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 4 Umsetzungsbeispiele

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

INHALTSVERZEICHNIS

Cyber Security Review der WV Musterdrei AG

Bericht zum Assessment entsprechend den Empfehlungen des IKT-Minimalstandards BWL/SVGW für Wasserversorger kleiner als 5000 Einwohner

Basierend auf dem IKT-Minimalstandard Wasserversorgung | Version 0.12, 2018 (Stand: 04.05.2018)

4 Umsetzungsbeispiel 3 (kleine Wasserversorgung)

Auditoren Team/Verfasser

Name	Vorname	Organisation	Funktion
Walder	Dario	BWL	Auditor/Projektleitung

Ansprechperson der Musterdrei AG

Name	Vorname	Organisation	Funktion
Sandra	Muster	WV Musterdrei AG	Brunnenmeisterin
Peter	Muster	WV Musterdrei AG	Ratsmitglied

Der Inhalt dieses Review-Berichts ist «~~VERTRAULICH~~» und richtet sich ausschliesslich an die WV Musterdrei AG.

Haftungsausschluss

Das vorliegende Dokument mit den Review-Resultaten entsprechend dem IKT-Minimalstandard BWL/SVGW (Stand 04.05.2018) wurde von den Auditoren nach bestem Wissen und Gewissen erstellt. Weder das Bundesamt für wirtschaftliche Landesversorgung (BWL) noch die involvierten Verbände (SVGW), Fachexperten und Unternehmen, auch kein Mitarbeitender oder das Auditoren Team, übernehmen eine Gewährleistung, weder ausdrücklich noch implizit. Die Haftung und Verantwortung für mögliche Schäden sowie für den sicheren Betrieb obliegt einzig den Anwendern.).

Zusammenfassung/Management Summary

Die Wirtschaftliche Landesversorgung[20] (WL) bzw. das Bundesamt für wirtschaftliche Landesversorgung sowie der Schweizerische Verein des Gas- und Wasserfaches empfehlen seit 2018 die Umsetzung des IKT-Minimalstandards für die Wasserversorgung. Für Wasserversorger mit einem Versorgungsgebiet von mehr als 5000 Einwohnern stehen ein umfassendes Cyber Security Framework (Anhang 2 zum IKT-Minimalstandard) sowie ein Excel-basiertes Assessment Tool zu dessen Umsetzung zur Verfügung. Die in diesem Review analysierte WV Musterdrei AG dagegen versorgt weniger als 5000 Einwohner und ist folglich angehalten, die vereinfachten Empfehlungen (18-Punkte-Programm) des Anhangs 3 zum IKT-Minimalstandard umzusetzen. Der hier vorliegende Bericht stellt die Resultate des Assessments anhand dieser Empfehlungen dar und bietet Handlungsempfehlungen zur Verbesserung identifizierter Schwachstellen.

Im Rahmen des hier vorliegenden Assessments wurde der Umsetzungsstand der WV Musterdrei AG hinsichtlich der im Rahmen des IKT-Minimalstandards BWL/SVGW empfohlenen 18 Punkte für kleine Wasserversorger erhoben. In dreizehn von 18 Punkten entspricht das Maturitätsniveau der WV Musterdrei AG den Empfehlungen des IKT-Minimalstandards. In fünf Punkten dagegen besteht Handlungsbedarf, um das empfohlene Sicherheitsniveau zu erreichen.

Die WV Musterdrei AG betreibt ihr Prozessleitsystem in der Betriebswarte selbst, hat aber alle sonstigen Services (z. B. E-Mail-Hosting) in die Cloud ausgelagert. Sowohl Cyber Security als auch der sichere Betrieb der Anlage werden von der WV Musterdrei AG aktiv angegangen. Das Review, entsprechend den Empfehlungen für Wasserversoger mit einem Versorgungsgebiet von weniger als 5000 Einwohnern, hat dies bestätigt. Dreizehn der insgesamt 18 Massnahmen für einen wirkungsvollen Schutz werden von der WV Musterdrei AG vollständig umgesetzt, respektive einhergehendes Risiko erkannt und akzeptiert. Bei fünf der Massnahmen dagegen wurde durch die nur teilweise Umsetzung noch folgender Handlungsbedarf identifiziert:

- Ein **regelmässiges Aktualisieren von Antivirus-Software** (nicht zuletzt auch auf den privaten Geräten mit Zugriff auf das Prozessleitsystem) sowie der Betriebssysteme.
- Das **Zuweisen von individuellen Accounts** mit starken Passwörtern, insbesondere auch für das Prozessleitsystem.
- **Testen der unterbruchfreien Stromversorgung** und nach Möglichkeit auch des Inselbetriebes (Betrieb der Wasserversorgung durch Verwendung des selbst produzierten Stromes).
- **Erarbeiten und umsetzen von Vorgaben** für den Gebrauch von mobilen Geräten mit Zugriff auf das PLS.
- **Regelmässige Überprüfung der Fortschritte bei der Umsetzung** der hier vorliegenden Empfehlungen sowie zyklisches Wiederholen eines Cyber Security Assessments entsprechend den Empfehlungen (Anhang 3) des IKT-Minimalstandards BWL/SVGW.

[20] Website der Wirtschaftlichen Landesversorgung: www.bwl.admin.ch [Stand 27.04.2018].

4.1 Übersicht WV Musterdrei AG

Die WV Musterdrei AG stellt den Haushaltungen sowie den Industrie- und Gewerbebetrieben Trink- und Brauchwasser zur Verfügung. Sie versorgt …[21] Einwohnerinnen und Einwohner. Daneben sorgt sie auch für die Bereitstellung von genügend Wasser für Feuerlöschzwecke.

Organisation
Die Wasserversorgung erfüllt ihre Aufgabe selbstständig und in eigener Verantwortung. Sie arbeitet mit anderen Gemeinwesen und Dritten, namentlich mit der Einwohnergemeinde …[22], zusammen, soweit es der zweckmässigen und wirtschaftlichen Erfüllung ihrer Aufgaben dient. Die Organisation ist …

Wassergewinnung
Der grösste Teil des Wassers wird von Quellen aus …[23] gewonnen.

IT Organisation
Die WV Musterdrei AG ist grösstenteils selbst organisiert und aus Sicht der IT nicht einer Gemeinde oder einem Kanton angeschlossen. Die WV Musterdrei AG unterhält ihr Prozessleitsystem selbst und mit der Unterstützung des Herstellers. Die Office-IT dagegen ist grösstenteils ausgelagert (z. B. E-Mail Services in der Cloud oder Data-Storage bei …[24] (Cloud)). Neben dem Server (Hardware) für das Prozessleitsystem betreibt die WV Musterdrei AG folglich keine weitere Hardware. Auch die Arbeitsgeräte für den Remote-Zugriff (z. B. Laptops) werden von den Mitarbeitenden selbst beschafft (BYOD[25]).

Die WV Musterdrei AG arbeitet eng mit der Wasserversorgung …[26] zusammen. Da die WV Musterdrei AG beschränkten Zugriff auf personelle Ressourcen hat, wurde im Rahmen des Pikettdienstes eine Zusammenarbeit mit der WV …[27] angestrebt. Letztere hat folglich einen dedizierten Zugriff auf das Prozessleitsystem der WV Musterdrei AG (und umgekehrt) und kann, wenn notwendig, steuernd eingreifen. Ein weiterer Aspekt bestehender Resilienzbestrebungen bildet der Anschluss an das Leitungsnetz (Wasser) der Wasserversorgungen …[28] sowie …[29]. Insbesondere die WV …[30] weist genügend Kapazität auf, um bei Störungen die WV Musterdrei AG ausreichend zu unterstützen. Die WV Musterdrei AG betreibt dazu (sowie für den Normalbetrieb im Winter) zwei eigene Pumpen in einem Pumpwerk der WV…[31].

[21] Aus Gründen der Vertraulichkeit werden keine Informationen publiziert, welche einen Rückschluss auf die untersuchte Organisation ermöglichen.

[22] Ibid.

[23] Ibid.

[24] Ibid.

[25] BYOD: Bring your own device. Damit ist hier insbesondere die Verwendung von privaten mobilen Geräten mit Zugriff auf das Prozessleitsystem verstanden.

[26] Aus Gründen der Vertraulichkeit werden keine Informationen publiziert, welche einen Rückschluss auf die untersuchte Organisation ermöglichen.

[27] Ibid.

[28] Ibid.

[29] Ibid.

[30] Ibid.

[31] Ibid.

4.2 Übersicht der Resultate

Die WV Musterdrei AG betreibt ihr Prozessleitsystem in der Betriebswarte selbst, hat aber alle sonstigen Services (z. B. E-Mail-Hosting) in die Cloud ausgelagert. Sowohl Cyber Security als auch der sichere Betrieb der Anlage werden von der WV Musterdrei AG aktiv angegangen. Das Review, entsprechend den Empfehlungen für Wasserversoger mit einem Versorgungsgebiet von weniger als 5000 Einwohnern, hat dies bestätigt. Dreizehn der insgesamt 18 Massnahmen für einen wirkungsvollen Schutz werden von der WV Musterdrei AG vollständig umgesetzt. Bei fünf der Massnahmen dagegen wurde durch die nur teilweise Umsetzung noch Handlungsbedarf identifiziert:

- **Massnahme 2 (Halten Sie Ihr Antivirus-Programm aktuell)**: Dieser Punkt wird von der WV Musterdrei AG nur teilweise umgesetzt. Insbesondere durch das BYOD-Konzept ist eine Policy hinsichtlich Antivirus nicht nur auf dem Prozessleitsystem (PLS), sondern auch auf den privaten Geräten notwendig. Die Handhabung von Antivirus auf dem Server in der Betriebswarte sowie allen weiteren Geräten (z.B. private Laptops mit Zugriff auf das PLS) soll schriftlich festgehalten und kommuniziert werden.
- **Massnahme 4 (Aktualisieren Sie Ihre Software regelmässig)**: Dieser Punkt wird von der WV Musterdrei AG nur teilweise umgesetzt. Schriftlich festgehaltene Vorgaben betreffend Betriebssystem für das PLS, aber auch die privaten Geräte der Mitarbeitenden mit Zugriff auf das PLS werden empfohlen.
- **Massnahme 5 (Verwenden Sie starke Passwörter)**: Dieser Punkt wird von der WV Musterdrei AG nur teilweise umgesetzt, insbesondere da das Betriebssystem des PLS-Servers zurzeit noch nur durch ein gemeinschaftliches Passwort geschützt wird. Der WV Musterdrei AG wird empfohlen, auch auf dem Windows-Betriebssystem für den PLS-Server individualisierte Passwörter für jeden Benutzer anzulegen.
- **Massnahmen 6 (Schützen Sie Ihre mobilen Geräte)**: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG nur teilweise umgesetzt, insbesondere da keine Vorgaben für die privaten Geräte der Mitarbeitenden bestehen, mit diesen aber auf das PLS zugegriffen werden kann. Erarbeiten und kommunizieren Sie klare Vorgaben zum regelmässigen Aktualisieren von Antivirus und sonstiger Software auf den mobilen Geräten mit Zugriff auf das PLS (siehe auch Handlungsempfehlung zu Punkt 4).
- **Massnahme 13 (Überprüfen Sie Ihre Systeme)**: Dieser Punkt wird von der WV Musterdrei AG nur teilweise umgesetzt. Ein Testen der USV wird noch nicht regelmässig durchgeführt. Ein Prozess für das regelmässige Testen der USV soll erstellt und entsprechend durchgeführt werden. Dieser Test könnte beispielsweise auch bei der Abnahme des neuen PLS gemeinsam mit dem Hersteller besprochen werden.

Im Folgenden werden die Resultate aus dem Cyber Security Review entsprechend dem IKT-Minimalstandard BWL/SVGW (Stand 20.05.2018) detailliert dargestellt:

	Massnahmen für einen wirkungsvollen Grundschutz[32]		
1.	**Sichern Sie Ihre Daten regelmassig mit Backups**		
	Datenverluste entstehen auf verschiedene Arten: Daten werden versehentlich überschrieben, Informationen auf einer Harddisk durch einen Defekt unleserlich oder ein Brand beziehungsweise ein Wasserschaden zerstört Ihre Daten. Solche Verluste können Sie mit regelmässigen Datensicherungen (Backups) vermeiden. • 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. • 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 z. B. bei Ransomware-Angriffen dar.		
	Umsetzungstand		
	Vollständig umgesetzt. Kommentar: Dieser Punkt wird entsprechend Grösse und vorhandenen Ressourcen der WV Musterdrei AG umgesetzt, jedoch ist beim Backup weiteres Optimierungspotenzial vorhanden, dem sich die Wasserversorgung, entsprechend ihrer vorhandener Ressourcen, widmen sollte.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Der Brunnenmeister ist dafür verantwortlich, dass regelmässig ein Backup durchgeführt wird. Dieses Backup von ihm persönlich jede Woche (freitags) angefertigt. Das Backup umfasst insbesondere Systemdaten des Prozessleitsystems. Gleichzeitig zum vor Ort durchgeführten Backup stellt auch der Systemhersteller ein Backup des Prozessleitsystems her. Die Art und Weise sowie der Umfang dieses Backups wurden durch die WV Musterdrei AG in einem Service-Level-Agreement (SLA) mit dem Hersteller definiert. Die Vollständigkeit des Backups wird durch den Betriebswart (oder den Brunnenmeister) visuell überprüft. Ein aktives Üben und gleichzeitiges Überprüfen des Backups sowie der Wiederherstellungsprozesse finden jedoch weder mit Hilfe des Herstellers noch selbständig statt. Für die Office-Daten (E-Mails, Verträge usw.) stehen Cloud-Lösungen zur Verfügung. Wichtige Dokumente, wie beispielsweise unterschriebene Verträge, werden im Archiv der Gemeinde gelagert. Davon wird jeweils eine elektronische Kopie erstellt, die auf eingekauften Cloud-Lösung gespeichert wird. Mit dem Cloud Provider sind SLA erarbeitet worden, welche die Art und Weise der Lagerung definieren. Handlungsempfehlung: • Um die Funktionalität des Backups, aber auch den Wiederherstellungsprozess zu prüfen und dessen korrektes Ablaufen auch im Krisenfall sicherzustellen, wird ein Üben des Wiederherstellungsprozesses empfohlen. Ideal wäre das Üben der Wiederherstellung durch das Backup. Als zusätzlicher Schritt kann der Wiederherstellungsprozess auch mit dem Hersteller besprochen und die entsprechenden SLA überprüft werden. Der Hersteller soll der WV Musterdrei AG versichern, dass er fähig ist, das Prozessleitsystem bei einer gröberen Störung innerhalb der entsprechend definierten Frist wiederherzustellen. • Die Aufgaben und Verantwortlichkeiten des Brunnenmeisters und des Brunnenwartes hinsichtlich Backups sollen schriftlich festgehalten und insbesondere bei Neueintritten kommuniziert werden.		

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

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: Dieser Punkt wird von der WV Musterdrei AG teilweise umgesetzt. Insbesondere durch das BYOD-Konzept ist eine Policy hinsichtlich Antivirus nicht nur auf dem PLS, sondern auch auf den privaten Geräten notwendig.	Nicht umgesetzt. Kommentar:
	Die WV Musterdrei AG betreibt einen eigenen Server für den Betrieb des Prozessleitsystems. Dieser Server ist nur über eine Firewall von ausserhalb der Betriebswarte zugänglich. Der PC in der Betriebswarte selbst wird durch ein Antivirus-Programm geschützt. Dieses wird täglich automatisch aktualisiert und die korrekte Funktionsweise durch den Betriebswart sichergestellt. Vier Personen (Betriebswart, Brunnenmeister, stellvertretender Brunnenmeister, Leiter Pumpwerke) haben von ihren privaten Geräten aus (z. B. Laptop) über VPN Zugriff auf das Prozessleitsystem. Es bestehen keine Vorgaben zur Aktualisierung des Antivirus auf den privaten Geräten. Handlungsempfehlung: • Die Handhabung von Antivirus auf dem Server in der Betriebswarte sowie allen weiteren Geräten (z. B. private Laptops mit Zugriff auf das PLS) soll schriftlich festgehalten und kommuniziert werden.		
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 für illegale Attacken auf Dritte miss-brauchen. Zudem gelangen sie an Geschäftsdaten, die eventuell dem Datenschutzgesetz unterstehen. • Im Handel sind Produkte erhältlich, die gleichzeitig eine Firewall und einen Virenschutz bieten. Gerade für kleinere Betriebe sind kombinierte Produkte sehr zu empfehlen. • 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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Die WV Musterdrei AG hat sich entschieden, eine Firewall für das Prozessleitsystem zu verwenden. Bei dieser ist lediglich ein einzelner Port geöffnet, während alle anderen geschlossen bleiben. Die Firewall-Konfiguration ist mit einem starken Passwort gesichert. Das Prozessleitsystem kann via VPN («über das Internet») erreicht werden. Dies ist jedoch jeweils nur über VPN (mit Login und starkem Passwort) und danach über Login (mit starkem Passwort) auf das Prozessleitsystem selbst möglich. Für alle anderen Dienstleistungen (z. B. Mail-Services von …[33] oder Cloud-Storage von …[34]) werden in den SLA entsprechende Sicherheitsniveaus definiert. Ausserdem betreibt die WV Musterdrei AG kein Wireless-LAN. Das Prozessleitsystem selbst verfügt (ausser über die definierten VPN-Schnittstellen) über keinen direkten Zugang zum Internet (z. B. über einen Web-Browser).		
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: Dieser Punkt wird von der WV Musterdrei AG teilweise umgesetzt. Insbesondere durch das BYOD-Konzept ist eine Policy hinsichtlich Antivirus nicht nur auf dem PLS sondern auch auf den privaten Geräten notwendig.	Nicht umgesetzt. Kommentar:
	Das Betriebssystem des Servers (Windows) wird regelmässig und automatisch aktualisiert. Dies wird monatlich vom Dienstwart überprüft. Das Prozessleitsystem dagegen wird weniger regelmässig aktualisiert. Die Software-Ebene des PLS wird in etwa alle drei bis vier Jahre aktualisiert (aus personellen und insbesondere finanziellen Gründen). Die Hardware-Komponenten des PLS dagegen werden in noch grösseren Abständen ersetzt (ca. alle 20 Jahre). Das Risiko, das mit diesem Punkt einhergeht, wird akzeptiert. Für die privaten Geräte der Mitarbeitenden dagegen, mit denen auf das PLS zugegriffen wird, bestehen keine Vorgaben betreffend Aktualisierung der Software (z. B. Betriebssystem, Antivirus). Handlungsempfehlung: • Schriftlich festgehaltene Vorgaben betreffend Betriebssystem für das PLS, aber auch betreffend die privaten Geräte der Mitarbeitenden mit Zugriff auf das PLS werden empfohlen.		

[33] Ibid.
[34] Ibid.

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: Dieser Punkt wird von der WV Musterdrei AG teilweise umgesetzt, insbesondere da das Betriebssystem des PLS-Servers zurzeit noch nur durch ein gemeinschaftliches Passwort geschützt wird.	Nicht umgesetzt. Kommentar:
	Die WV Musterdrei AG verwendet sowohl für das PLS als auch für die Office-IT individuelle Passwörter. Aktuell besteht jedoch für das Betriebssystem (Windows) ein einziges, gemeinsam verwendetes Passwort. Es ist vorgesehen, auch für das Betriebssystem individualisierte Passwörter anzulegen (noch im Juni 2018). An der Brunnenmeistertagung informierte sich der Brunnenmeister der WV Musterdrei AG über Cyber Security und hob darauf basierend die Komplexität der Passwörter an. Jetzt entsprechen die Passwörter neuesten Empfehlungen entsprechend den Inputs aus der Brunnenmeistertagung. Handlungsempfehlung: • Der WV Musterdrei AG wird empfohlen, auch auf dem Windows-Betriebssystem für den PLS-Server individualisierte Passwörter für jeden Benutzer anzulegen.		
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 (s. 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 (Hot Spots) 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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt, insbesondere da keine Vorgaben für die privaten Geräte der Mitarbeitenden bestehen, mit diesen aber auf das PLS zugegriffen werden kann.	Nicht umgesetzt. Kommentar:
	Mit den privaten mobilen Geräten von drei Mitarbeitenden der WV Musterdrei AG und eines Mitarbeiters der WV …[35] kann auf das PLS zugegriffen und steuernd eingegriffen werden. Im Rahmen des Pikettdienstes besteht ein Vertrag zur Zusammenarbeit mit der WV …[36]. Grundsätzlich werden keine Daten auf den privaten Geräten gespeichert, sondern in den zur Verfügung gestellten Cloud-Lösungen. Es bestehen jedoch keine Vorgaben hinsichtlich Cyber Security (z. B. betreffend Passwörter) für die Mitarbeitenden. Handlungsempfehlung: • Erarbeiten, kommunizieren und überprüfen Sie klare Vorgaben (z. B. starke Passwörter) für den Zugriff über VPN, auf das PLS sowie für die Cloud-Lösungen. • Erarbeiten und kommunizieren Sie klare Vorgaben zum regelmässigen Aktualisieren von Antivirus und sonstiger Software auf den mobilen Geräten mit Zugriff auf das PLS (siehe auch Handlungsempfehlung Punkt 4).		
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 der 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 mit der internen Post, Plakate in der Kantine, Beiträge in der Firmenzeitung usw. • Organisieren Sie eine Basisausbildung für alle Mitarbeitenden (z. B. auf der Gundlage dieser Broschüre). Die wichtigsten Lernziele sind: – Nutzen der IKT-Sicherheit – Bestimmen starker Passwörter – sicherer Umgang mit Internet, E-Mail und Virenschutz – Ablagestruktur von Dokumenten • Regeln Sie – Installation und 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, Weiterleitung, 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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

[35] Aus Gründen der Vertraulichkeit werden keine Informationen publiziert, die Rückschluss auf die untersuchte Organisation ermöglichen.

[36] Ibid.

	Bei Anstellung und Auflösung des Arbeitsverhältnisses wird der Mitarbeitende auf die Datensicherheit und Vertraulichkeit hingewiesen. Dies wird im Arbeitsvertrag schriftlich festgehalten. Die Möglichkeiten zur Installation von Software auf dem PLS ist sehr beschränkt, nur dem Systemadministrator ist dies möglich. Auf den privaten Geräten dagegen sind keine Vorgaben für den sicheren Umgang festgehalten. Der Brunnenmeister informiert sich regelmässig (z. B. an der Brunnenmeistertagung) über aktuelle Themen im Bereich Cyber Security und setzt neue Empfehlungen entsprechend um. Für den Fernzugriff der WV …[37] ist Cyber Security im Pikettvertrag geregelt.		
8.	**Schützen Sie die Umgebung Ihrer IKT-Infrastruktur**		
	Wissen Sie, wer in Ihrem Unternehmen tagsüber ein- und ausgeht? Einige wenige Vorkehrungen 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 Büroteil 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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Der Steuerungsraum (mit dem PLS-Server) ist gegen physisches Eindringen unberechtigter Personen geschützt. Die Eingangstüre ist verstärkt und mit einbruchsicheren Gitterstäben versehen. Auch die Fenster und Lüftungsschächte sind durch einen Einbruchschutz geschützt. Ausserdem ist der Steuerungsraum alarmgesichert. Die Zugangsschlüssel für den Steuerungsraum werden entsprechend dem «Least-to-know-Prinzip» lediglich an vier berechtigte Personen vergeben.		

[37] Aus Gründen der Vertraulichkeit werden keine Informationen publiziert, die einen Rückschluss auf die untersuchte Organisation ermöglichen.

	Massnahmen für mehr Vertraulichkeit		
9.	**Regeln Sie den Zugriff auf Daten**		
	Durch unbefugten Zugriff können Informationen missbraucht werden. Schützen Sie deshalb den Datenzugriff entsprechend, so dass 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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Der Zugriff auf die Daten wird entsprechend einem Rechtekonzept geregelt. Leserechte werden dabei grosszügiger vergeben als Schreibrechte. Es bestehen individuelle Zugriffsrechte für das PLS sowie die Cloud-Lösungen (E-Mail usw.). Für die Cloud-Lösung besteht ausserdem die Möglichkeit der Wiederherstellung von mutwillig oder unachtsam gelöschten Daten. Die Administratorenrechte werden strikte gehandhabt und sind nur an drei Parteien vergeben (Brunnenmeister und Stv., Betriebswart). Der Hersteller schult die WV Musterdrei AG hinsichtlich der Vergabe von Rechten. Die Vergabe der Rechte geschieht durch den Betriebswart.		
10.	**Verschlüsseln Sie mobile Datenträger**		
	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, welche zusätzlich mit einem Virtual Privat Network (VPN) geschützt sind (siehe auch Punkt 6).		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt bzw. die damit einhergehenden Risiken werden akzeptiert.	Vollständig umgesetzt. Kommentar:	Vollständig umgesetzt. Kommentar:
	Mobile Geräte (z. B. BYOD) werden nicht verschlüsselt. Die WV Musterdrei AG hat diesen Entscheid bewusst getroffen und akzeptiert die damit einhergehenden Risiken. Die Daten aus dem PLS werden nur über einen dedizierten Port der Firewall und über eine VPN-Verbindung übermittelt und sind damit geschützt. Auch die Daten in der Cloud werden von der WV Musterdrei AG nicht aktiv verschlüsselt. Die einhergehenden Risiken sind jedoch akzeptiert.		

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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Bei Anstellung und Auflösung des Arbeitsverhältnisses wird der Mitarbeitende auf Datensicherheit und Vertraulichkeit hingewiesen. Dies wird im Arbeitsvertrag schriftlich festgehalten. Mitarbeitende müssen diese Dokumente lesen und unterschreiben. Dieser Prozess ist gut etabliert und wird eingehalten.		
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, Werbung 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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Für die Entsorgung von Datenträgern wird der Hersteller beauftragt.		

	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: Dieser Punkt wird von der WV Musterdrei AG teilweise umgesetzt. Ein Testen der USV wird noch nicht regelmässig durchgeführt.	Nicht umgesetzt. Kommentar:
	Für die regelmässigen Wartungsarbeiten ist der Betriebswart beauftragt worden. Dieser überprüft regelmässig die Systemprotokolle sowie die Statusmeldung der USV (unterbruchfreie Stromversorgung). Auch die Integrität der Backups wird regelmässig durch den Betriebswart überprüft. Ein Testen der USV und des Backups wird jedoch nicht regelmässig durchgeführt, könnte jedoch insbesondere für die USV ohne grösseren Aufwand durchgeführt werden. Handlungsempfehlung: • Ein Prozess für das regelmässige Testen der USV soll erstellt und letztere entsprechend getestet werden. Dieser Test könnte beispielsweise auch bei der Abnahme des neuen PLS gemeinsam mit dem Hersteller besprochen werden. • Betreffend Backup siehe Handlungsempfehlung zur Massnahme 1 (Sichern Sie Ihre Daten regelmässig mit Backups).		
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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Es stehen klar definierte Zugriffsvarianten zur Verfügung, die für das PLS und die restliche Office-IT unterschiedlich aussehen. Um auf das PLS zugreifen zu können, müssen mindestens zwei verschiedene Schritte durchlaufen werden. Erstens muss via VPN (oder lokal in der Betriebswarte) auf den PLS-Server zugegriffen werden. Dieser Zugriff ist jeweils passwortgeschützt. Danach erst kann auf		

	die Software des PLS selbst zugegriffen und damit steuernd eingegriffen werden. Auch dieser Schritt ist erneut passwortgeschützt. Auch für das Support-Personal wurden klare Regeln festgelegt (vertraglich mit den Cloud-Anbietern sowie dem Hersteller des PLS). Es ist immer möglich, Handlungen einer bestimmten Person zuzuweisen und somit die Nachvollziehbarkeit sicherzustellen. Handlungsempfehlung: • Bei der Abnahme des PLS sollen die Systemzugriffe sowie eine entsprechende Authentifizierung erneut mit dem Hersteller besprochen und damit erneut bestätigt werden.		
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 einem 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 Peripheriegeräte 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: Dieser Punkt wird von der WV Musterdrei AG vollständig umgesetzt. Ein Testen des Inselbetriebes wird noch nicht regelmässig durchgeführt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Für das Prozessleitsystem steht eine USV zur Verfügung, die den Betrieb der Anlage während rund einer Stunde sicherstellt. Danach müsste diese heruntergefahren werden. Die Wasserversorgung selbst könnte jedoch auch dann noch sichergestellt werden. Denn durch das natürliche Gefälle der Wassergewinnung ist lediglich eine Stromversorgung für die UV-Aufbereitungsanlage notwendig. Für letztere steht ein Notstromaggregat zur Verfügung. Alle weiteren Prozesse könnten noch von Hand (manuell) bedient werden. Ausserdem ist mit der Wasserversorgung …[38] vertraglich festgelegt, dass diese in einem Ereignisfall aushelfen wird. Dazu ist die WV Musterdrei AG mit einem Pumpwerk der WV …[39] verbunden, in dem Sie über eine eigene Pumpe verfügt. Die WV Musterdrei AG könnte grundsätzlich durch die eigene Stromproduktion in einen Inselbetriebszustand wechseln, dies wurde jedoch seit längerem nicht mehr getestet. Handlungsempfehlung: • Der Inselbetrieb mit eigener Stromproduktion soll entsprechend dem eigenen Notfallkonzept und nach Möglichkeiten regelmässig getestet werden (Betrieb der UV-Anlage mit selbst produziertem Strom).		
16.	**Halten Sie wichtige Elemente redundant**		
	Der Ausfall eines kritischen Elements in Ihrem Netzwerk wie beispielsweise 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, welches 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.		

[38] Aus Gründen der Vertraulichkeit werden keine Informationen publiziert, die einen Rückschluss auf die untersuchte Organisation ermöglichen.

[39] Ibid.

	• 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 sind und bereits vorkonfiguriert sind, damit sie im Ereignisfall sofort eingesetzt werden können.		
	Umsetzungsstand		
	Vollständig umgesetzt. Kommentar: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Für den Server zum Betrieb des PLS stehen gewisse Komponenten redundant zur Verfügung (z. B. Netzwerkkarte, Harddisk) Ausserdem wurde für das PLS ein SLA vereinbart, das den Ersatz von ausgefallenen Komponenten in vorgegebener Zeit sicherstellt. Für die Cloud-Lösungen werden dementsprechend keine Komponenten redundant gehalten. Dieser Aspekt ist im SLA abgedeckt. Einhergehende Risiken werden akzeptiert, da auch bei einem Ausfall der Office-IT oder des PLS die Kernprozesse noch manuell aufrechterhalten werden können. Dazu wird lediglich Strom für die UV-Aufbereitungsanlage benötigt.		
17.	**Planen Sie die Notfallvorsorge**		
	Ein existenzbedrohender Notfall tritt meistens plötzlich ein. Besonders höherer Gewalt ist man schutzlos aus-geliefert. 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 oder 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, die 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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:

	Die WV Musterdrei AG hat entsprechend den erkannten Risiken ein Notfallkonzept erarbeitet und mit dem Hersteller vertraglich Reaktionszeiten festgelegt. Ausserdem wurde mit der WV …[40] ein Anschluss an das eigene Leitungsnetz erstellt. Die WV …[41] ist zusätzlich an die WV …[42] angeschlossen und kann dort im Notfall ebenfalls Wasser beziehen. Mit der WV …[43] wurde ein Pikettvertrag abgeschlossen. Ausserdem stehen für den Ausfall des PLS Notfallprozesse zur Verfügung, wodurch die Wasserversorgung aufrechterhalten werden kann. Sowohl von …[44] als auch von …[45] könnte ganz ohne Stromversorgung noch Wasser an die WV Musterdrei AG geliefert werden.		
18.	**Verteilen Sie das Know-how**		
	Gerade bei 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 im 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: Dieser Punkt wird entsprechend der Grösse und vorhandenen Ressourcen der WV Musterdrei AG vollständig umgesetzt.	Teilweise umgesetzt. Kommentar:	Nicht umgesetzt. Kommentar:
	Die WV Musterdrei AG betreibt durch die beschränkte Grösse der Gemeinde ihre Wasserversorgung mit wenig Personal. Der Brunnenmeister hat keinen direkten Stellvertreter und verfügt über sehr viel Fachwissen. Sein Ausfall könnte jedoch durch den Pikettvertrag mit der WV …[46] überbrückt werden. Mit der WV …[47] wird ein regelmässiger Know-how-Austausch sichergestellt. Im Notfall könnte auch der Hersteller des Prozessleitsystems die Arbeiten des Betriebswartes behelfsmässig überbrücken. Dies wäre jedoch eine ad-hoc Massnahme. Ein Ausbau dieser Kooperationsmassnahme ist nicht vorgesehen und das einhergehende Risiko wird akzeptiert.		

Tab. 1 18 Schritte zu besserer IKT-Sicherheit

[40] Aus Gründen der Vertraulichkeit werden keine Informationen publiziert, welche einen Rückschluss auf die untersuchte Organisation ermöglichen.

[41] Ibid.

[42] Ibid.

[43] Ibid.

[44] Ibid.

[45] Ibid.

[46] Ibid.

[47] Ibid.

4.3 Schlussfolgerungen

Cyber Security Vorfälle, ob absichtlich oder durch Fehlmanipulationen, können vernichtende Auswirkungen auf die Wasserversorgung haben. Sowohl das Prozessleitsystem als auch die Aufbereitungsanlage bilden bei vielen Wasserversorgungen wesentliche Schwachstellen. Dabei spielt es oftmals keine Rolle, ob die Wasserversorgung mehrere zehntausend oder lediglich …[48] Einwohner mit Trinkwasser versorgt. Wie auch durch dieses Review eindrücklich bestätigt, bilden Resilienzmassnahmen (z. B. in Form eines Notfallkonzeptes, eines Inselbetriebs oder der Zusammenarbeit mit umliegenden Wasserversorgern) einen essentiellen Teil der Cyber Security-Strategie und die WV Musterdrei AG hat dies entsprechend umgesetzt.

Die WV Musterdrei AG hat sich trotz beschränkt vorhandener Ressourcen durch zahlreiche Massnahmen für Notsituationen vorbereitet. Hierzu gehören neben einer Pikettorganisation, USV, Notfallkonzept, Inselbetrieb sowie Zusammenarbeit mit umliegenden WV auch eine Aufrechterhaltung der Kernprozesse ohne das PLS (durch manuellen Betrieb). Trotzdem sind noch nicht alle Empfehlungen entsprechend Anhang 3 des IKT-Minimalstandards umgesetzt. Der hier vorliegende Review-Bericht und insbesondere die darin enthaltenen Handlungsempfehlungen ermöglichen der WV Musterdrei AG die Einhaltung dieser Empfehlungen und stellen damit einen weiteren Schritt hinsichtlich des sicheren Betriebes der Wasserversorgung dar.

[48] Ibid.