especially designed to permit substitutions or modifications at all levels (use case, hazard, controls), with the BSI Standards forming its only basis.

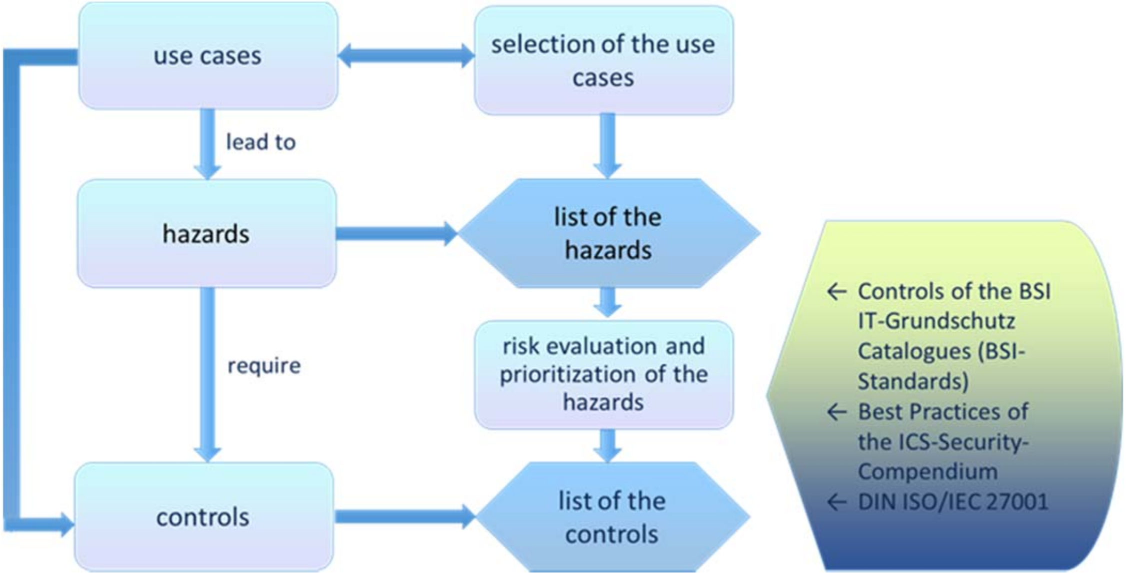
use cases
selection of the use cases
lead to
hazards
list of the hazards
require
risk evaluation and prioritization of the hazards
controls
list of the controls
← Controls of the BSI IT-Grundschutz Catalogues (BSI-Standards)
← Best Practices of the ICS-Security-Compendium
← DIN ISO/IEC 27001

Figure 1: Use cases are related with hazards and those require controls.

The IT Security Code of Practice has been designed from the outset to be easily adaptable to the updated BSI Standards "Modernisierter IT-Grundschutz", due to be published in 2018.

As the BSI Standards is the only referenced document, the IT Security Code of Practice always needs to be brought into line with the latest findings in IT security. In this context, the B3S WA explicitly relies on the technical competence of the Federal Republic of Germany's leading organisation in the field of IT security and is, therefore, always up to date.

The Federal Office for Information Security (*BSI*) officially recognised the suitability of the B3S WA at the end of June 2017. The DVGW and/or DWA Guidelines, which are identical in text, as well as the IT Security Code of Practice as a web-based online application tool, were published in Oktober 2017. The regulations on the industry-specific procedure on furnishing proof are published on the web sides of the 2 associations and can be downloaded for free. In accordance with the BSI-KritisV, drinking water and wastewater operators of Critical Infrastructures are advised to consider these regulations when providing proof – as they have to do every other year – to the BSI that they comply with the `state of the art'.

References

[1] Terhart, L., Wagner, K.: IT-Sicherheit in der Wasserversorgung – Branchenstandard IT-Sicherheit Wasser/Abwasser, at: DVGW energie | wasser-praxis, edition 12/2016, page 134–136 and Terhart.L, Marquardt, U: Branchenspezifischer Sicherheitsstandard Wasser/Abwasser gemäß IT-Sicherheitsgesetz anerkannt. Rechtssicherheit für die Betreiber Kritischer Infrastrukturen im Sektor Wasser/Abwasser, Korrespondenz Wasserwirtschaft · 2017 (10) · Nr. 8, page 454-455.

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

[3] Federal Office for Information Security (BSI): ICS Security-Compendium, online at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/ICS/ICS-Security_compendium.html).

Bibliography - The authors

Dipl.-Ing. Uwe Marquardt is head of Technical Coordination at GELSENWASSER AG and spokesperson of the DVGW W-GTK-2-8 IT Security.

Dr. Ludger Terhart is head of the Information Technologies department at Emschergenossenschaft/Lippeverband and spokesperson of DWA working group WI 5.4 Cyber Security.