Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA
Swiss Gas and Water Industry Association SGWA

W1018 d Ausgabe März 2019

REGELWERK

Empfehlung

Minimalstandard für die Sicherheit der Informations- Und Kommunikationstechnologie (IKT) in der Wasserversorgung

Anhang 3 Empfehlungen für Wasserversorger mit einem Versorgungsgebiet kleiner als 5000 Einwohner

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für wirtschaftliche Landesversorgung BWL
Geschäftsstelle IKT

SVGW, Grütlistrasse 44, Postfach 2110, 8027 Zürich
Telefon 044 288 33 33, Fax 044 202 16 33, www.svgw.ch

Schweizerischer Verein des Gas- und Wasserfaches SVGW
Société Suisse de l'Industrie du Gaz et des Eaux SSIGE
Società Svizzera dell'Industria del Gas e delle Acque SSIGA
Swiss Gas and Water Industry Association SGWA

W1018 d Ausgabe März 2019

REGELWERK

Empfehlung

Minimalstandard für die Sicherheit der Informations- Und Kommunikationstechnologie (IKT) in der Wasserversorgung

Anhang 3 Empfehlungen für Wasserversorger mit einem Versorgungsgebiet kleiner als 5000 Einwohner

IMPRESSUM

Es gelten die allgemeinen Geschäftsbedingungen unter
www.svgw.ch/AGB

Bezug bei der Geschäftsstelle des SVGW
(support@svgw.ch)

SVGW, Grütlistrasse 44, Postfach 2110, 8027 Zürich
Telefon 044 288 33 33, Fax 044 202 16 33, www.svgw.ch

INHALTSVERZEICHNIS

1 Einleitung

Die Wasserversorgung besteht aus einer äusserst heterogenen Gruppe von Akteuren. Für Wasserversorger mit einem Versorgungsgebiet von mehr als 5000 Einwohnern steht ein separates Excel basiertes Assessment-Tool zur Verfügung. Den Wasserversorgern mit einem Versorgungsgebiet kleiner als 5000 Einwohner wird geraten, die hier zur Verfügung gestellten Empfehlungen umzusetzen.

2 Informationssicherheit in einer kleinen Wasserversorgung

2.1 Massnahmenschwerpunkt

Um die Informationssicherheit in einem KMU vollumfänglich zu erhöhen, müssen die drei Bereiche Technik, Organisation & Prozesse und persönliches Verhalten betrachtet werden (Abb. 1).

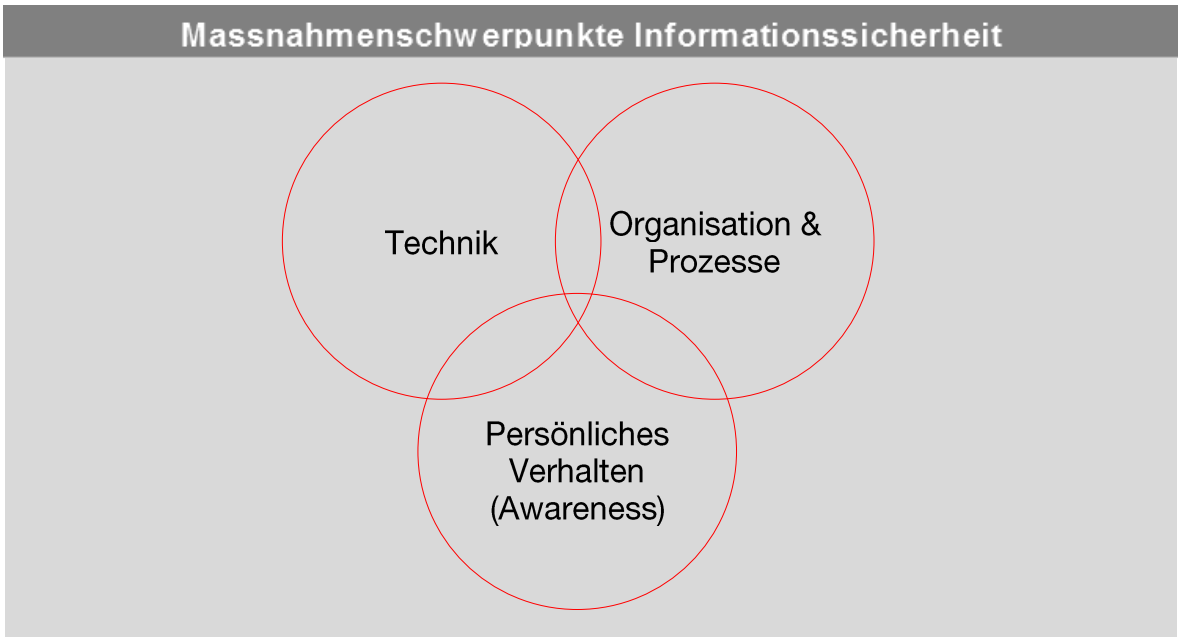

Abb. 1 Massnahmenschwerpunkte Informationssicherheit

2.1.1 Technik

Technische Lösungen steigern die Komplexität und kosten viel. Es ist deshalb sinnvoll, auf «Good Practice» Massnahmen zu setzen und auf teure Experimente zu verzichten. Folgende Liste zeigt Beispiele von «Good Practice» Massnahmen:

- Zwei Rechencenter an verschiedenen Standorten; redundante Systeme
- Eine angemessene Netzwerkzonierung
- Verschlüsselung mobiler Geräte
- Firewall, Webfilter, Malware Protection
- Network Access Control System
- Mobile Device Management Software
- Elektronisches Zutrittssystem

2.1.2 Organisation & Prozesse

Organisatorische Massnahmen werden dort eingesetzt, wo technische Massnahmen nicht sinnvoll und zu komplex sind. Beispiele können sein:

- Inventarisierung über die bestehenden Assets
- Vergabe von Berechtigungen (Vieraugenprinzip/doppelte Unterschrift)
- Notfallvorsorge (z. B. Szenarien, Alarmierung, Organisation, Sofortmassnahmen, vorbehaltene Entschlüsse, Notfallbetrieb, Rückkehr zum Normalbetrieb)
- Geheimhaltungsvereinbarung mit Mitarbeitenden
- Vertraulichkeitsvereinbarung mit externen Partnern
- Dokumentenklassifizierung
- Risikomanagement Prozess
- Entsorgungskonzept

2.1.3 Persönliches Verhalten

Der Mensch kann neue Angriffsverfahren erkennen und entsprechende Schutzmechanismen einführen – er ist aber auch die grösste Bedrohung. Als wertvolle Ressource soll der Mensch zu Gunsten der Informationssicherheit eingesetzt werden. Es geht um die Sensibilisierung zum verantwortungsbewussten Umgang mit Informationen und um einen Appell an die Eigenverantwortung. Beispiele dafür sind:

- Notebook und Aktenkoffer immer im Kofferraum verstauen.
- Starke Passwörter verwenden.
- Vorsicht im Umgang mit unbekannten Mails.
- Vertrauliche Papierdokumente zerstören (z. B. Shredder) und nicht einfach in den Papierkorb werfen.
- Keine vertraulichen Telefongespräche im öffentlichen Raum führen.

2.2 18 Schritte zu besserer Informationssicherheit

2.2.1 Risikobasiertes Vorgehen

Das risikobasierte Vorgehen erlaubt jeder Wasserversorgung (egal ob gross oder klein) das Risiko selbständig zu erheben und die eigene Risikobereitschaft festzulegen. Je nach Grösse der Wasserversorgung können bei der Risikobereitschaft deutliche Unterschiede bestehen. So kann ein Ausfall der IKT bei einem kleinen Wasserversorger unter Umständen leichter manuell überbrückt werden als bei einem grossen Wasserversorger. Konkret bedeutet dies, dass eine Wasserversorgung einzelne Empfehlungen nach ihrem eigenen Risikoverständnis nicht oder nur teilweise umsetzen muss.

2.2.2 Empfehlung für kleine Wasserversorger

Die folgende Hilfestellung ist insbesondere (aber nicht nur) für kleinere Wasserversorger gedacht, bei denen ein ganzheitliches Umsetzen des Cyber Security Frameworks nicht möglich ist. Es ersetzt jedoch nicht die Risikoeinschätzung und die Definition der eigenen Risikobereitschaft. Die folgenden Empfehlungen gelten als Hilfestellungen und Best-Practice-Anleitung. Sie ist in 18 Hauptpunkte (Empfehlungen) mit jeweils mehreren Unterpunkten unterteilt. Die Vollständigkeit der Umsetzung muss dem risikobasierten Ansatz der Wasserversorgung angepasst werden. Entsprechend können einige, alle oder sogar zusätzliche Unterpunkte umgesetzt werden. Zentral ist dabei, dass der Wasserversorger die Vollständigkeit der Umsetzung entsprechend seinem risikobasierten Ansatz belegen und zyklisch verbessern kann.

Die folgende Hilfestellung basiert auf dem erweiterten 10-Punkte-Programm der Information Security Society Switzerland (ISSS)[1]:

	Massnahmen für einen wirkungsvollen Grundschutz[2]
1.	**Sichern Sie Ihre Daten regelmässig mit Backups**
	Datenverluste entstehen auf verschiedene Arten: Daten werden versehentlich überschrieben, Informationen auf einer Harddisk werden durch einen Defekt unleserlich oder ein Brand beziehungsweise ein Wasserschaden zerstört Ihre Daten. Solche Verluste können Sie mit regelmässigen Datensicherungen (Backups) vermeiden beziehungsweise in Grenzen halten. • Grundsätzlich sind alle Daten mit geschäftsrelevantem Inhalt zu sichern. Softwarekonfigurationen sollten ebenfalls gesichert werden. • Die Häufigkeit der Datensicherung richtet sich nach Tätigkeit und Grösse Ihres Unternehmens. Mindestens einmal pro Woche sollte jedes KMU seine Daten sichern. • Regeln Sie schriftlich, wer für Datensicherungen zuständig ist und führen Sie eine Kontrollliste über die erfolgreiche Sicherung der Daten. • Sichern Sie die Daten immer auf mobilen Medien (Bandlaufwerk, auswechselbarer Datenträger). • Es lohnt sich, von wichtigen Daten, die nur in Papierform vorliegen (z. B. von Verträgen, Urkunden), Kopien anzufertigen und diese ebenfalls ausser Haus aufzubewahren.

[1] ISSS – Mehr Informationssicherheit für Klein- und Mittelbetriebe (KMU). Das erweiterte 10-Punkte-Programm schafft mehr Schutz. https://www.kmu.admin.ch/kmu/de/home/praktisches-wissen/kmu-betreiben/infrastruktur-und-it/it-sicherheit.html Auf dieser Webseite das Register «Downloads», dann den ersten Link auf «Mehr Informationssicherheit für Klein- und Mittelbetriebe» klicken.

[2] Die Empfehlungen gelten dann als eingehalten, wenn alle Punkte vollständig umgesetzt sind. Die Vollständigkeit der Umsetzung richtet sich in erster Linie nach dem risikobasierten Ansatz des Unternehmens und nicht nach den hier aufgeführten Unterpunkten aus.

	• Beachten Sie, dass die Bilanz, die Erfolgsrechnung, die Geschäftsbücher, die Inventare, die Buchungsbelege und die buchungswirksame Geschäftskorrespondenz während zehn Jahren aufbewahrt werden müssen. • Überprüfen Sie periodisch, ob sich die Daten von den Sicherungsmedien zurückspielen lassen. Jede Sicherung ist nutzlos, wenn die Daten nicht korrekt auf das Backup-Medium übertragen wurden. • Machen Sie sich Überlegungen zum Sichern ihrer Daten auf externen Datenträgern. Die Sicherung ihrer Daten auf einem externen Datenträger stellt eine zusätzliche Resilienz-Ebene beispielsweise hinsichtlich Ransomware-Angriffe dar. Ausserdem sollten die Backups möglichst nicht an den gleichen Orten wie die Originaldaten aufbewahrt werden.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
2.	**Halten Sie Ihr Antivirus-Programm aktuell**		
	Schädliche Programme, wie zum Beispiel Viren und Würmer, können Ihre IKT-Infrastruktur lahmlegen und damit die wirtschaftliche Existenz Ihres Unternehmens gefährden. • Computerviren können Daten und Programme verändern, manipulieren oder sogar vollständig zerstören. Bösartige Computerprogramme werden via E-Mail-Anhänge (Attachments) und Instant-Messengers usw. übertragen. Im Internet sind Viren oft als nützliche oder unterhaltende Gratisprogramme getarnt und werden durch einen einfachen Mausklick aktiviert. • Unzureichend geschützte Computersysteme werden häufig zur Verbreitung von Viren und für gezielte Attacken gegen ein drittes Unternehmen missbraucht. Wer als Geschäftsleiterin oder Geschäftsleiter ungenügende Vorkehrungen zum Schutz seiner Computersysteme trifft, handelt fahrlässig und muss allenfalls mit Strafverfolgung rechnen. • Schutz vor bekannten Viren und Würmern bietet ein Antivirus-Programm. Es identifiziert Eindringlinge und macht sie unschädlich. • Installieren Sie ein Antivirus-Programm auf sämtlichen Servern, Arbeitsstationen sowie auf Ihren Notebooks. • Da laufend neue Schadprogramme entwickelt werden, müssen Schutzprogramme (Antivirensoftware) laufend aktualisiert werden. Die Aktualisierung sollte auf jeden Fall täglich durchgeführt werden. • Fordern Sie die Mitarbeitenden auf, Warnmeldungen über Schadprogramme, z. B. Viren, unverzüglich dem IKT-Verantwortlichen zu melden.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
3.	**Schützen Sie Ihren Internetzugang**		
	Wenn es in Ihrem Betrieb Firewalls gibt, achten Sie darauf, dass nur die notwendigen Ports geöffnet sind. In der Welt des Internets und des elektronischen Datenaustauschs erfüllt die Firewall diese Sicherheitsaufgabe. • Ohne Firewall können Unbefugte auf Ihren Computersystemen relativ leicht Schaden anrichten. Sie können darauf unbemerkt Befehle ausführen oder Ihre Rechner zu illegalen Attacken auf Dritte missbrauchen. Zudem gelangen sie an Geschäftsdaten, die eventuell dem Datenschutzgesetz unterstehen.		

	• Im Handel sind Produkte erhältlich, die gleichzeitig eine Firewall und einen zusätzlichen Netzwerk-Virenschutz bieten. Gerade für kleinere Betriebe sind kombinierte Produkte empfehlenswert. • Manche Betriebssysteme haben eine eigene Firewall eingebaut. Nutzen Sie auf jeden Fall auch diese Möglichkeit und aktivieren Sie diese Firewalls. • Wenn Sie in Ihrem Betrieb Wireless-LAN für Ihre Computer einsetzen, sorgen Sie dafür, dass diese richtig und sicher funktionieren. • Sämtliche Netzwerkübergänge müssen mit einer Firewall gesichert werden. • Wickeln Sie den gesamten Internetverkehr über die Firewall ab. Erlauben Sie keine anderen Zugänge zum Internet (z. B. via Modem). • Setzen Sie keine privaten Laptops und Wireless-LAN-Geräte im Unternehmen ohne entsprechenden Schutz und schriftliche Einwilligung des IKT-Verantwortlichen ein. • Schützen Sie die Konfiguration Ihrer Firewall mit einem starken Passwort.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
4.	**Aktualisieren Sie Ihre Software regelmässig**		
	So wie Sie Ihr Auto regelmässig warten, müssen auch Computerprogramme in einem Unternehmen gepflegt und auf den neuesten Stand gebracht werden. • Heutige Software beinhaltet oft Millionen von Zeilen Code. Dabei schleichen sich trotz Kontrollen Fehler ein. Für den Hersteller ist es nahezu unmöglich, Anwendungen in jeder denkbaren Umgebung und möglichen Konfiguration zu testen. Die Hersteller bieten regelmässig sogenannte «Patches», also «Software-Flicken» an. Sie beheben die bekannten Fehler. • Wenn Sie Ihre Software nicht oder nur selten aktualisieren, können Angreifer bekannte Fehler ausnützen, um Daten zu manipulieren oder um Ihre Infrastruktur für bösartige Zwecke zu missbrauchen. • Minimieren Sie Ihre «Angriffsfläche», indem Sie nur Software installieren, die Sie tatsächlich benötigen und unnötige Dienste, Netzwerkfreigaben und Protokolle deaktivieren. • Installieren Sie die neuesten «Patches» für Betriebssysteme und Anwendungsprogramme. • Installieren Sie verfügbare «Sicherheits-Updates» so schnell wie möglich. • Installieren Sie «Patches» auf sämtlichen Computern, d.h. auch auf Notebooks und Geräten von externen Mitarbeitenden.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
5.	**Verwenden Sie starke Passwörter**		
	Wer den Benutzernamen und das Passwort eines Anwenders kennt, kann sich in einem System anmelden und übernimmt damit die (Computer-) Identität des entsprechenden Anwenders mit allen Zugriffsberechtigungen! Durch Passwortdiebstahl können somit Unbefugte ohne grossen Aufwand an vertrauliche Geschäftsformationen gelangen. Verhindern Sie, dass in Ihrem Betrieb der Identitätsdiebstahl möglich ist. • Werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IKT-Verantwortlichen sofort geändert werden.		

	• Halten Sie Ihre Mitarbeitenden dazu an, nur starke Passwörter einzusetzen, die regelmässig geändert werden. Machen Sie allen bewusst, dass sie für Handlungen verantwortlich sind, die unter ihrem Benutzernamen ausgeführt werden. • Starke Passwörter sind mindestens acht Zeichen lang, enthalten Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen. • Verwenden Sie keine Passwörter, die Namen, AHV- und Passnummern und Geburtsdatum aus dem Familienumfeld enthalten. • Verwenden Sie ebenfalls keine Passwörter, die in Wörterbüchern (alle Sprachen) zu finden sind. • Schreiben Sie Passwörter niemals auf, ohne die Notiz sicher z. B. im Tresor zu verwalten. • Geben Sie Ihr Passwort niemals an Dritte weiter.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
6.	**Schützen Sie Ihre mobilen Geräte**		
	Mobiltelefone, und Notebooks mit Wireless-LAN sind ausgesprochen praktisch und vielseitig. Falsch eingesetzt, stellen diese Geräte aber ein Sicherheitsrisiko dar. Wer aus geschäftlichen Gründen gezwungen ist, sensible Daten auf mobilen Geräten zu speichern, muss spezielle Vorkehrungen treffen. • Sämtliche mobilen Geräte müssen mit einem starken Passwort geschützt werden (siehe Punkt 5) und die Daten müssen verschlüsselt gespeichert werden. Beim Verlust des Geräts oder im Fall eines Diebstahls haben Unbefugte sonst leichtes Spiel, an Ihre Geschäftsdaten zu gelangen. • Auf mobilen Geräten sollten nur diejenigen Daten gespeichert sein, die tatsächlich benötigt werden. • Auch mobile Geräte müssen regelmässig auf Schadsoftware (z. B. Viren) geprüft werden, weil sie z. B. via E-Mail-Funktionen mit Ihren übrigen Computern synchronisiert werden. • Durch falsch konfigurierte Wireless-LAN-Geräte können Hacker innerhalb weniger Minuten aus Distanzen von über einem Kilometer in Ihr Firmennetzwerk eindringen! Die Nutzung von externen und öffentlichen Access Points (HotSpots) muss speziell geregelt werden. • Aktivieren Sie Bluetooth bei Ihren Geräten (Handy, Notebooks) nur bei Bedarf und nicht erkennbar. Ihr Gerät reagiert sonst ohne Ihr Wissen auf Anfragen fremder Geräte (im Umkreis von bis zu 100 Metern). • Aktivieren Sie die Verschlüsselung der kabellosen Datenübermittlung (WPA2). • Übermitteln Sie vertrauliche Daten nur über Verbindungen, die zusätzlich mit einem Virtual Privat Network (VPN) geschützt sind.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
7.	**Machen Sie Ihre IKT-Benutzerrichtlinien bekannt**		
	Ohne verbindliche und verständliche IKT-Benutzerrichtlinien können Ihre Mitarbeitenden nicht wissen, welche Handlungen erlaubt und welche verboten sind. Regeln werden nur ernst genommen, wenn sich auch Vorgesetzte daranhalten. Handeln Sie in allen Sicherheitsaspekten als Vorbild.		

	• Definieren Sie als Bestandteil zu den Anstellungsbedingungen schriftliche IKT-Benutzerrichtlinien und informieren Sie die Mitarbeitenden. • Machen Sie Sicherheit in Ihrem Unternehmen immer wieder und auf unterschiedliche Weise zum Thema. • Führen Sie ein bis zwei Mal pro Jahr Sensibilisierungsaktionen durch. Diese lassen sich auch mit einfachen Mitteln realisieren: z. B. durch E-Mails an alle Mitarbeitenden, Rundschreiben in der internen Post, Plakate in der Kantine, Beiträge in der Firmenzeitung usw. • Organisieren Sie eine Grundausbildung für alle Mitarbeitenden (z. B. auf der Basis dieses Dokuments). Die wichtigsten Lernziele sind: – Nutzen der IKT-Sicherheit – Bestimmen starker Passwörter – sicherer Umgang mit Internet, E-Mail und dem Virenschutz – Ablagestruktur von Dokumenten • Regeln Sie – die Installation und den Einsatz von eigenen Programmen und Hardware (Spiele, USB-Memory Sticks, private Notebooks usw.), – den Gebrauch des Internets (was ist erlaubt, was nicht), – den Gebrauch von E-Mail (Vertraulichkeit, Weiterleiten, private E-Mail-Adressen, Kettenbriefe usw.), – den Umgang mit vertraulichen Informationen, – das Verhalten bei sicherheitsrelevanten Vorkommnissen. • Kündigen Sie Sanktionen bei einem Verstoss gegen die Benutzerrichtlinien an.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
8.	**Schützen Sie die Umgebung Ihrer IKT-Infrastruktur**		
	Wissen Sie, wer in Ihrem Unternehmen tagsüber ein- und ausgeht? Einige wenige Vorkehrrungen verhindern bereits, dass Unbefugte an wichtige Geschäftsinformationen gelangen. Gelebte, sichtbare Sicherheit ist heute ein Qualitätskriterium und schafft Vertrauen bei Kunden und Lieferanten. Was nützt die beste Firewall, wenn sich Fremde in die Büroräume einschleichen können? • Alle Zugänge zum Gebäude bzw. Firmenareal sind abzuschliessen oder zu überwachen. Falls dies nicht möglich ist, muss zumindest der Büro-Teil geschützt werden. • Lassen Sie Besucher, Kunden und Bekannte nicht unbeaufsichtigt in Ihrem Betrieb umhergehen. • Alle Drittpersonen werden am Empfang abgeholt, während ihres Aufenthaltes dauernd begleitet und beim Verlassen des Gebäudes am Ausgang wieder verabschiedet. • Wenn Sie nicht über einen Empfang verfügen, der den Eingangsbereich überblickt, sollten Sie die Eingangstüre schliessen und ein Schild «Bitte läuten!» anbringen. • Stellen Sie sicher, dass sämtliche Einstiegsmöglichkeiten (Fenster, Türen usw.) über einen ausreichenden Einbruchschutz verfügen. • Schlüssel und Badges müssen korrekt verwaltet und die entsprechenden Listen aktualisiert werden. Schlüssel mit Passepartout-Funktion sind restriktiv zu verteilen. Die entsprechenden Berechtigungen müssen mindestens jährlich auf ihre Notwendigkeit geprüft werden. • Mitarbeitende, die aus dem Unternehmen austreten, geben ihre Schlüssel, Badges und andere Zugangsberechtigungen beim Austritt ab.		

	• Stellen Sie Server in abschliessbare, klimatisierte Räume. Ist kein entsprechender Raum verfügbar, schliessen Sie die Server in einen Computerschrank (Rack). • Lagern Sie brennbare Materialien wie Papier usw. nicht im oder unmittelbar vor dem Serverraum. • Stellen Sie Netzwerkdrucker nicht in öffentlich zugängliche Räume, da Unbefugte Einblick in Dokumente erhalten können. • Schliessen Sie Netzwerkkabel, die durch öffentliche Räume führen, sowie Modems, Hubs, Router und Switches ein. • In sensiblen Bereichen ihrer Wasserversorger sollte Besuchern der Gebrauch von Aufnahmegeräten (mobile Phone usw.) verboten werden.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

	Massnahmen für mehr Vertraulichkeit		
9.	**Regeln Sie den Zugriffschutz auf Daten**		
	Durch unbefugten Zugriff können Informationen missbraucht werden. Schützen Sie deshalb den Datenzugriff entsprechend, sodass nur berechtigte Personen Zugang haben. • Wer unbefugten Zugriff zu Informationen hat, kann diese einsehen, kopieren, verändern oder löschen. • Legen Sie fest, wer Zugriff auf bestimmte IKT-Anwendungen oder Informationen hat. Dabei sollten die Zugriffsrechte rollenbasiert vergeben werden, z. B. Sekretariat, Verkauf, Buchhaltung, Personalwesen, Systemadministrator. • Es sind nur so viele Zugriffsrechte zu vergeben, wie zur Durchführung einer Aufgabe benötigt werden («Need-to-know-Prinzip»). Die Zugriffsrechte werden von der jeweils verantwortlichen Person festgelegt. • Die Rechteverwaltung muss dokumentiert werden. Festgehalten wird, welche Person welche Funktion wahrnimmt und welche Person Zugriff auf welche Applikationen und Daten hat. Überprüfen Sie diese Rechte regelmässig und passen Sie sie entsprechend an. • Beim Austritt von Mitarbeitenden aus dem Unternehmen oder bei internem Wechsel sind deren Benutzerkonten und die Zugriffsrechte sofort zu sperren bzw. anzupassen. • Besonders zu beachten sind die Systembetreuer und die Administratoren. Sie verfügen in der Regel über sehr weitgehende Rechte.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
10.	**Verschlüsseln Sie mobile Datenträger und Übermittlung**		
	Vertrauliche Daten können bei ungeschützter Übermittlung (z. B. E-Mail) von Dritten eingesehen werden. Mobile Geräte können verloren gehen und Ihre Daten in falsche Hände geraten. Um die Vertraulichkeit zu gewährleisten, ist eine Verschlüsselung der Daten auf den Geräten sowie der Übermittlung notwendig. • E-Mails können von Dritten gelesen werden. E-Mails mit vertraulichem Inhalt sollten Sie deshalb verschlüsseln. • Mobile Geräte wie Notebooks sind generell zu verschlüsseln.		

	• Übermitteln Sie vertrauliche Daten nur über Verbindungen, die zusätzlich mit einem Virtual Privat Network (VPN) geschützt sind (siehe auch Punkt 6).		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
11.	**Sensibilisieren Sie ihre Mitarbeitenden**		
	Nur sensibilisierte Mitarbeitende setzen Sicherheitsmassnahmen um. Erläutern Sie Ihren Mitarbeitenden die Notwendigkeit der Massnahmen und den korrekten Umgang mit vertraulichen Daten. Schliessen Sie mit ihren Mitarbeitenden und externen Partnern eine Vertraulichkeitsvereinbarung ab. • Eigene und externe Mitarbeitende bearbeiten oft vertrauliche Daten. Diesen Personen muss bewusst sein, dass sie entsprechende Massnahmen ergreifen müssen, um die Vertraulichkeit zu gewährleisten. • Fügen Sie eine Vertraulichkeitsklausel in den Arbeitsvertrag ein. Dies gilt auch für externe Mitarbeitende oder Partner. Diese Vertraulichkeitsvereinbarung definiert, wie mit vertraulichen Informationen umgegangen werden muss. • Sensibilisieren Sie die neuen Mitarbeitenden bereits bei deren Einstellung für die Belange der IKT-Sicherheit. • Kündigen Sie Sanktionen bei einem Verstoss gegen die Richtlinien an.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
12.	**Regeln Sie die Entsorgung von Informationen und Informationsträgern**		
	Vertrauliche Informationen können bei unsachgemässer Entsorgung in falsche Hände geraten. Erklären Sie Ihren Mitarbeitenden, wie Informationen und Informationsträger (Papier, elektronische Informationsträger) sicher und umweltgerecht entsorgt werden. • Regeln Sie die Entsorgung: – von Altpapier (Zeitungen, Werbungen und andere öffentliche Dokumente) – alle übrigen internen und vertraulichen Dokumente – Karton – elektronische Datenträger wie USB-Stick, CD und externe Festplatten • Legen Sie fest, wie das Archiv entsorgt werden soll. • Kündigen Sie Sanktionen bei einem Verstoss gegen die Richtlinien an.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

	Massnahmen für mehr Verfügbarkeit
13.	**Überprüfen Sie Ihre Systeme**
	Das reibungslose Funktionieren der IKT-Systeme muss jederzeit gewährleistet sein. Deshalb müssen IKT-Systeme überprüft und regelmässig gewartet werden. Eine korrekte Wartung vermindert Störungen und verhindert Schäden an der Informationstechnologie.

	• Prüfen Sie regelmässig die Funktionstüchtigkeit Ihrer IKT-Systeme: – Funktioniert das Backup-System? – Sind die Backup-Daten tatsächlich lesbar? – Funktioniert die unterbrechungsfreie Stromversorgung (USV)? – Enthalten die automatischen Systemprotokoll-Dateien Fehlermeldungen? • Beachten Sie auch organisatorische Aspekte: – Werden gesetzliche und andere Richtlinien eingehalten? – Ist die Notfallvorsorge überprüft worden? • Überwachung und Wartungsarbeiten müssen in regelmässigen Abständen durchgeführt werden. • Erstellen Sie eine Wartungsliste: – Was muss wann durch wen geprüft und gewartet werden. – Stellen Sie die Kontrolle und die Nachvollziehbarkeit der Wartung sicher. • Lassen Sie die externen Wartungstechniker eine Vertraulichkeitsvereinbarung unterzeichnen (siehe Punkt 11).		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
14.	**Schützen Sie den Zugang in Ihr Firmennetz durch eine Zwei-Faktor-Authentifizierung**		
	Ein Zugriff von Extern in das Firmennetz setzt aus Sicherheitsgründen eine Zwei-Faktor-Authentifizierung voraus. Diese bietet einen angemessenen Schutz und gilt als üblicher Industriestandard. • Definieren Sie mögliche Zugriffsvarianten wie: – Applikationsbasierter Zugriff – Netzwerkbasierter Zugriff – Site-to-Site-VPN Zugriff • Definieren Sie Kategorien (interne und externe Mitarbeitende, Kunden, Lieferanten, Gäste) und legen Sie fest, wem welche Zugriffsvariante mit welchem Service zugeordnet wird.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
15.	**Sorgen Sie für eine unterbruchfreie Stromversorgung**		
	Wenn Sie auf eine hohe Verfügbarkeit Ihrer Daten und Systeme angewiesen sind, können Sie sich keinen Ausfall leisten. Eine unterbruchfreie Stromversorgung (USV) schützt Ihre Systeme vor Stromausfall und Spannungsspitzen (z. B. Blitzeinschlag) und verhindert Datenverluste. • Die unterbruchfreie Stromversorgung (USV) wird zwischen der normalen Stromversorgung und den zu schützenden Geräten geschaltet. • Bei einem Stromausfall versorgt die Batterie der USV die Komponenten so lange mit Strom, bis sie geregelt abgeschaltet werden können. • Zusätzlich kann eine USV als Filter wirken und Ihre Systeme vor Spannungsschwankungen schützen. • Neben dem Server müssen auch weitere wichtige Peripherie-Geräte an der USV angeschlossen werden. Dazu gehören beispielsweise wichtige Rechner im Netzwerk, Router, Backup-Systeme usw.		

	• Erstellen Sie eine Liste mit den Komponenten, die an die USV angeschlossen werden müssen. Aus dieser Zusammenstellung wird die benötigte Leistungsfähigkeit der USV bestimmt. • Kontrollieren Sie regelmässig die Leistungsfähigkeit der Batterien der USV und ersetzen Sie schwache Batterien sofort (siehe Punkt 13).		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
16.	**Halten Sie wichtige Elemente redundant**		
	Ein Ausfall eines kritischen Elements in Ihrem Netzwerk, z. B eines Servers, kann viel Geld kosten und den Betrieb stören. Viele Unternehmen sind sich nicht bewusst, wie abhängig sie von kritischen Systemen sind. Um nach einem Ausfall möglichst schnell wieder den Betrieb aufzunehmen, empfiehlt es sich, kritische IKT-Systeme (z. B. Harddisk, Netzteile, Netzwerkkomponenten oder ganze Server) redundant zu halten. • Redundanz heisst, dass mindestens ein identisches Ersatzgerät oder -system vorhanden ist, das das beschädigte Gerät oder System bei einem Ausfall ersetzt. • Um den Ausfall einer Festplatte zu verhindern, kann eine sogenannte Festplattenspiegelung benützt werden. Falls eine Festplatte ausfällt, übernehmen automatisch andere Festplatten deren Aufgabe, ohne dass der Betrieb unterbrochen wird. Wichtige Daten sollten georedundant gehalten werden. • Schliessen Sie mit Ihren Lieferanten Serviceverträge für Hard- und Software Interventionen (Reaktionszeiten, Lieferfristen usw.) ab. • Erarbeiten Sie eventuell mit Ihrem Lieferanten Notfallpläne für Ausfallszenarien (siehe Punkt 17). • Benutzen Sie nur Komponenten von namhaften Herstellern. Diese sind in der Regel von guter Qualität und wurden intensiv getestet. • Denken Sie nicht nur an redundante IKT-Systeme, sondern auch an eine redundante Internet-Anbindung. • Wichtig ist, dass die Ersatzgeräte identisch und bereits vorkonfiguriert sind, damit sie im Ereignisfall sofort eingesetzt werden können.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
17.	**Planen Sie die Notfallvorsorge**		
	Ein existenzbedrohender Notfall tritt meistens plötzlich ein. Besonders höherer Gewalt ist man schutzlos ausgeliefert. Durch das richtige Verhalten kann in einer Notfallsituation der Schaden in Grenzen gehalten werden. Es muss deshalb im Voraus festgelegt werden, wie man sich bei einem Notfall verhält und welche Aktionen auszulösen sind. • Überlegen Sie sich, welche Notfallsituationen in Ihrem Unternehmen eintreten können und wie darauf reagiert werden soll. Setzen Sie sich mit folgenden Ausfallszenarien auseinander: Ausfall der IKT, Ausfall von Personal, Ausfall der Arbeitsplätze, des Gebäudes und Ausfall externer Partner und Dienstleistungen. • Bei einem Notfall muss schnell alarmiert und gehandelt werden. Jede Person muss genau wissen, wer alarmiert werden muss und wer verantwortlich ist. Erstellen Sie dazu einen Alarmierungsplan und eine Verantwortlichkeitsregelung. • Erstellen Sie einen Notfallvorsorgeplan. Dazu gehören Sofortmassnahmen zur Einleitung des Notfallbetriebs, Regelungen für den Ablauf des Notfallbetriebs und Massnahmen zur schnellen Wiederherstellung des Normalbetriebes.		

	• Instruieren Sie die Mitarbeitenden, wie sie sich in Notfallsituationen zu verhalten haben und welche Sofortmassnahmen eingeleitet werden müssen. • In Stress-Situationen handelt der Mensch oft intuitiv. Das richtige Verhalten im Ereignisfall muss deshalb geübt werden. • Dokumentieren Sie alle IKT-Komponenten ordnungsgemäss. Bewahren Sie diese Dokumentation extern auf. • Zu einer Dokumentation gehören beispielsweise eine Liste der Benutzer, Gruppen und Rechte (siehe Punkt 9), das Netzwerklayout, die Konfigurationen der Systeme, Installationsbeschreibung, Konzepte, Arbeitsabläufe und Stellenbeschreibungen für sicherheitsrelevante Stellen. Führen Sie diese Dokumentationen regelmässig nach. • Organisieren Sie Ausweichmöglichkeiten für die IKT-Systeme mit der höchsten Verfügbarkeitsanforderung, damit schnell ein Weiterbetrieb gewährleistet werden kann. • Überprüfen Sie die Reaktionszeit des Supports mit Ihren Verfügbarkeitsanforderungen. Kann z. B. ein Serverausfall wirklich in der benötigten Zeit behoben werden?		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
18.	**Verteilen Sie das Know-how**		
	Gerade in kleineren Wasserversorgern steckt das entscheidende Wissen über die IKT-Systeme (z. B. SCADA) oft nur bei einer Person. Fällt sie aus oder verlässt sie das Unternehmen, gerät es in Schwierigkeiten. • Das Schlüsselwissen steckt in der Konfiguration, im Betrieb und Unterhalt der IKT-Systeme des Unternehmens. Versuchen Sie das Schlüsselwissen von Personen zu verteilen und zu dokumentieren • Krankheit, Unfall, Todesfall oder der Austritt aus dem Unternehmen können zum Verlust des Schlüsselwissens führen. • Damit das Wissen bei einem Ausfall nicht verloren geht, sollten wichtige Systeme und Prozesse dokumentiert werden. Das erleichtert auch den Nachfolgern und neuen Mitarbeitenden, sich schnell zurechtzufinden. • Bewahren Sie wichtige Passwörter im Doppel (z. B. in einem Safe) auf. • Sichern Sie die geschäftsrelevanten Daten von ausgeschieden Mitarbeitern.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar:	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

Tab. 1 18 Schritte zu besserer IKT-Sicherheit

3 Appendix

3.1 Abbildungsverzeichnis

3.2 Tabellenverzeichnis