step by STEP

IKT-Minimalstandard Abwasser

Erstausgabe Juni 2019

Aktualisiert März 2021

https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/abwasser.html

Einleitung

Reto Steinemann / Melchior Zimmermann / Max Schachtler

Adaption Minimalstandard Abwasser

Von der Theorie zu den Praktikern überführen

- Regelt Verantwortungen
- Checklisten für Eigenanalyse beurteilen des Schutzes
- Handlungsanweisungen

Cybersicherheit

IKT Minimalstandard Abwasser

Zielsetzungen

Vor Ereignisfall	Situationen kennen → Stärken / Schwächen
Im Ereignisfall	Vorbereitet handeln → Handlungsanweisungen
Qualität	vermeiden von Folge-Ereignissen Einfache Handhabung
Nachführung	Periodisch
Praxistauglich	von Praktikern für Praktiker OT (PLS) und IT (Verwaltung)
Umsetzung	step by STEP gibt gesammelte Erfahrungen weiter

Referenten

Reto Steinemann – Chestonag Automation AG

- Seit 2003 in der Chestonag Automation AG
- Elektrotechnik HF / DAS ICT
- Diverse Automationsprojekte realisiert (ARA & Industrie)
- Leiter Entwicklung / Mitglieder der GL

chestonag automation

Referenten

Melchior Zimmermann – Pictet

- Seit Oktober 2020 Cyber-Security Analyst bei Pictet
- 2019 GRID
- 2018 GSEC & GIAC Advisory Board member
- 2017 – 2020 Entwickler & IT-Sicherheits-experte, Chestonag Automation AG
- Master in Biologie und Informatik, Universität Genf

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für Wirtschaftliche Landesversorgung BWL
Fachbereich IKT

IKT-Minimalstandard Abwasser

Einführung in das Handbuch und Erklärung der Funktionsweise

Sven PETER
Projektleiter NCS
Bundesamt für wirtschaftliche Landesversorgung BWL
Fachbereich IKT

Vorstellung

Sven Peter

Berufsausbildung
- Bachelor Universität Neuchâtel: Wirtschaftswissenschaften
- Master Universität Freiburg: Informations- und Kommunikationstechnologie
- Projektmanagement-Praktikum bei Tamedia
- Seit 2 Jahren Projektleiter NCS bei BWL

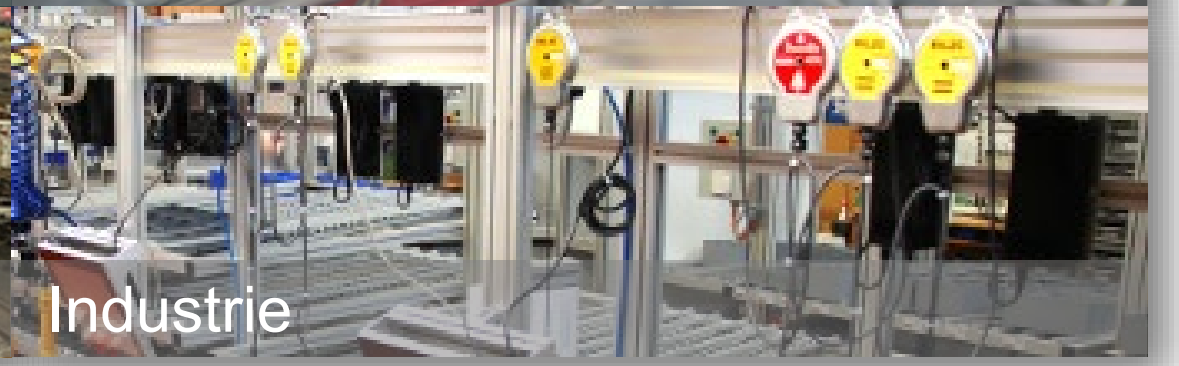
Projekte im BWL
- Unterstützung bei der Veröffentlichung für :
  - IKT-Minimalstandard Trinkwasser
  - IKT-Minimalstandard Abwasser
  - IKT-Minimalstandard ÖV
- Projektleiter für den IKT-Minimalstandard Gas
- Neue Projekte: Projektleiter für IKT-Minimalstandard Fernwärme + Logistikterminal

Kontakt
- Tel: +41 58 483 93 75
- E-Mail: sven.peter@bwl.admin.ch

Auftrag

- **Bundesverfassung Art. 102**
- **Bundesgesetz über die Wirtschaftliche Landesversorgung**
- **Art. 1, Zweck:**
  Dieses Gesetz regelt die vorsorglichen Massnahmen […] zur Sicherstellung der Landesversorgung mit lebenswichtigen Gütern und Dienstleistungen

Organisation des BWL



WL : Public Private Partnership

Bund
35 Leuten

BWL
Bundesverwaltung
Geschäftsleitung

Delegierter
Werner Meier

Rolf Enggist
Interne Revision

Regula Rutz
Kantone &
Kommunikation

Alfred Flessenkämper
Stv. Direktor

Patrick Rötheli
Geschäftsstellen
Energie & Industrie

Franz Flütsch
Recht & Compliance

Dr. Ueli Haudenschild
Geschäftsstellen
Ernährung & Heilmittel

Peter Lehmann
Sektion
Vorratshaltung

Dr. Ruedi Rytz
Geschäftsstellen
Logistik & IKT

WL Fachbereiche
Kaderorganisation der Wirtschaft
Leiter Fachbereiche

vakant
Energie

Christian Hofer
Ernährung

Andreas Jeppesen
Logistik

Urs Näf
Industrie

Prof. Stefan Mühlebach
Heilmittel

Marcel von Vivis
IKT

Wirtschaft
250 Leuten

Aufgabenteilung Cyber im Bund

Aufgaben:

- Verteidigung (Cyberdefence)
- Strafverfolgung (Cybercrime)
- Schutz kritischer Infrastrukturen (Cybersecurity)

Organisation :

- Organisatorische Trennung, aber enge Zusammenarbeit und gegenseitige Absprache.

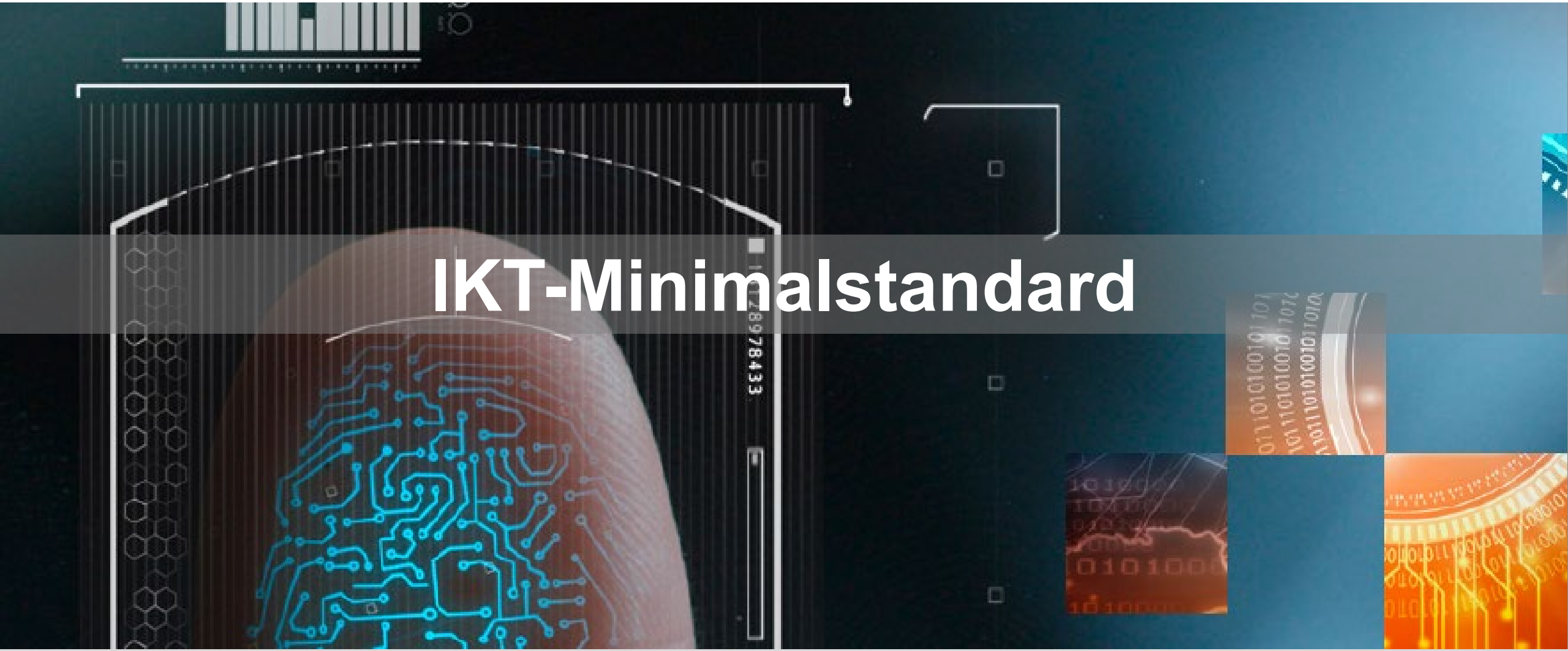
Strategie zum Schutz der Schweiz vor Cyberrisiken NCS

- Der Bundesrat hat 2012 die «Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken» beschlossen (NCS).
- Das BWL hat seither Verwundbarkeitsanalysen in 13 kritischen Teilsektoren durchgeführt und Massnahmen vorgeschlagen.
- Der vorliegende Minimalstandard ist eine präventive Massnahme zur Stärkung der IKT-Resilienz im Sinne der NCS.
- Im Jahr 2018 hat der Bundesrat die zweite nationale Strategie mit neuen Zielen für das BWL beschlossen.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für Wirtschaftliche Landesversorgung BWL
Fachbereich IKT



IKT-Minimalstandard

Beispiele für Cyberangriffe auf verschiedene Sektoren

ICTjournal

NEWS

Infrastructures critiques

Un hacker a failli empoisonner l'eau potable d'une ville de Floride

Mer 10.02.2021 - 16:44
par Rodolphe Koller

Via TeamViewer, un pirate est parvenu à augmenter la teneur en soude caustique dans l'eau d'une petite ville de Floride. Plus de peur que de mal, puisqu'un employé a pu rapidement annuler le changement dans le système de traitement.

Blick TV News Sport Meinung Politik Wirtschaft People Green Mehr

Urheber in London und Korea

Hacker-Attacke auf Wasserversorgung in Ebikon LU

Die autonome Betriebssteuerung der Wasserversorgung der Gemeinde Ebikon LU hat im November Tausende bösartige Software-Anfragen bekommen.

netzwoche

NEWS

Grosser Cyberangriff

Hacker erbeuten 30'000 Passwörter von Suisse Velo

Mo 13.09.2021 - 09:57 Uhr
von Oliver Wietlisbach, Watson

Suisse Velo, Anbieterin der "Suisse Velo Vignette" und weiteren Dienstleistungen rund ums Velo, ist das neuste Hacking-Opfer in der Schweiz. Die Täter erbeuteten rund 30'000 E-Mail-Adressen und Passwörter.

LA CÔTE PREMIUM

RÉGIONS SUISSE SPORTS ECONOMIE MONDE SORTIR LIFESTYLE DOSSIERS PREMIUM

Piratage: Rolle s'explique sur les milliers de données volées et publiées sur le darknet

PIRATAGE Le piratage informatique qu'a subi la commune est plus grave que ce qui a été présenté la semaine passée. Une majorité des Rollois sont concernés. En exclusivité, la commune s'explique et reconnaît "une certaine naïveté". Elle détaille les mesures pour aider les citoyens.

PAR GREGORY BALMAT, LAURA LOSE 26.08.2021, 05:00
LECTURE: 7MIN

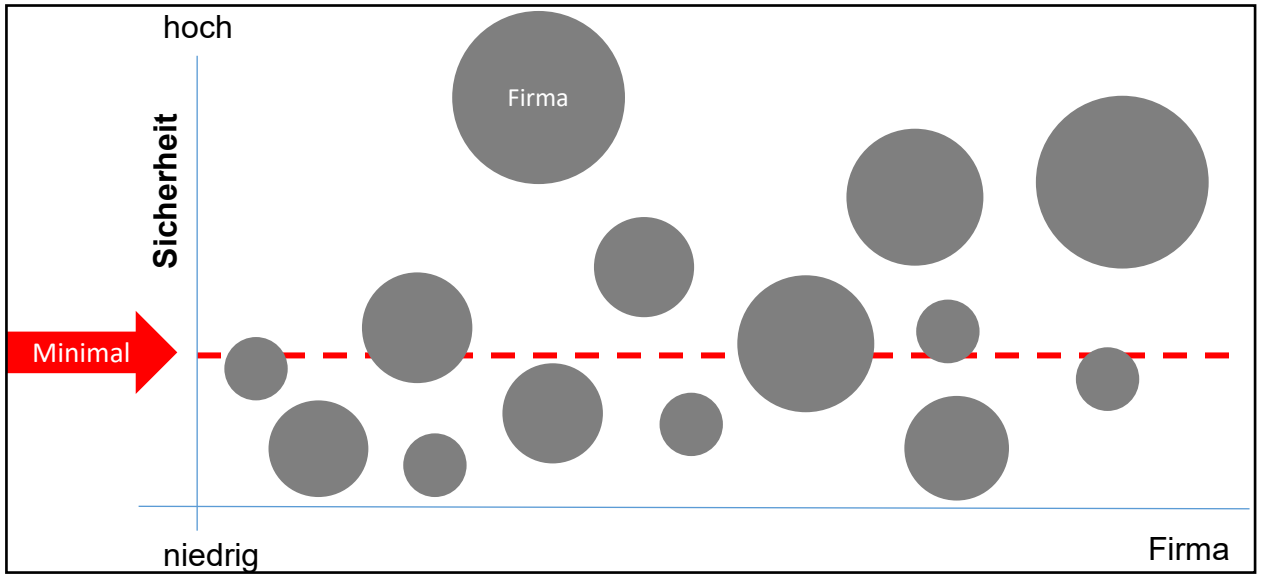
PREMIUM

Quellen:
Un hacker a failli empoisonner l'eau potable d'une ville de Floride | ICTjournal
Hacker-Attacke auf Wasserversorgung in Ebikon LU – Blick
Hacker erbeuten 30'000 Passwörter von Suisse Velo | Netzwoche
Piratage: Rolle s'explique sur les milliers de données... (lacote.ch)

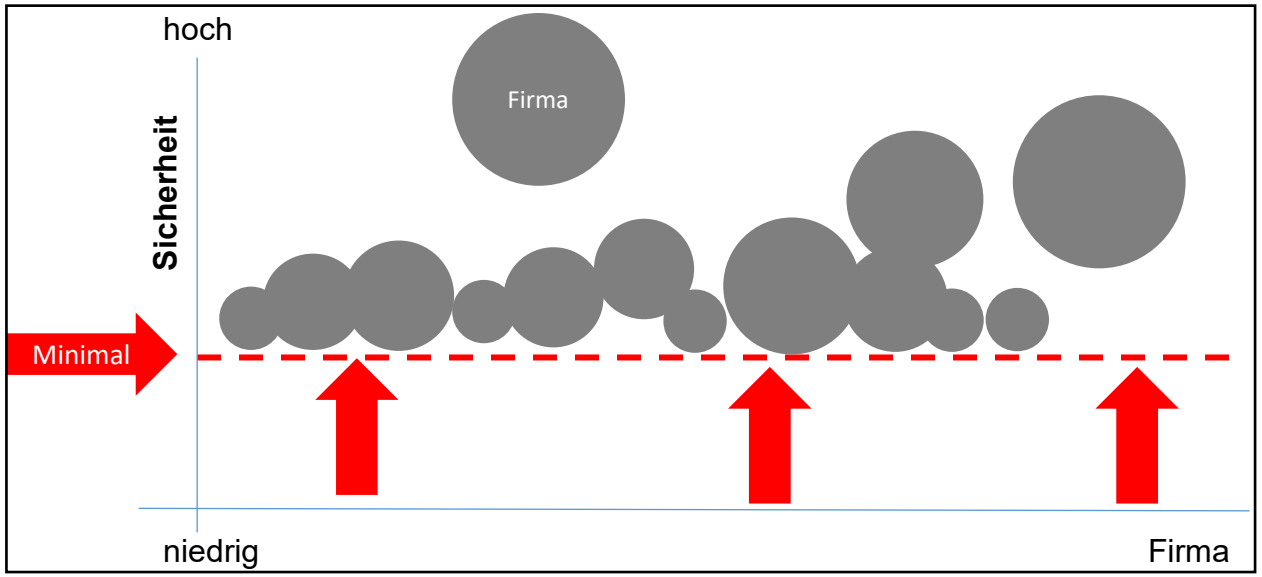
IKT-Minimalstandard

- Der Standard ist universell einsetzbar
- Der primäre Fokus liegt auf kritischen Infrastrukturen
- Der Standard ist eine Empfehlung
- Der Standard gibt vor, *was* zu tun ist, lässt dem Anwender aber die Freiheit zu entscheiden, *wie* er es tun möchte
- Der Standard ist kompatibel mit internationalen Industriestandards, wie z.B. ISO, ISA, BSI, COBIT-Standards…

Ziel des MINIMALstandards

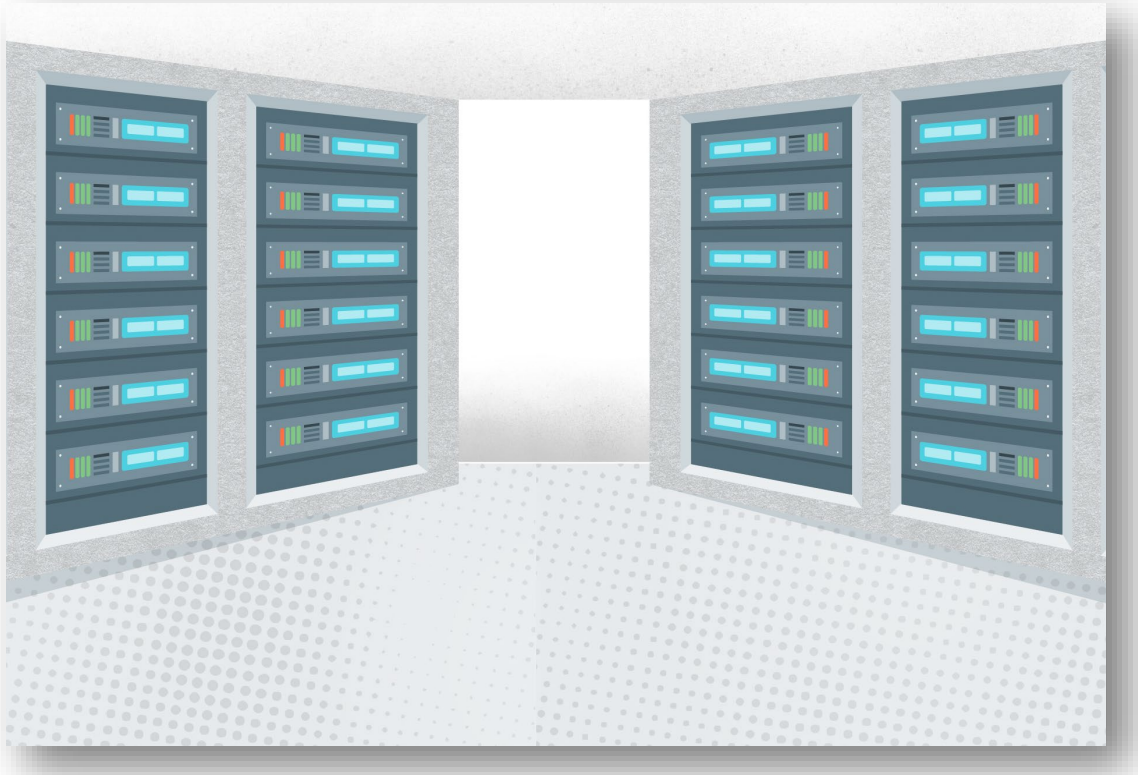


- Aktuelle Vision des betreffenden Sektors



- Vision des Sektors nach Anwendung des IKT-Minimalstandards

Ziele des Standards



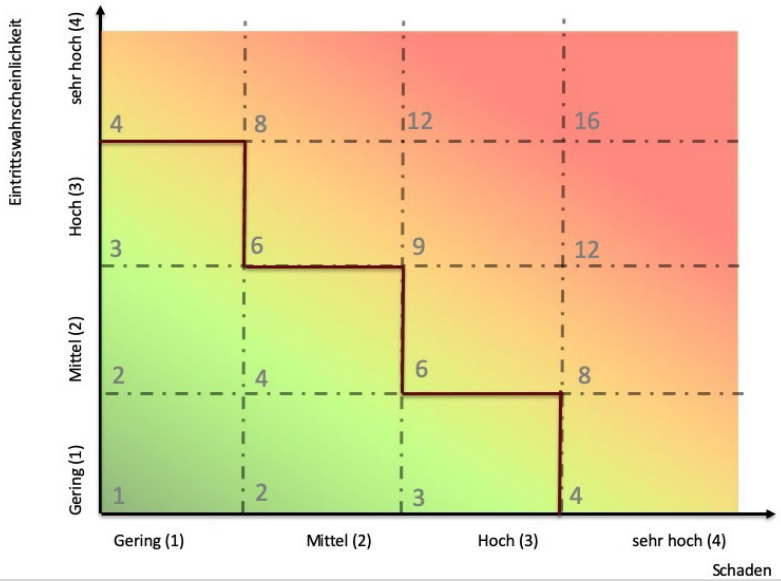
- Das im Cybersicherheitsprogramm des IKT-Minimalstandards enthaltene Massnahmenpaket zielt darauf ab, das Sicherheitsniveau mindestens einer der drei Cybersicherheits-säulen zu verbessern.

Wie funktioniert der Standard?

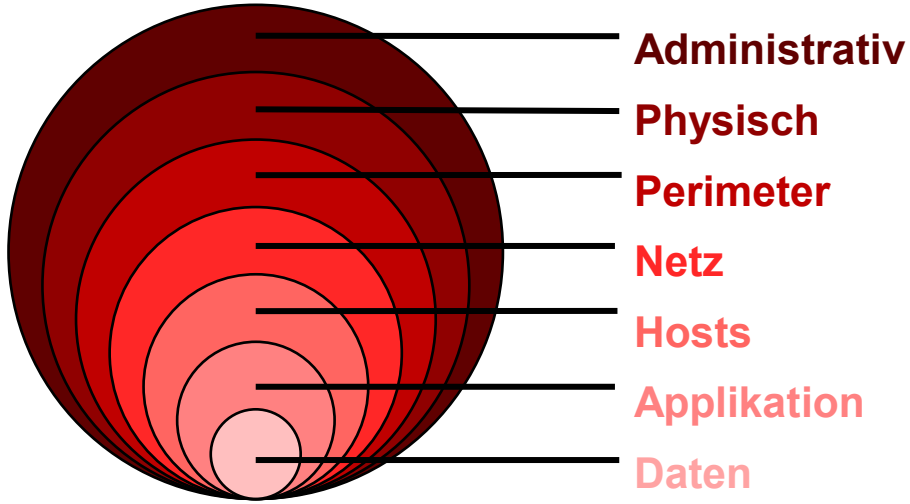
- Der IKT-Minimalstandard basiert auf dem NIST Framework Core, der vom National Institute of Standards and Technology entwickelt wurde.
- Die Massnahmen des NIST Framework Core basieren auf zwei Konzepten:
  - ein risikobasierter Ansatz
  - die Defense-in-depth Strategie
- Letztendlich besteht der IKT-Minimalstandard aus 106 Massnahmen, die in 5 Kapitel unterteilt sind.
- Zu jedem Kapitel empfiehlt der Standard spezifische Aktivitäten.

Konzepte: Risikobasierter Ansatz und die Defense-in-depth Strategie

- **Die Analyse des akzeptablen Risikos** ist für eine Organisation essentiell, da sie es ihr ermöglicht, die Massnahmen des NIST Framework Core nach ihren eigenen Bedürfnissen (abhängig von ihrer Branche, Grösse, Ressourcen und Bedrohungen) umzusetzen. Nach dieser Analyse ist jede Organisation in der Lage, je nach ihren Ressourcen das optimale Schutzniveau zu bestimmen.



- **Die Defense-in-Depth-Strategie** leitet sich aus dem militärischen Prinzip ab, dass ein komplexes, mehrschichtiges Verteidigungssystem schwerer zu durchbrechen ist als eine einzelne Barriere. Ziel dieser Strategie ist es daher, mehrere Sicherheitsmassnahmen auf unterschiedlichen Schutzebenen anzuwenden und so den Angreifer zu zwingen, eine Vielzahl von komplexen Sicherheitsbarrieren zu überwinden.



Kurzbeschreibungen der 5 Funktionen

Identifizieren: Das Ziel der Massnahmen dieser Funktion ist es, alle Elemente, die mit IKT in der Organisation zusammenhängen, sowie die Cyber-Risiken, die sie betreffen können, aufzulisten. Dazu gehört ein " Inventar" der Systeme, Verfahren, Ressourcen, Mitarbeiterverantwortlichkeiten und Vermögenswerte der Organisation. Sobald alle IKT-Elemente inventarisiert sind, ist es einfacher, sie durch die Implementierung der entsprechenden Sicherheitsverfahren effektiv zu schützen.

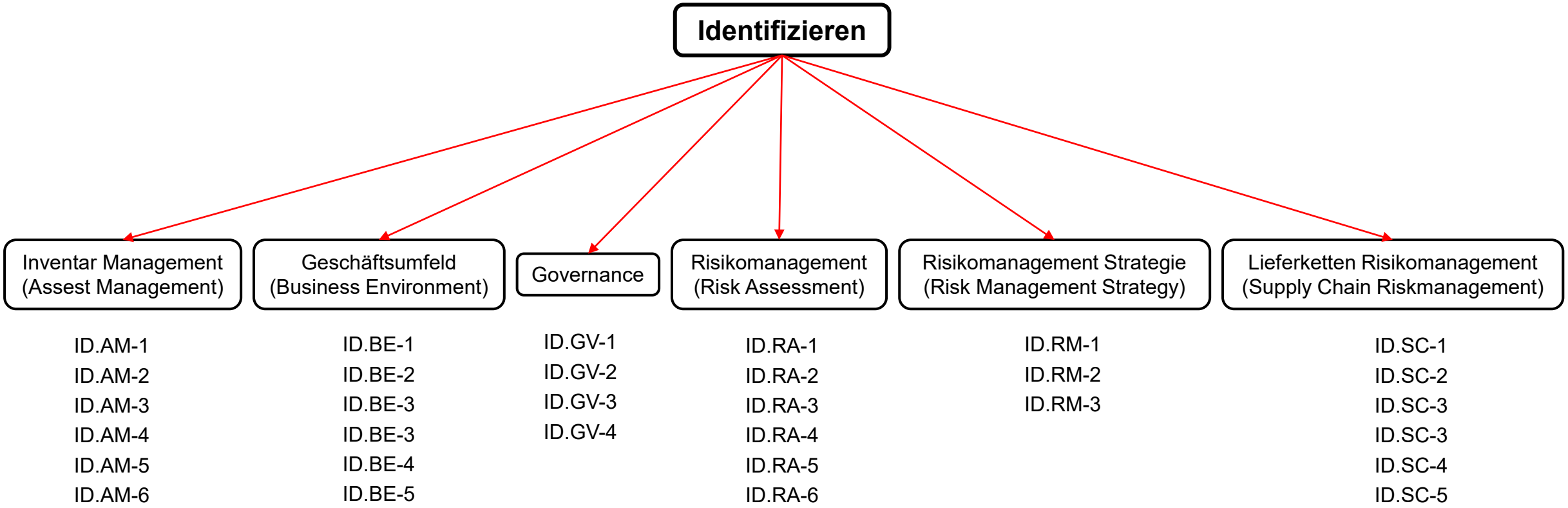
Schützen: Diese Funktion umfasst Massnahmen zur Gewährleistung eines angemessenen Schutzes und von Sicherheitskontrollen für alle IKT-Ressourcen der Organisation. Dies betrifft vor allem technische Prozesse (Anti-Virus, DMZ, Netzwerkarchitektur usw.), aber auch Elemente wie das Bewusstsein für Cyberrisiken unter Mitarbeitenden. Ziel ist es, den Schaden, der durch eine potenzielle Bedrohung entsteht, zu vermeiden oder zu begrenzen

Erkennen: Sobald die IKT-Elemente identifiziert und die entsprechenden Schutzmassnahmen angewendet wurden, ist eine kontinuierliche Überwachung der Sicherheit der Infrastruktur erforderlich. Ziel dieser Funktion ist es, ein effektives und zielgerichtetes Überwachungssystem für IKT-Elemente zu implementieren, um Bedrohungen frühzeitig zu erkennen und so die Auswirkungen eines Cybervorfalls zu vermeiden oder abzumildern.

Reagieren: Innerhalb dieser Funktion werden Massnahmen ergriffen, um Sicherheitsverfahren anzupassen, wenn Cyber-Bedrohungen erkannt werden. Das Ziel ist es, angemessen auf einen Cybervorfall zu reagieren und gleichzeitig die Auswirkungen auf das Unternehmen zu minimieren. Idealerweise sollten detaillierte und genehmigte Verfahren vorhanden sein, um den Vorfall so effizient wie möglich zu lösen.

Wiederherstellen: Diese Funktion beinhaltet Massnahmen zur Wiederherstellung aller Fähigkeiten, die durch einen Cybersecurity-Vorfall beeinträchtigt wurden. Es geht um die Anwendung von Resilienzplänen zur Wiederherstellung der Infrastruktur der Organisation, damit diese schnell wieder einen normalen Arbeitsrhythmus aufnehmen kann. Diese Funktion ist von entscheidender Bedeutung, damit die IKT-Elemente eines Unternehmens auf einer soliden Basis neu gestartet werden können und somit die Auswirkungen eines Cybersicherheitsvorfalls reduziert werden.

Beispiel : Kapitel Identifizieren



Beispiel : Massnahmen der Kategorie «Inventar Management»

Funktion	Kategorie	Aktivität	Bewertung	Kommentare	Referenzen
Identifizieren	**Inventar Management (Assest Management)** Die Daten, Personen, Geräte, Systeme und Anlagen, einer Organisation sind ein einer Art und Weise identifiziert, katalogisiert und bewertet, die ihrer Kritikalität hinsichtlich der zu erfüllenden Geschäftsprozesse, sowie der Risikostrategie der Organisation entsprich.	**ID.AM-1:** Erarbeiten Sie einen Inventarisierungsprozess welcher sicherstellt, dass zu jedem Zeitpunkt ein vollständiges Inventar ihrer IKT-Betriebsmittel (Assets) vorhanden ist.	**n/a**		· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **ISO/IEC 27019:2013** 7.1.1, 7.1.2 · **NERC CIP-002** · **BSI-Standard** 100-2, Kapitel 4.2 Strukturanalyse · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Inventarisieren Sie all Ihre Softwareplattformen / -Lizenzen und Applikationen innerhalb ihrer Organisation.	**n/a**		· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **ISO/IEC 27019:2013** 7.1.1, 7.1.2 · **NERC CIP-002** · **BSI-Standard** 100-2, Kapitel 4.2 Strukturanalyse, M 2.225 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Katalogisieren Sie all Ihre internen Kommunikations- und Datenflüsse.	**n/a**		· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **ISO/IEC 27019:2013** 7.2.1 · **NERC CIP-005** · **BSI-Standard** M 2.393 Regelung des Informationsaustausches · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: Katalogisieren Sie alle externen IKT-Systeme, die für ihre Organisation relevant sind.	**n/a**		· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **ISO/IEC 27019:2013** 7.2.1 · **NERC CIP-002** · **BSI-Standard** B 2.10 Mobiler Arbeitsplatz · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Priorisieren Sie die inventarisierten Ressourcen (Geräte, Anwendungen, Daten) hinsichtlich ihrer Kritikalität.	**n/a**		· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **ISO/IEC 27019:2013** 7.2.1 · **NERC CIP-002** · **BSI-Standard** BSI-Standard 100-2, Kapitel 4.3 Schutzbedarfsfeststellung · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Definieren Sie klare Rollen und Verantwortlichkeiten im Bereich der Cyber Security.	**n/a**		· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **ISO/IEC 27019:2013** 8.1.1 · **NERC CIP-003** · **BSI-Standard** BSI-Standard 100-2, Kapitel 3.4.2 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

Kurzdefinitionen der Implementierungsebenen

0 Diese Massnahme ist der Organisation nicht bekannt, es wurde nichts unternommen.

1 Die Organisation ist sich der Existenz dieser Massnahme bewusst, aber es gibt immer noch keine standardisierten Verfahren zum Umgang mit den Risiken, die reaktiv angegangen werden.

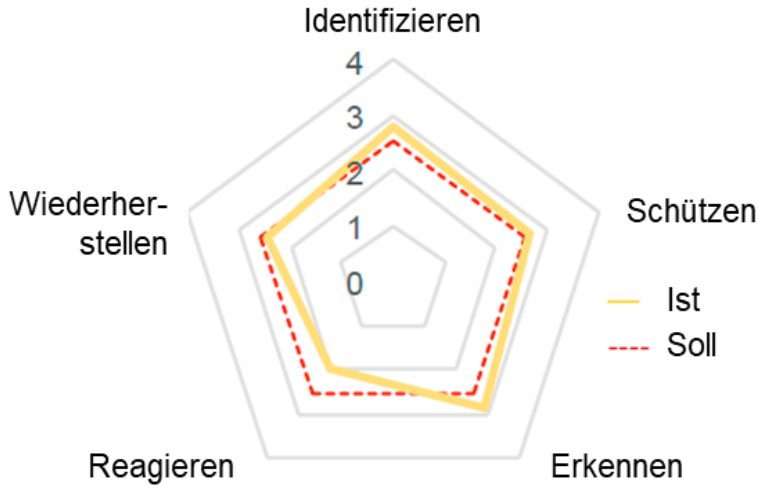
2 Es gibt ein Standardverfahren für das Management der mit dieser Massnahme verbundenen Risiken, aber die Organisation hat es nicht verpflichtend eingeführt oder setzt es nur teilweise um.

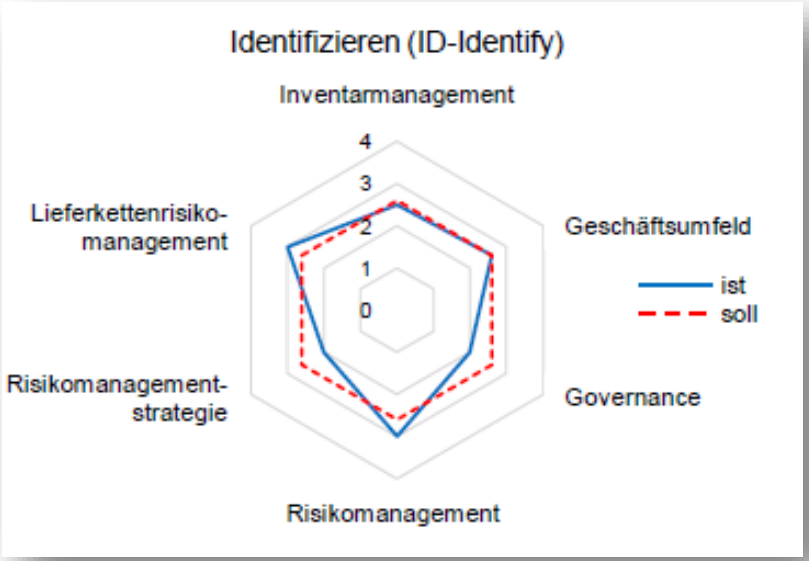
3 Das Risikomanagement-Verfahren wurde formal validiert, ebenso wie die Anweisungen zu seiner ordnungsgemässen Umsetzung. Die IKT-Risiken werden standardisiert aufgelistet und die Richtlinien zu ihrer Behandlung werden regelmässig aktualisiert

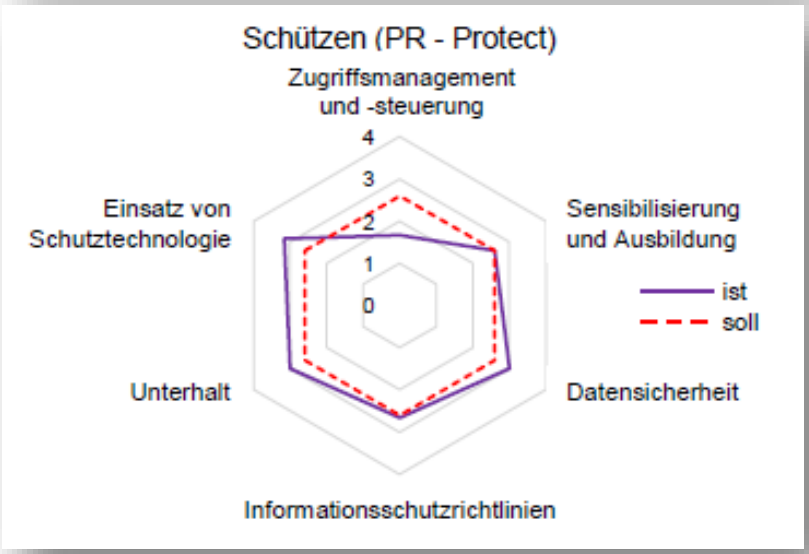
4 Die Organisation erfüllt die Anforderungen der Stufen 1 bis 3 in vollem Umfang und analysiert kontinuierlich die eigenen Prozesse, Methoden und Fähigkeiten, um sie zu verbessern und ein hohes Mass an Cybersicherheit zu gewährleisten

Ergebnis des Bewertungstools

Cyber Security Maturity Rating	Ist	Soll
Identifizieren (*Identify*)	2.8	2.6
Schützen (*Protect*)	2.7	2.6
Erkennen (*Detect*)	2.9	2.6
Reagieren (*Respond*)	2.0	2.6
Wiederherstellen (*Recover*)	1.4	2.6



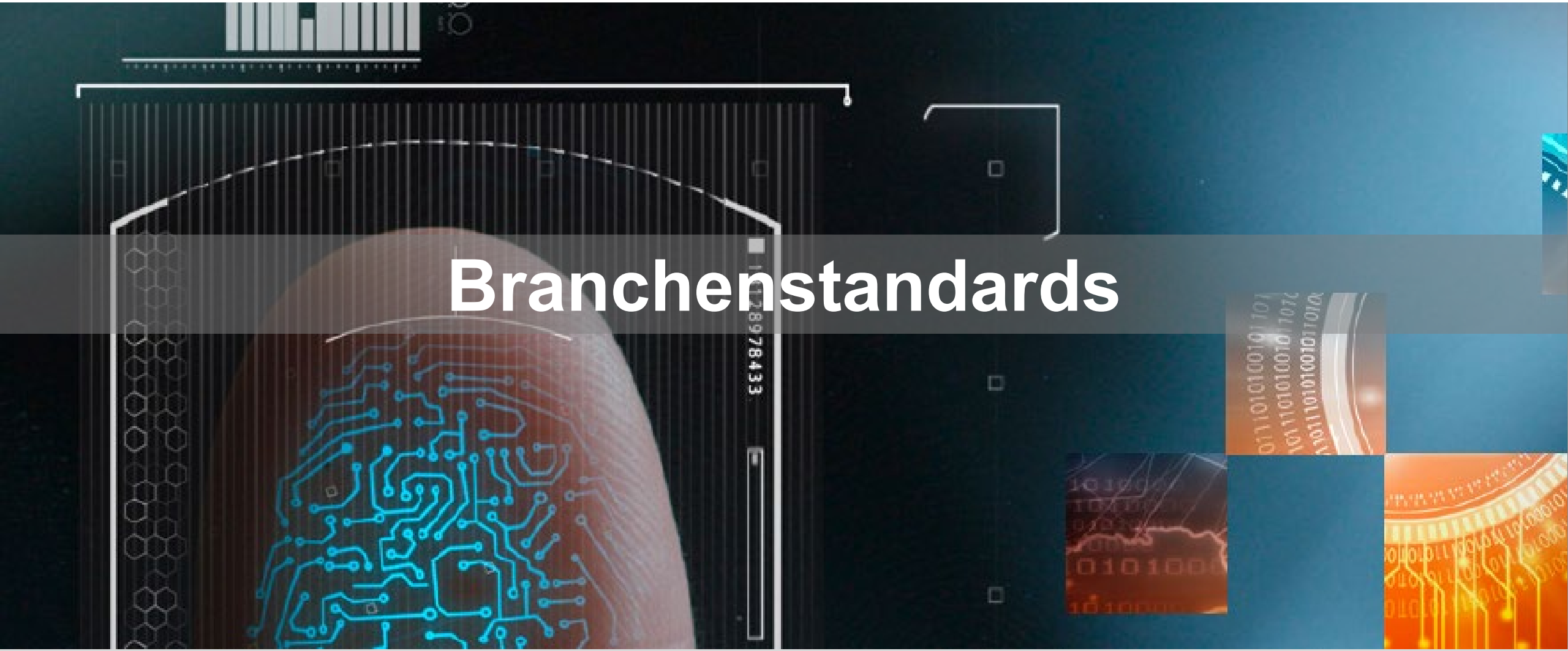




Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für Wirtschaftliche Landesversorgung BWL
Fachbereich IKT



Branchenstandards

Kooperation mit Wirtschaftsverbänden

IKT-Minimalstandard

- In Zusammenarbeit mit Industrieverbänden entwickelt das BWL IKT-Minimalstandards, die speziell auf die Bedürfnisse des betreffenden Sektors zugeschnitten sind.
- Diese Branchenstandards basieren auf dem gleichen Framework und beinhalten die gleichen Massnahmen wie der "allgemeine" IKT-Minimalstandard, werden aber durch die Identifizierung kritischer Aktivitäten an die Bedürfnisse der betroffenen Sektoren angepasst.

Strom

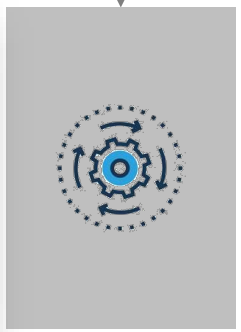
Trinkwasser

Lebensmittel

Abwasser

Gas

ÖV



Fernwärme
Hospital
Entsorgung
Logistik Terminals

Vom allgemeinen IKT-Minimalstandard zu den Branchenstandards

- Analyse des Versorgungsprozesses
- Identifizierung von Akteuren
- Identifizierung kritischer Aktivitäten und ihrer IKT-Systeme
- Analyse der Verwundbarkeiten

Ziele der Branchenstandards

- Durch risikobasierte Massnahmen kann der Standard an unterschiedliche Bedürfnisse angepasst werden, indem er folgendes berücksichtigt: Grösse, Ressourcen, Bedürfnisse und Bedrohungen jeder Organisation.

- Die Identifizierung kritischer Aktivitäten ermöglicht die Priorisierung bestimmter Massnahmen im Cybersicherheitsprogramm, um die Sicherheit kritischer Elemente im Gassektor zu gewährleisten.

- Die Sicherheit von IKT-Systemen ist ein ständiges Ziel, das einer regelmässigen Überwachung und einem kontinuierlichen Verbesserungsprozess unterworfen werden muss. Der IKT-Minimalstandard dient als Leitfaden für die Umsetzung dieses Prozesses zur Erreichung dieses Ziels.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Wirtschaft, Bildung und Forschung WBF

Bundesamt für Wirtschaftliche Landesversorgung BWL
Fachbereich IKT

IKT-Minimalstandard Abwasser

IKT-Minimalstandard Abwasser 1/2

- Produziert von step by STEP in Zusammenarbeit mit dem VSA/FES und dem BWL
- Veröffentlicht im Jahr 2019, aktualisiert im Jahr 2021 und französische Version veröffentlicht Ende 2021
- Teil der step by STEP Methode, kann aber auch separat verwendet werden
- Cybersicherheitsprogramm unterscheidet sich leicht vom IKT-Minimalstandard mit etwa 80 Massnahmen
- Ermöglicht es den Abwasserbehandlungsunternehmen, sich auf die Kernelemente ihres Sektors zu konzentrieren

IKT-Minimalstandard Abwasser 2/2

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Inventur Hardware OT Haben Sie eine Inventur aller OT-Systeme (Server, Netzwerkkomponenten, Bedientableaus, mindestens alle Geräte mit einer IP-Adresse)?			(x)	x		ID.AM-1
Inventur Software OT Haben Sie eine Inventur der benutzten Software (Betriebssystem, Office, Programme etc.)?			(x)	x		ID.AM-2
Inventur Hardware IT Haben Sie eine Inventur aller IT-Systeme (PCs, Drucker, Routers, Tablets, Smartphones, etc., mindestens alle Geräte mit einer IP-Adresse)?			(x)		x	ID.AM-1
Inventur Software IT Haben Sie eine Inventur der benutzten Software (Betriebssystem, Office, Programme etc.)?			(x)		x	ID.AM-2
Inventar Netzwerkverbindungen und Datenflüsse (OT und IT) Haben Sie ein Inventar aller Netzwerkverbindungen und der Datenflüsse, welche über diese Verbindungen geleitet werden?			(x)	x	x	

- Validierung oder Nichtvalidierung der Massnahme
- Bewertung der Kritikalität (hoch-niedrig-kein)
- Definieren Sie Unterstützungen für jede Massnahme (ES, OT, IT)
- Differenzierung der Massnahmen zwischen IT und OT
- Gibt die Gleichwertigkeit der Massnahmen mit dem IKT-Minimalstandard vor
- Enthält spezifische Massnahmen für den Abwassersektor

Kontakt

Bundesamt für Wirtschaftliche Landesversorgung BWL

Bernastrasse 28
3003 Berne

Sven Peter
Projektleiter NCS
Sven.peter@bwl.admin.ch
Tél. : +41 58 462 21 71

Minimalstandard Cybersicherheit in Abwasserbetrieben

step by STEP

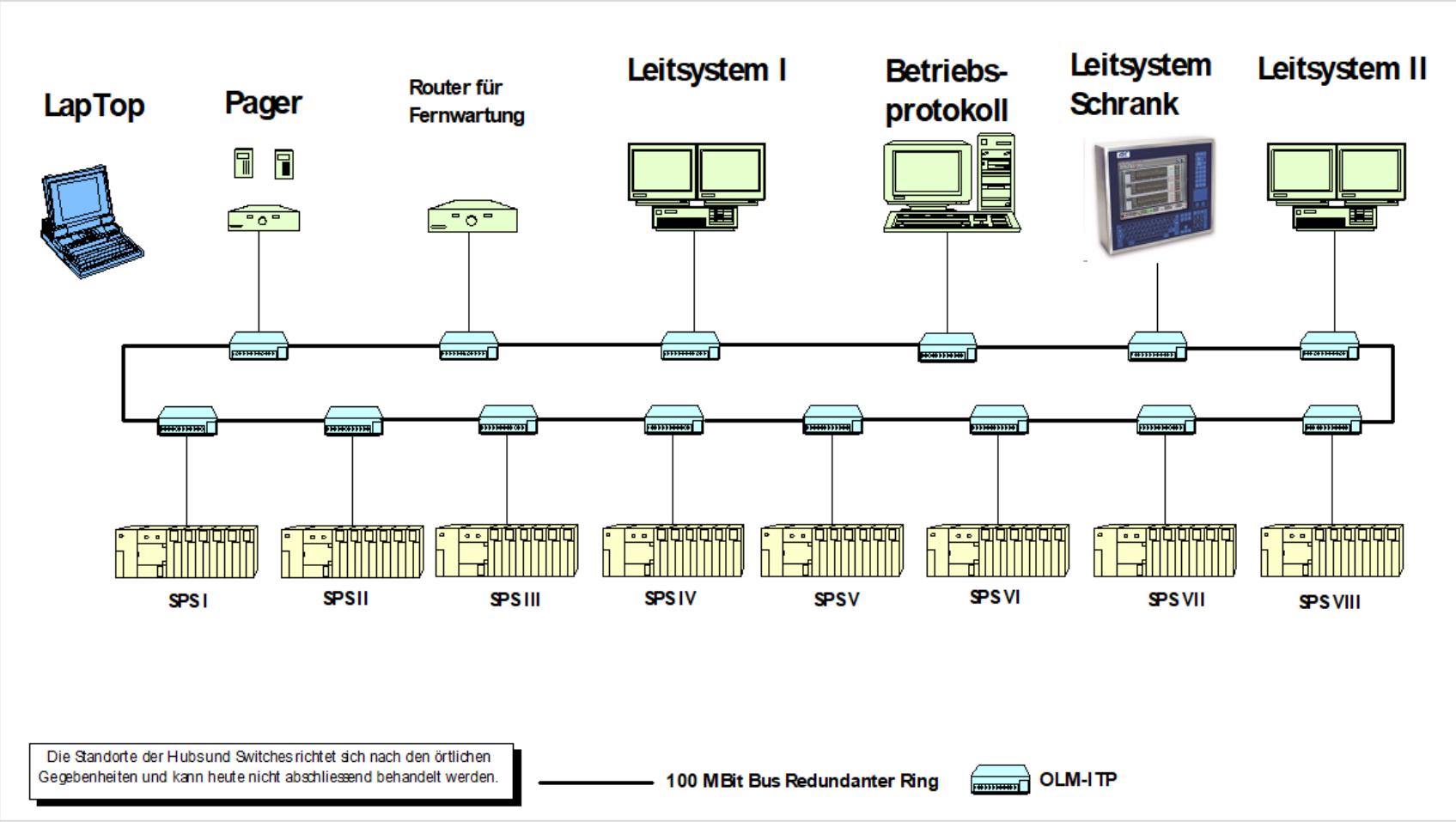
OT-Netzwerk (PLS-Netzwerk)
Systemarchitektur und wovor wir uns schützen müssen

Reto Steinemann / Melchior Zimmermann

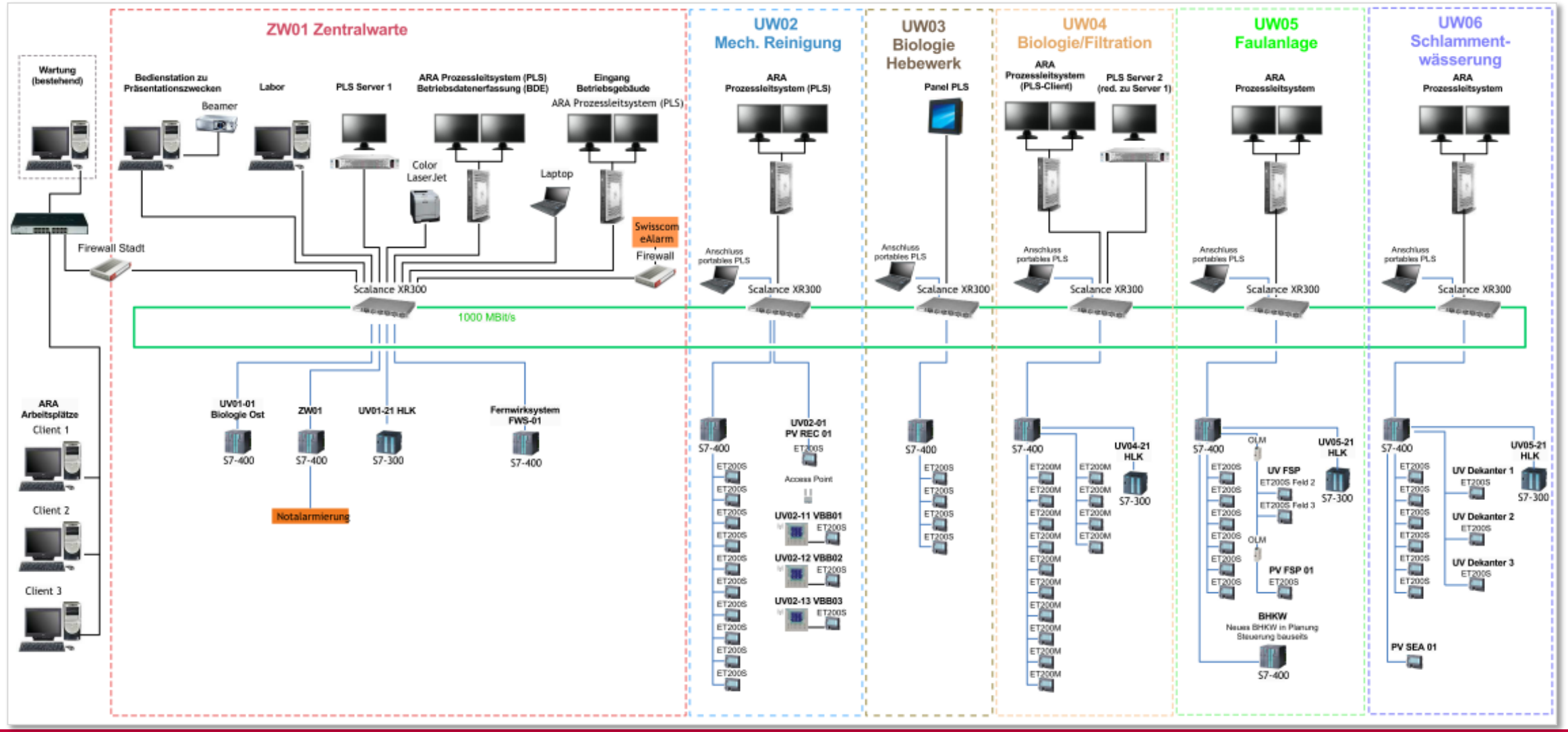
Cyber-Sicherheit im OT-Netz

- Ein typisches OT-Netzwerk
- Der Wandel der Zeit
- Bedrohungen und Akteure
- Wie können wir uns schützen?

Das OT-Netzwerk 2000



Das OT-Netzwerk 2021

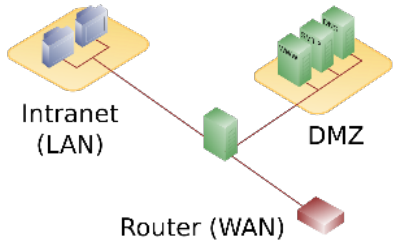


Das OT-Netzwerk – im Wandel der Zeit

- Das Automationsnetz ist im Grundsatz gleich geblieben
  - Der defensive Ansatz ist geblieben
  - Möglichst isolierte und exklusive Nutzung des Netzes
  - Schutz der Leitsystemrechner und der Steuerungssysteme
- Neue Fernwartungsansprüche
  - „Anytime – Anywhere – AnyDevice“
- Zunehmend mehr Zugriffe auf andere Netze
  - Vernetzung mit der IT-Welt
  - Internetzugriff für Alarmierung, Wetterdaten, etc.

Das OT-Netzwerk – im Wandel der Zeit

- Neue Devices und neue Netze
  - IT-Netz (Büro)
  - Kantons- / Gemeinde-Netz
  - Fremdsystem-Netz
  - Telefonie-Netz
  - Kamera-Netz
  - W-Lan (Betrieb, Gäste, Telefonie, etc.)
  - DMZ-Netze (Fernwartung)
- Anbindung von Aussenstellen
  - Aussenstellen-Netz (LWL, SHDSL, etc.)
  - VPN (All IP, xDSL, Cabel, LTE, etc.)



Das OT-Netzwerk - Fazit

- Risiken
  - Schlechtes Netzwerk-Layout
  - Konfigurationslücken in sicherheitsrelevanten Komponenten
  - Angreifbare Schwachstellen in den Systemen (veraltete Firmware, etc.)
  - Malwarebefall durch Internet oder portable Medien
- Wir brauchen ein Bewusstsein für die Sicherheit
  - Sicherheit braucht Wartung
  - Sicherheit kostet Geld

- Nur Firewalls einbauen reicht nicht
- OT-Sicherheit ist eine neue Disziplin in der Automation geworden

Bedrohungen und Akteure

Der Hackerangriff auf die WV Ebikon im November 2018

- „Mit tausenden von bösartigen Anfragen aus London und Korea wurde die Anlage angegriffen“
- „Das neue System hat die Angriffe sofort abgewehrt“

Was ist passiert?

- Der Industrierouter war einer „Brute Force“ SSH-Attacke ausgesetzt.
- Dabei sollen mit beliebig vielen Login-Versuchen die Zugangsdaten ermittelt werden.
- Die resultierende Systembelastung hat den Router praktisch blockiert und das VPN ist ausgefallen.

→ Was ist in der Presse damit passiert?

watson

Schweiz International Wirtschaft Sport Leben Spass Digital Wissen Blogs Videos Wettbewerbe

Hacker aus London beis Wasservers Ebikon LU d

Hacker haben im November die IT-Infras Wasserversorgung der Gemeinde Ebikor System, das im letzten Herbst installiert die Attacken abwehren. Als Konsequenz Sicherheitsstufe erhöht.

Mehrere tausend Mal sei die Software Anfragen aus London und Korea ange die Gemeinde am Mittwoch mit. Der Syst die Angriffe registriert und der Gemeind Markus Dubach, Leiter der Wasserversor Nachrichtenagentur Keystone-SDA.

Blick

News Sp

News Schweiz Zentral

Urheber in London und

Hacker-A Wasserve Ebi

10:55 19.12.

Die auto Gemein Softwar

inside-it.ch

ictjobs.ch Beschaffung Newsletter Inserieren Inside-chann

Mittwoch, 19.12.2018 / 11:37 0

Hacker beissen sich an Wasserversorgung von Ebikon die Zähne aus

Wenn Medien über Hacker berichten, dann ist der Anlass le ihrer "Erfolge". Da tut es gut, für einmal auch über einen erf Angriff berichten zu können. Einen solchen meldet die Luze Ebikon. Hacker hätten im November die IT-Infrastruktur der der Gemeinde angegriffen. Das System, das im letzten Her habe die Attacken aber abwehren können. Trotzdem wurde Sicherheitsstufe noch einmal erhöht.

Mehrere tausend Mal sei die Software von bösartigen Anfr worden, teilte die Gemeinde mit. Der Syste t und der Gemeinde gemeldet, sagte Mari g auf Anfrage von 'Keystone-SDA'.

n Eindringungsversuche ins Netzwerk geh e, Reservoire überwache und bei Wasserc er sehr guten Verschlüsselung hätten die Systembetreiber habe die IP-Adressen d nd so den Ursprungsort ermitteln könner Dubach.

n Betriebssteuerung handle es sich um d Europa. Wäre trotz der Sicherheitsvorkel nnten die Betreiber das System als Notlös hanuell bedienen.

6'500 Personen mit Wasser. Angeschloss Adligenswil, Buchrain oder Dierikon. Zudem liefert Ebikon Root. (sda/hjm)

VIDEO

Hacker-Angriff au Wasserversorgur zum mehreren Ta Anfragen»

Ende November wurde das System de gehackt. Der Angriff konnte erfolgrei zeigt.

• Aktualisiert
Sandra Monika Ziegler
19.12.2018, 20:03 Uhr

Hacker versuchten das digitale Leitungsnetz der Wasserversorgung Ebikon lahmzulegen. (Symbolbild: Getty)

tele1

VERKEHRSSERVICE 2 MELDUNGEN | 2° IN LUZERN SCHÖN | LOGIN

Zentralschweizer Fernsehen NEWS TV-PROGRAMM SENDUNGEN EVENTS TICKETS WERBUNG

7°

SRF

Suche MENÜ

News > Zentralschweiz >

Angriffe abgewehrt

Hackerangriff auf die Wasserversorgung von Ebikon

Mittwoch, 19.12.2018, 17:12 Uhr

Dieser Artikel wurde 1-mal geteilt.

Wäre die Attacke erfolgreich gewesen, hätte das grosse Folgen haben können
02:07 min, aus Regionaljournal Zentralschweiz vom 19.12.2018.

- Mehrere tausend Mal versuchten Hacker von London und Korea aus in das Computersystem der Wasserversorgung von Ebikon einzudringen.
- Das im letzten Herbst neu installierte System konnte aber alle Angriffe abwehren und aufzeichnen. So konnten die Angriffe zurückverfolgt werden.
- Wären die Angriffe erfolgreich gewesen, hätte das gröbere Folgen haben können, sagt der Leiter der Wasserversorgung Ebikon, Markus Dubach.
- Dass ausgerechnet Ebikon Opfer von Cyberattacken wurde, sei reiner Zufall meint Dubach. Trotzdem wurden die Sicherheitsstandards erhöht.

SRF 1, Regionaljournal Zentralschweiz, 17:30 Uhr; joel

News > Zentralschweiz >

Der Luzerner Gesundheitsdirektor Guido Graf zum Sparprogramm des Kantonsspitals: «Der Kostendruck war noch nie so gross»
Kilian Küttel / 21.12.2018, 05:00 Uhr

Der Rundweg soll weg vom Ufer des Baldeggersees
Ernesto Piazza / 21.12.2018, 05:00 Uhr

DONNERSTAG, 20. DEZEMBER 2018 / 20MINUTEN

Luzern/Reg

Hacker greifen Ebikoner Wasserversorgung an

EBIKON. Tausende Male ist die Software der Wasserversorgung von Ebikon von bösartigen Anfragen angepinnt worden. Doch das System hielt den Attacken stand.

Aus London und Korea seien bei der IT-Infrastruktur der Wasserversorgung in Ebikon Tausende bösartige Anfragen eingegangen, teilte die Gemeinde gestern mit. Hacker versuchten, sich Zugang zum System zu verschaffen, mit dem Pumpen gesteuert und Reservoire überwacht werden. «Die Motivation für den Angriff ist uns nicht bekannt», sagt Sprecher Roland Beyeler. Es sei kein gezielter Angriff gewesen: «Bei solchen Angriffen werden jeweils verschiedenste Systeme angegriffen.» Die Hacker würden es an etlichen Zielorten versuchen – erst wenn sie beim Angriff Erfolg hätten, schauten sie, was es zu holen gebe.

Dank der guten Verschlüsselung hatten die Hacker keinen Erfolg. Beyeler: «Das System hat den Angriff registriert und sofort gemeldet.» Es war der erste Vorfall dieser Art. In Ebikon freut man sich über die Abwehr: «Das hat bestätigt, dass wir mit dem modernen System vor Angriffen gut geschützt sind», sagt Beyeler. Dennoch reagierte man auf den Vorfall: «Das System wird zwar den Anforderungen gerecht, wir haben aber nun zusätzliche Massnahmen ergriffen, um die Sicherheit noch weiter zu erhöhen.» Würden Hacker trotzdem erfolgreich sein, könnten die Betreiber das System herunterfahren und die Anlagen manuell bedienen. «Die Wasserversorgung könnte nicht fremdgesteuert werden.» GWA/SDA

Das System hielt den Hacker-Attacken aus London und Korea stand. GEMEINDE EBIKON

Bedrohungen und Akteure

Es stellen sich nun ein paar grundsätzliche Fragen…

- Wer bedroht uns?
- Welche Angriffsvektoren sind für uns relevant?
- Wovor können und müssen wir uns schützen?
- Wie kommen wir zu einem guten Grundschutz?
- Wo kann uns der IKT Minimalstandard helfen?

„Es gibt eine Vielzahl an Risiken…

…von welchen Bedrohungen müssen wir aber tatsächlich ausgehen?“

Akteure

- Script-Kiddies
  - Einsatz „gefundener“ Tools, nicht zielgerichtet
  - Mittlere Angriffs-Wahrscheinlichkeit, wenig Erfolgschancen
- Cyberkriminelle
  - Geschäftsmodelle um Geld zu verdienen
  - Hohe Angriffs-Wahrscheinlichkeit, mittlere Erfolgschancen (vor allem im Bereich IT)
- Staatliche Akteure
  - Politisch, religiös oder kulturell motivierte Angriffe
  - Kleine Angriffs-Wahrscheinlichkeit, grosse Erfolgschancen
- Bösartige Insider
  - Der Anlage schaden zufügen
  - Kleine Angriffs-Wahrscheinlichkeit, grosse Erfolgschancen

Der Angriffsvektor

„Der Angriffsvektor bezeichnet einen möglichen **Angriffsweg** und die **Angriffstechnik**, die ein unbefugter Eindringling, ganz gleich welcher Art, nehmen kann, um ein fremdes Computersystem zu kompromittieren, das heißt unbefugt einzudringen und es danach entweder zu übernehmen oder zumindest für eigene Zwecke zu missbrauchen.“

Meistens werden dafür bekannt gewordene Sicherheitslücken in dem angegriffenen System genutzt. Ein solches Ausnutzen bezeichnet man als **Exploit**.

(Quelle: Wikipedia)

→ Welche Angriffswege können im OT-Netzwerk ausgenutzt werden?

Angriffswege

- Internetanbindung
  - Unsichere Firmware oder Fehlkonfiguration in der Firewall
  - Unsichere Geräte direkt vom Internet erreichbar
- Internetzugriff
  - Webseite mit Malware
  - Programm heruntergeladen mit Malware
  - Email mit Malware im Anhang
- Fernwartungszugriff (VPN)
  - Schlecht abgesicherter Zugang
  - Befallenes Gerät im Netz (PC, Notebook, Tablet, etc.)

Angriffswege

- Portable Medien (Memory-Stick oder externe Festplatte)
  - Datei mit Schadenscode (Office-Dokument mit Makro)
  - Manipulierter Memory-Stick
- IT-Umgebung
  - Befallenes Gerät (Büro-PC, etc.)
- Wireless Lan
  - Schlecht geschützter Zugang
  - Befallenes Gerät im Netz (Notebook, Tablet, etc.)

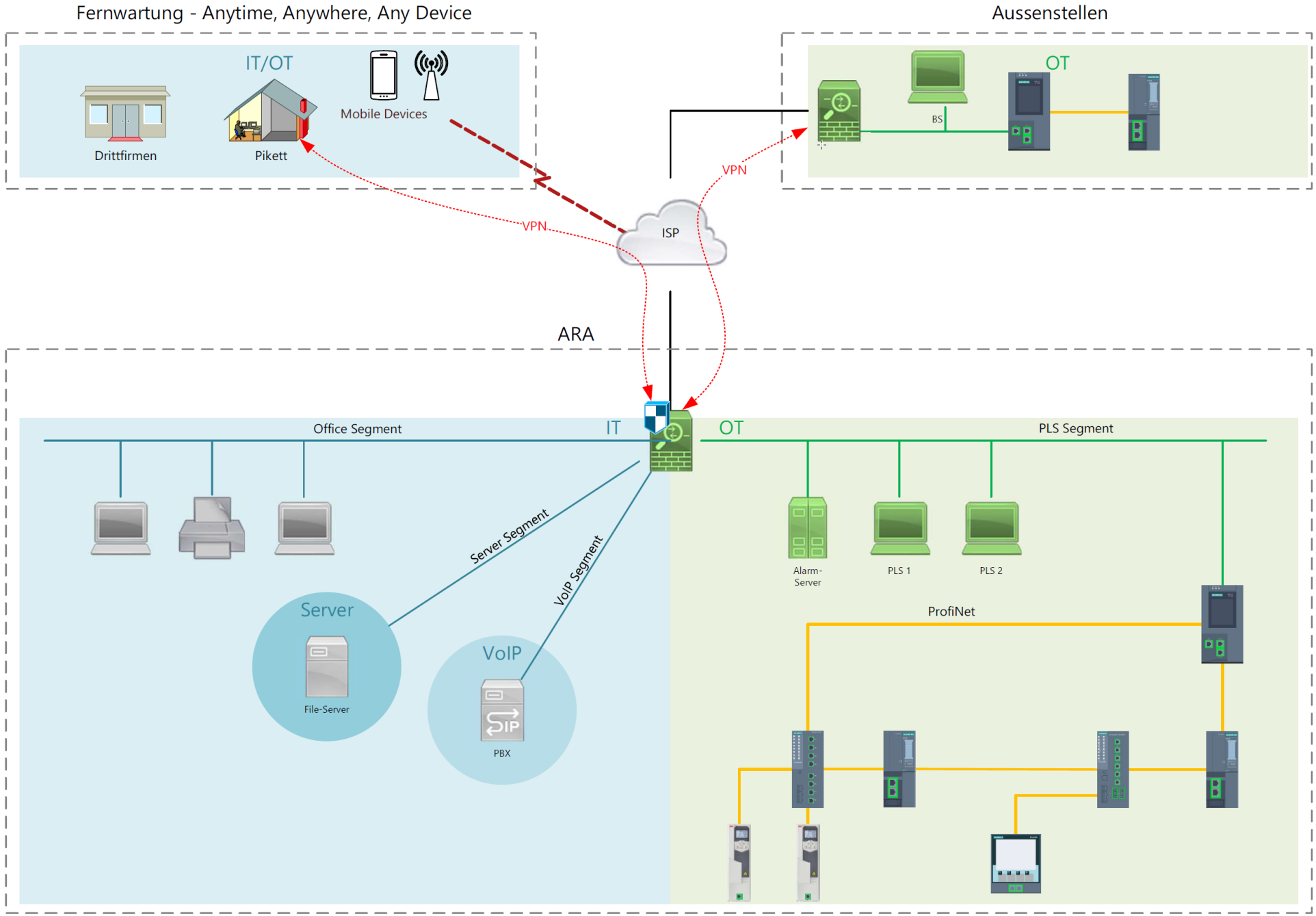
Wie können wir uns schützen?

- Defense-in-Depth
  - Angriffe brauchen mehrere Schritte, damit sie erfolgreich sind
  - Jeder Schritt ist eine Gelegenheit, den Angriff abzuwehren
  - Je mehr Schritte, desto weniger Chancen hat ein Angriff
- Risikobasierter Ansatz
  - Mann muss nicht alles machen, aber…
  - …man muss wissen, was man nicht macht und warum
  - Risiko = (Auswirkungen x Wahrscheinlichkeit) / Kosten
  - Die OT-Verfügbarkeit muss mitberücksichtigt werden
  - Die IT-Vertraulichkeit muss mitberücksichtigt werden
- Wir brauchen einen „Grundschutz“ der die relevanten Risiken abdeckt

Grundschutz

- Segmentierung der Netze
  - Nur so viel Internetzugriff wie nötig
  - Möglichst kein Zugriff in das OT-Netz (VPN!)
  - Nur gezielter Zugriff aus dem OT-Netz
  - Weiter Netze für spezifische Anforderungen

- Regelmässige Wartung
  - Patchen der Systeme (Firewall, PC‘s, etc.)
  - Kontrolle der Konfigurationen
  - Kontrolle der Benutzerlisten und Passwörter


Fernwartung - Anytime, Anywhere, Any Device
IT/OT
Drittfirmen
Pikett
Mobile Devices
Aussenstellen
OT
BS
VPN
VPN
ISP
ARA
IT
Office Segment
OT
PLS Segment
Server Segment
VoIP Segment
Server
File-Server
VoIP
PBX
Alarm-Server
PLS 1
PLS 2
ProfiNet

Grundschutz

- Bewusstsein bei den Benutzern schaffen
  - Welche OT-Systeme haben wir
  - Welche IT-Systeme haben wir
  - Welche Risiken bestehen
- Persönliche Benutzer und Passwortrichtlinien
  - Alle Systeme müssen gegen ungewollten Zugriff geschützt sein
  - Benutzer müssen eindeutig identifiziert werden
- Backup der Projekte / Archivdaten
  - Rasche Wiederherstellung
  - Datenverlust verhindern

Fazit

- Technisch
  - Guter Grundschutz
  - Regelmässige Wartung

- Organisatorisch
  - Die IT- und die OT-Systeme und die Risiken müssen bekannt sein
  - Es muss definiert sein was wir tun, wenn etwas passiert

- Der IKT-Minimalstandard hilft…
  - Erfassung der Systeme
  - Einführung der Prozesse
  - Regelmässige Überprüfung der Prozesse

Vielen Dank für Ihre Aufmerksamkeit!

step by STEP

IT-Netzwerk (Verwaltung)
Systemarchitektur und wovor wir uns schützen müssen

Reto Steinemann / Melchior Zimmermann

Verantwortung IT-Sicherheit

- Management

•Organisatorische Massnahmen festlegen
•Ziele definieren
•Richtlinien erstellen

- Techniker

•Technische Konzepte
•Umsetzung
•Wartung

- Benutzer

•???

Cyber-Sicherheit im IT-Netz

- Angriffswege
- Wie habe ich einen „einfachen Grundschutz“
- Social Engineering
- Passwörter

Angriffswege

- Wie kommen Angreifer auf einen PC?

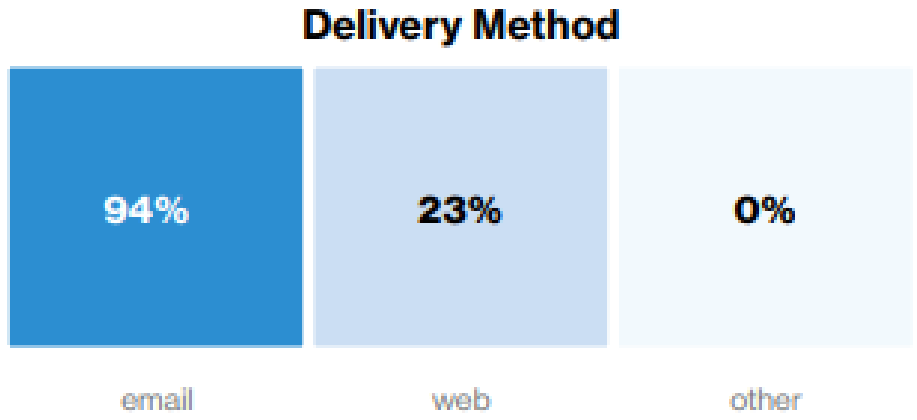


Figure 19. Malware types and delivery methods

2019 Verizon data-breach investigations report

- E-Mail und Browser sind die meistverwendeten Angriffswege
- Ein System mit den neusten Updates von Aussen anzugreifen, ist extrem schwierig (wird gezielt eingesetzt, in den meisten Fällen vernachlässigbar)

Updates

- Es war noch nie so einfach, Updates durchzuführen

- Automatisch
- Zuverlässiger und stabiler

- Die wichtigsten Updates

- Betriebssystem
- Browser

JUST DO IT.

Browser

- Ad-Blocker (nicht nur weil es angenehmer ist)
- Nur auf bekannte oder «grosse» Webseiten
- Nicht auf unbekannte Links klicken

uBlock origin

HTTPS Everywhere

E-Mail

- Sich nie unter Druck setzen lassen
- Keine unerwarteten Anhänge öffnen
- Keine Makros aktivieren
- Keine unbekannten Links anklicken
- Keine Passwörter eingeben

Was tun im Zweifelsfall?

- Email mit dubiosem Anhang aus vertrauter Quelle
- Zweite Meinung einholen
- Absender/-in direkt kontaktieren (z.B. per Telefon)

- Falls die Probleme bereits da sind:
- Netzwerk trennen
- PC nicht ausschalten
- Spezialisten kontaktieren

Social Engineering - Manipulation

- Wie bringt man ein potenzielles Opfer dazu, auf den Link zu klicken oder einen Anhang zu öffnen?

→ Durch «Social Engineering»

- Menschen dazu bewegen, etwas zu tun, was sie nicht tun sollen/wollen
- Manipulation durch kennen des menschlichen Verhaltens
- “Hochstapler-Tricks”

- Nicht nur für Hackerangriffe:
- Im Verkauf
- In den Medien
- In der Politik

Zusammenfassung

- Social Engineering ist oft der Anfangspunkt eines Angriffs
- Es geht um Menschliches, nichts Technisches

«Je billiger das Kommunikationsmedium, desto weniger darf man ihm vertrauen.»

Sichere Passwörter

- sind schwer zu erraten
- sind lange
- sind einfach zu merken
- nur für eine Webseite oder Applikation verwenden

Beispiele:

- **Thomas** : schlechtes Passwort, einfach zu erraten
- **@#hjSDF23** : schlechtes Passwort, schwer zu merken
- **jedenMorgenEsselchEineBratwurst** : gutes Passwort, schwer zu erraten, einfach zu merken

Passwort-Manager

- Alle Passwörter werden in eine Anwendung verwaltet
- Webseiten, Applikation, etc.
- Als Anwendung/App oder als Cloud-Service erhältlich

- Es gibt nur ein “Master-Passwort» zum merken
- Alle anderen Passwörter sind im Passwort-Manager gespeichert
- Viel einfacher, als sich 30 verschiedene Passwörter zu merken

- Keine “Redundanz”
- Ist der Passwort-Manager gehackt, ist alles bekannt
- Ist das Master-Passwort vergessen sind die Passwörter nicht mehr zugänglich

MFA – Multi-Faktor-Authentifizierung

- Authentifizierung braucht einen zweiten Faktor (2FA)
- APP
- SMS
- PUSH-Nachricht
- Externe Hardware

- Markante Erhöhung der Sicherheit
- Passwort erraten bringt nicht mehr viel
- Aufwand für einen erfolgreichen Angriff ist erhöht

Zusammenfassung

- Updates durchführen
- Benutzen eines Ad-Blocker
- E-Mails lieber zweimal lesen/analysieren
- MFA für kritische Konten gezielt einsetzen

- … und damit ist die Mehrheit der Angriffe schon abgewehrt.

aber: «IT-Security ist ein Prozess und kein Zustand»

Vielen Dank für Ihre Aufmerksamkeit!

step by STEP

Zusammenfassung und Praxis
IKT-Minimalstandard Abwasser

Reto Steinemann / Melchior Zimmermann / Max Schachtler

Wichtigste Fakten Cyber-Sicherheit (1/8)

Kläranlagen, Ingenieure, Firmen sind sensibilisiert

- Manche Firmen wollen auf den Zug aufspringen → Achtung IT-Sicherheitslücken!
- Sehen neues Geschäftsfeld → Sind gleich Cyber-Spezialisten/Experte

Betriebsleiter stellt Kriterien/Anforderung an Sicherheitsexperten (Cyber)

- **Zertifizierung** verlangen z. B. CISA, bedingt stetige Weiterbildung, Erfahrung
- Cyber-Security ist das **Haupttätigkeitsfeld** der Firma → aktuelle Fachkompetenz
- Neutral, unabhängig, **keine Interessenkonflikte** mit Lieferanten im Abwasserbetrieb

Wichtigste Fakten Cyber-Sicherheit (2/8)

Betreiber kennt sein IKT-Umfeld, stellt Unterlagen bereit. Hilfsmittel:

- Branchendokument Checklisten JA / NEIN im Kapitel 5 und Handlungsanweisungen im Kapitel 6

Vorgabe	Ja	Nein	Unterstützer			Referenz IKT
			SE	OT	IT	
Inventur Hardware OT Haben Sie eine Inventur aller OT-Systeme (Server, Netzwerkkomponenten, Bedientableaus, mindestens alle Geräte mit einer IP-Adresse)?			(x)	x		ID.AM-1
Inventur Software OT Haben Sie eine Inventur der benutzten Software (Betriebssystem, Office, Programme etc.)?			(x)	x		ID.AM-2

Wichtigste Fakten Cyber-Sicherheit (3/8)

Grundschutz

Keine voreiligen, überstürzten Aktionen starten → nicht zielführend

Persönliche Benutzer und Passwortrichtlinien verwenden

- Standard Kapitel 6

Back-up der Projekte / Archivdaten

- Rasche Wiederherstellung / Datenverlust verhindern

E-Mails; Internet

- Nicht alles interessante und vielversprechende ist zu öffnen

Wichtigste Fakten Cyber-Sicherheit (4/8)

ARA-Betreiber kann Grundlagen erstellen

- Tools von step by STEP nutzen → Erfahrungen nutzen und anfragen
- Zur Vervollständigung seinen OT-(PLS) und IT-Lieferanten anfragen

ARA-Betreiber kennt sein IKT-Umfeld wie seine Biologie!

- Das Erstellen des Inventars ist der Schlüssel um sein IKT-Umfeld zu kennen
- **Betreiber ist der Chef** → ist nicht delegierbar

ARA-Betreiber entscheidet → Massnahmen und Sicherheitsstandard!

Wichtigste Fakten Cyber-Sicherheit (5/8)

IKT-Systeme sind zu unterhalten → analog ARA Ausrüstung

- Erstkontrolle durch OT und IT-Lieferant → Leistungskatalog erstellen (step by STEP)
- Jahresservice-Vertrag mit OT- und IT-Lieferant

Sicherheitsexperte

- Prüft die IKT-Infrastruktur und gibt sie frei → analog Revision der Buchhaltung
- Dienstleistungsvereinbarung abschliessen

Sicherheit ist kein Zustand sondern ein ständiger Prozess

Wichtigste Fakten Cyber-Sicherheit (6/8)

ARA-Betreiber kennt seine Infrastruktur und ist verantwortlich

Ev. Dritten Fernzugriff erlauben

IKT-Infrastruktur OT

ARA | Aussenwerke

ARA-Fernzugriff

IKT-Infrastruktur IT

Ev. IT-Fernzugriff

Cyber-Experte
Prüft und gibt frei
Interessen-neutral

Bei Gesamtumbau Kosten in Projekt integrieren
- durch Verfahrens- oder Elektroplaner

Wichtigste Fakten Cyber-Sicherheit (7/8)

Was tun bei einem Cybervorfall?

Sofortmassnahmen (SOMA-Vorfallreaktionsplan)

- Betroffene Maschine vom Netzwerk trennen → **Netzwerkkabel ziehen**
- Zuständige Personen informieren

Wichtigste Fakten Cyber-Sicherheit (8/8)

Statt VIELE tun etwas → Branchenstandard nutzen

Erfahrungen von step by STEP nutzen

ARA	Ist verantwortlich	In Bezug seines IKT-Systems: - OT - IT - Fernzugriff
	Serviceverträge	Anfordern und Leistungen definieren: - OT (PLS) - IT (Verwaltung) - Cyberexperte
	Cyber-Massnahmen	In Etappen umsetzen

Vielen Dank!

Publikationen

VSA	Risikoexposition ICT Version DE; FR folgt bis anfangs 2022
step-ara	Branchenstandard und Factsheets in DE und FR IKT Minimalstandard Abwasser **Factsheet:** Risikoexposition nimmt mit steigender Vernetzung und Nutzerzahl zu
aqua & gas	2019/01 step by STEP Hilfreiches Arbeitsinstrument für Kläranlagen und Industrie- und Gewerbebetriebe
	2020/02 Cybersicherheit in Abwasserbetrieben Wie Kläranlagen den IKT Minimalstandard Abwasser umsetzen können
	2020/11 step by STEP und Cybersicherheit in der Praxis Erfolgreiche Umsetzung in der Kläranlage und Anwendung im Leitsystem

ETAT DE FRIBOURG
STAAT FREIBURG

Service de l'environnement SEn
Amt für Umwelt AfU

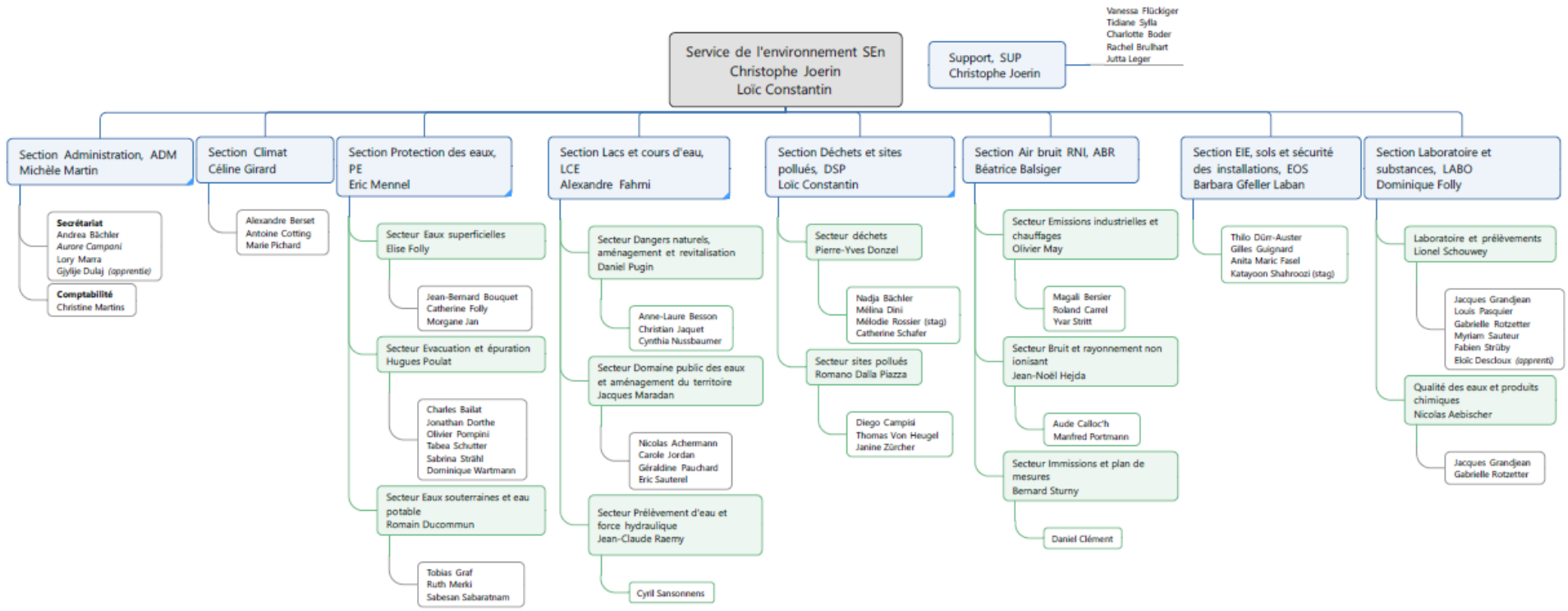
News von Sektion «Labor und Stoffe»

InfoSTEP 2021

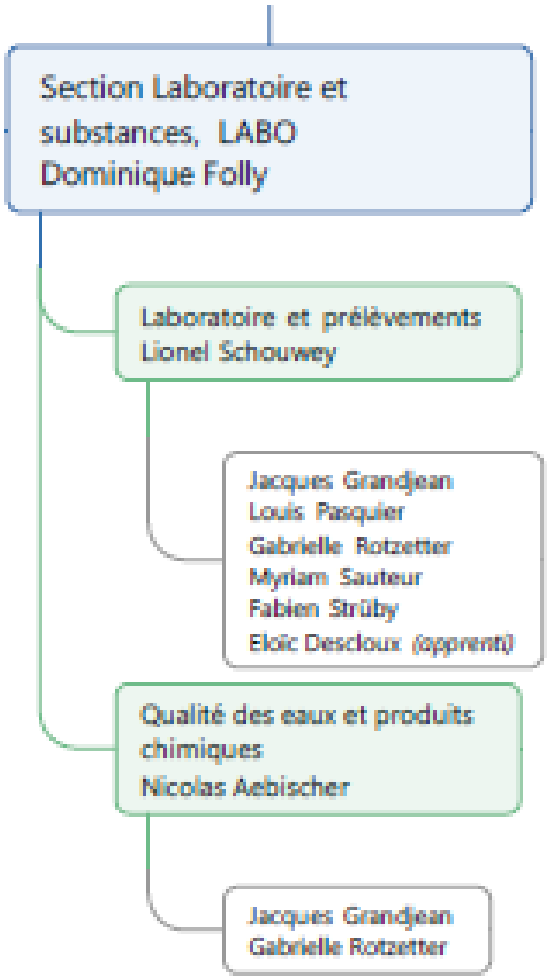
Givisiez, 13. Oktober 2021

Direction de l'aménagement, de l'environnement et des constructions **DAEC**
Raumplanungs-, Umwelt- und Baudirektion **RUBD**

Umstrukturierung der Sektion



Umstrukturierung der Sektion



InterSTEP 2021

Allgemeine Bedingungen

20 Teilnehmer

Neue Lab'Eaux-Datenbank seit 2019

Automatische Benachrichtigung – zweisprachig

Gemeinsame Exceldatei

ARA Kerzers
ARA Murten
ARA Zumholz
Section laboratoire et substances
STEP Broc
STEP Bussy
STEP Charmey
STEP Delley
STEP Domdidier
STEP Ecublens
STEP Estavayer-le-Lac
STEP Fribourg
STEP Grolley
STEP Marly
STEP Montagny
STEP Pensier
STEP Romont
STEP Torny-le-Grand
STEP Villars-sur-Glâne
STEP Vuippens

InterSTEP 2021

Allgemeine Bedingungen

Verbesserungswürdige Punkte:

Druckbare Datei auf einer Seite

Einstellbare Dezimalstellen

- ARA Kerzers
- ARA Murten
- ARA Zumholz
- Section laboratoire et substances
- STEP Broc
- STEP Bussy
- STEP Charmey
- STEP Delley
- STEP Domdidier
- STEP Ecublens
- STEP Estavayer-le-Lac
- STEP Fribourg
- STEP Grolley
- STEP Marly
- STEP Montagny
- STEP Pensier
- STEP Romont
- STEP Torny-le-Grand
- STEP Villars-sur-Glâne
- STEP Vuippens

InterSTEP 2021

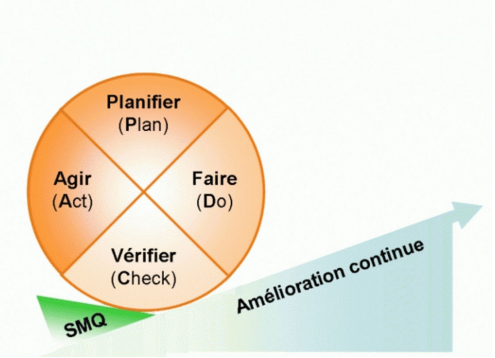
Warum?

Sicherstellen, dass ihre Routineergebnisse korrekt sind

Praktiken mit Partnern vergleichen

Korrigieren von Abweichungen

Dokumentieren der Entwicklung Ihrer Ergebnisse



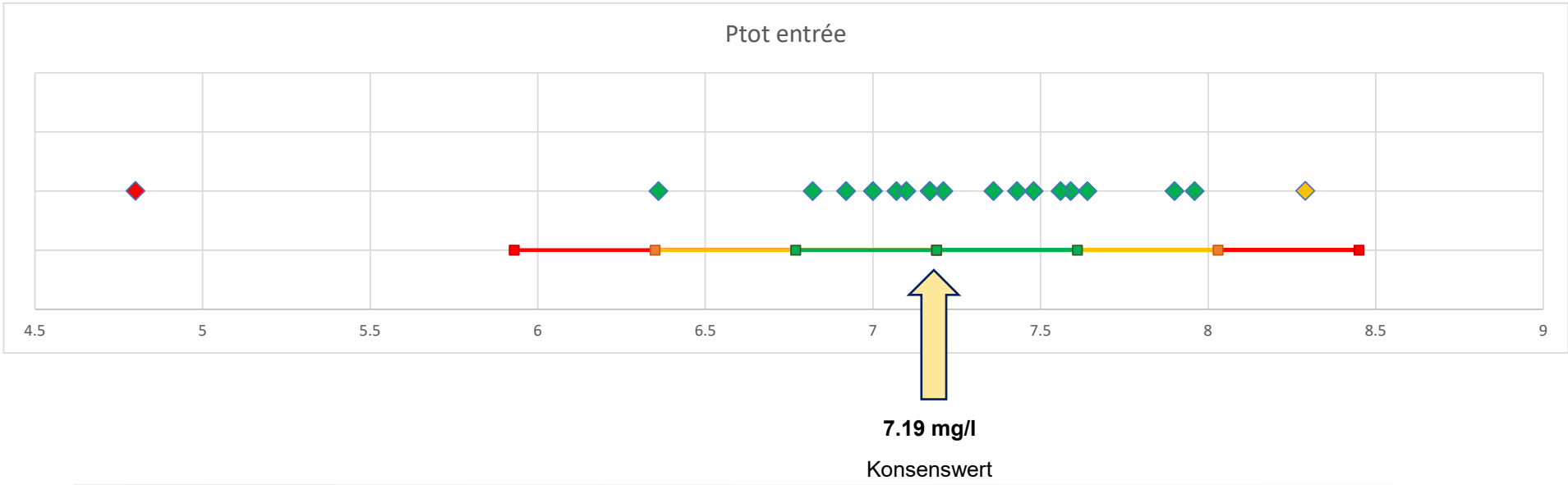
InterSTEP 2021

Z score

Auf eine barbarische Art und Weise:

$$z = \frac{X - \mu}{\sigma}$$

Auf anschauliche Weise:



InterSTEP 2021

Z score

InterSTEP 2021

Bericht

PARAMETRES / PARAMETERN		N / N	Mediane / Median	Ecart médian lissé (rel.) / Gemittelt Medianabweichung	Incertitude sur la médiane (rel.) / Median Unsicherheit	Z>2 / Z>2	Z>3 / Z>3	Z<2
DBO5 Oxitop E	ENTREE	9	340 mg/l	21.8%	9.1%	0	1	8
DBO5 Oxitop S	SORTIE	8	4 mg/l	74.1%	32.8%	0	0	8
DBO5 Winkler E	ENTREE	12	295 mg/l	27.8%	10.0%	1	0	11
DBO5 Winkler S	SORTIE	11	2 mg/l	74.1%	27.9%	2	0	9
DCO	ENTREE	20	770 mg/l	3.2%	0.9%	1	2	17
DCO S	SORTIE	20	19 mg/l	6.9%	1.9%	1	1	18
DOC S	SORTIE	20	6.4 mg/l	16.0%	4.5%	0	0	20
MeS S	SORTIE	20	8 mg/l	18.5%	5.2%	2	1	17
N-NH4 S	SORTIE	18	0.032 mg/l	56.4%	16.6%	1	3	14
N-NO2 S	SORTIE	18	0.008 mg/l	61.8%	18.2%	1	2	15
N-NO3 S	SORTIE	20	35.2 mg/l	2.5%	0.7%	1	1	18
Ntot E	ENTREE	9	58.6 mg/l	18.5%	7.7%	1	0	8
Ntot S	SORTIE	9	36.6 mg/l	7.7%	3.2%	0	1	8
pH E	ENTREE	20	7.8	1.6%	0.4%	1	3	16
Ptot E	ENTREE	20	7.19 mg/l	5.8%	1.6%	2	1	17
Ptot S	SORTIE	20	0.32 mg/l	2.4%	0.7%	0	3	17
Snellen S	SORTIE	20	50 cm	23.2%	6.5%	0	0	20
TOC E	ENTREE	20	189 mg/l	7.8%	2.2%	2	2	16

InterSTEP 2021

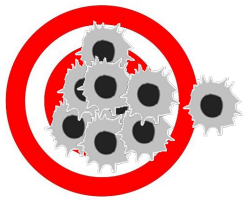
Bericht

PARAMETRES PARAMETERN		N N	Mediane Median	Ecart médian lissé (rel.) Gemittelt Medianabweichung	Incertitude sur la médiane (rel.) Median Unsicherheit	Z>2 Z>2	Z>3 Z>3
DBO5 Oxitop E	ENTREE	9	340 mg/l	21.8%	9.1%	0	1
DBO5 Oxitop S	SORTIE	8	4 mg/l	74.1%	32.8%	0	0
DBO5 Winkler E	ENTREE	12	295 mg/l	27.8%	10.0%	1	0
DBO5 Winkler S	SORTIE	11	2 mg/l	74.1%	27.9%	2	0
DCO	ENTREE	20	770 mg/l	3.2%	0.9%	1	2
DCO S	SORTIE	20	19 mg/l	6.9%	1.9%	1	1
DOC S	SORTIE	20	6.4 mg/l	16.0%	4.5%	0	0
MeS S	SORTIE	20	8 mg/l	18.5%	5.2%	2	1
N-NH4 S	SORTIE	18	0.032 mg/l	56.4%	16.6%	1	3
N-NO2 S	SORTIE	18	0.008 mg/l	61.8%	18.2%	1	2
N-NO3 S	SORTIE	20	35.2 mg/l	2.5%	0.7%	1	1
Ntot E	ENTREE	9	58.6 mg/l	18.5%	7.7%	1	0
Ntot S	SORTIE	9	36.6 mg/l	7.7%	3.2%	0	1
pH E	ENTREE	20	7.8	1.6%	0.4%	1	3
Ptot E	ENTREE	20	7.19 mg/l	5.8%	1.6%	2	1
Ptot S	SORTIE	20	0.32 mg/l	2.4%	0.7%	0	3
Snellen S	SORTIE	20	50 cm	23.2%	6.5%	0	0
TOC E	ENTREE	20	189 mg/l	7.8%	2.2%	2	2

InterSTEP 2021

Bericht

pH E								ENTREE
Laboratoire Labor	Date analyse Analyse Datum	Méthode Method	N N	Min. Min.	Max. Max.	Moyenne Mittelwert	Std Dev Std Dev	Z-score Z-score
1	21.04.2021	HQ 30 D	2	7.9	7.9	7.9	0.00	0.63
2	26.04.2021	PHC101	3	8.3	8.5	8.4	0.12	4.41
3	21.04.2021	ME-pH-013	3	7.8	7.8	7.8	0.00	-0.18
4	23.04.2021	Sonde LDO Ha	3	7.8	8	7.8	0.12	0.01
5	22.04.2021	Hach HQ 40 d	2	8	8	8	0.02	1.56
6	21.04.2021	potentiométri	2	7.8	7.8	7.8	0.02	-0.22
7	21.04.2021	sonde portativ	3	7.8	7.9	7.8	0.06	0.09
8	21.04.2021		1	7.8	7.8	7.8		-0.01
9	13.05.2021	WTW	2	7	7	7	0.01	-6.69
10	20.04.2021	WTW Multi 34	2	8	8	8	0.00	1.69
11	22.04.2021	WTW 3510 ID	1	7.8	7.8	7.8		-0.18
12	21.04.2021		2	8.1	8.2	8.1	0.01	2.62
13	21.04.2020		1	7.8	7.8	7.8		0.07
14	21.04.2021		1	7.9	7.9	7.9		0.71
15	21.04.2021	Metrohm 605	3	7.9	8	8	0.07	1.20
16	21.04.2021		1	7.8	7.8	7.8		-0.09
17	21.04.2021	WTW	1	7.8	7.8	7.8		-0.18
18	21.04.2021	Hach One	3	7.6	7.7	7.7	0.06	-1.25
19	21.04.2021	pH Meter	1	7.7	7.7	7.7		-0.90
20	21.04.2021	HQ 40 D HACH	1	7.4	7.4	7.4		-3.17



Inter... 2021

Be...

...	...	...BO5 Oxitop S					SOR...
...e Date analyse... / Analyse Datu...	...e / ...d	N / N	Min. / Min.	Max. / Max.	Moyen... / Mittelwer...	...v	Z-score / Z-score
26.04.20...		1			6 mg/l		0.62
22.04.2...	...l 250 ml	2			6 mg/l		0.77
21.04.2...		1			3 mg/l		-0.31
13.05.2...	...	2			5 mg/l		0.31
22.04.2...	...p 0-40	1			3 mg/l		-0.31
21.04.20...		1			6 mg/l		0.62
21.04.20...		1		...	1 mg/l		-0.93
21.04.202...		1	1	1	1 mg...		-0.93

... Winkler ... ...anden, aber ... ...rgebnis!...

DBO5 ...	ENTREE	9			9.1%
DBO5 Wi...	ENTREE	12	2...	27.8%	10.0%

InterSTEP 2021

Schlussfolgerungen

♥ **Kein Trend bei den Input/Output-Differenzen**

E: Kompliziertere Matrizen / S: Analyten in niedriger Konzentration

→ Kläranlagenwasseranalysen sind keine einfachen Analysen

♣ **93 % der Ergebnisse innerhalb der Zielvorgaben**

273 Ergebnisse mit einem z-Score < 2, verglichen mit 21 Ergebnissen mit einem z-Score über 2 (< 8%)

♦ **Beachtung der Sondenkalibrierung**

Kleine Lücke, große Wirkung

♠ **Einige Ausreißer**

Prüfen Sie immer die Plausibilität und zögern Sie nicht, eine zweite Analyse durchzuführen.

InterSTEP 2023

Perspektiven

Interkantonale Interlaboratorium der ARA 2023

- 2021: 96 teilnehmende Laboratorien
- Mix aus Kläranlagen und kantonalen Labors
- Zuverlässigere Statistiken

Sektion Labor und Stoffe

Fragen

Aktualitäten Gewässerschutz 2021

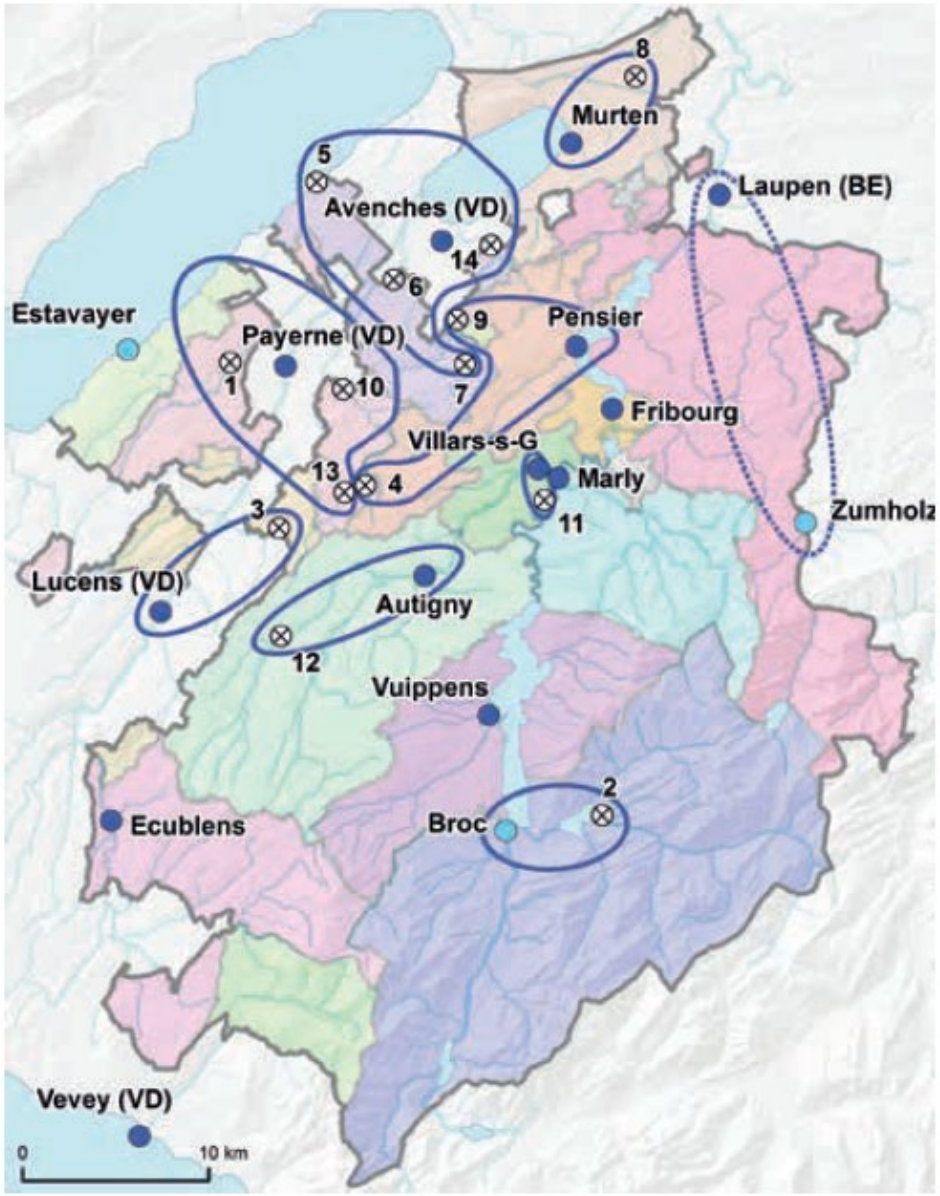
Aktualitäten Gewässerschutz

—

> Kantonale Planung:

- > Stand der ARA-**Zusammenschlüsse**
- > Stand der **laufenden Projekte**

Aktualitäten Gewässerschutz



Zentrale ARA von kantonaler Bedeutung mit Beseitigung der Mikroverunreinigungen

Zentrale ARA von kantonaler Bedeutung ohne Beseitigung der Mikroverunreinigungen

Anzuschliessende ARA

Zusammenschluss

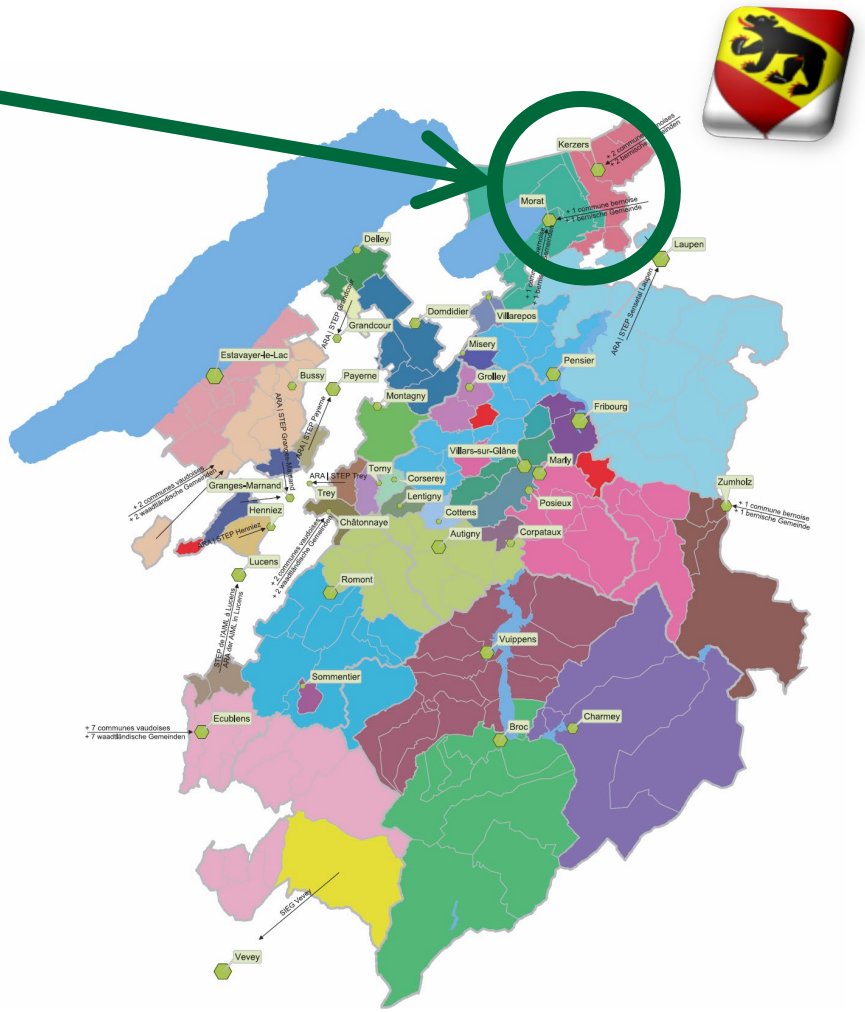
Allfälliger langfristiger Zusammenschluss

Reinigungsperimeter der ARA

1. Bussy
2. Charmey
3. Châtonnaye
4. Corserey
5. Delley
6. Domdidier
7. Grolley
8. Kerzers
9. Misery
10. Montagny
11. Posieux
12. Romont
13. Torny
14. Villarepos

Kantonale Planung der Abwasserreinigung

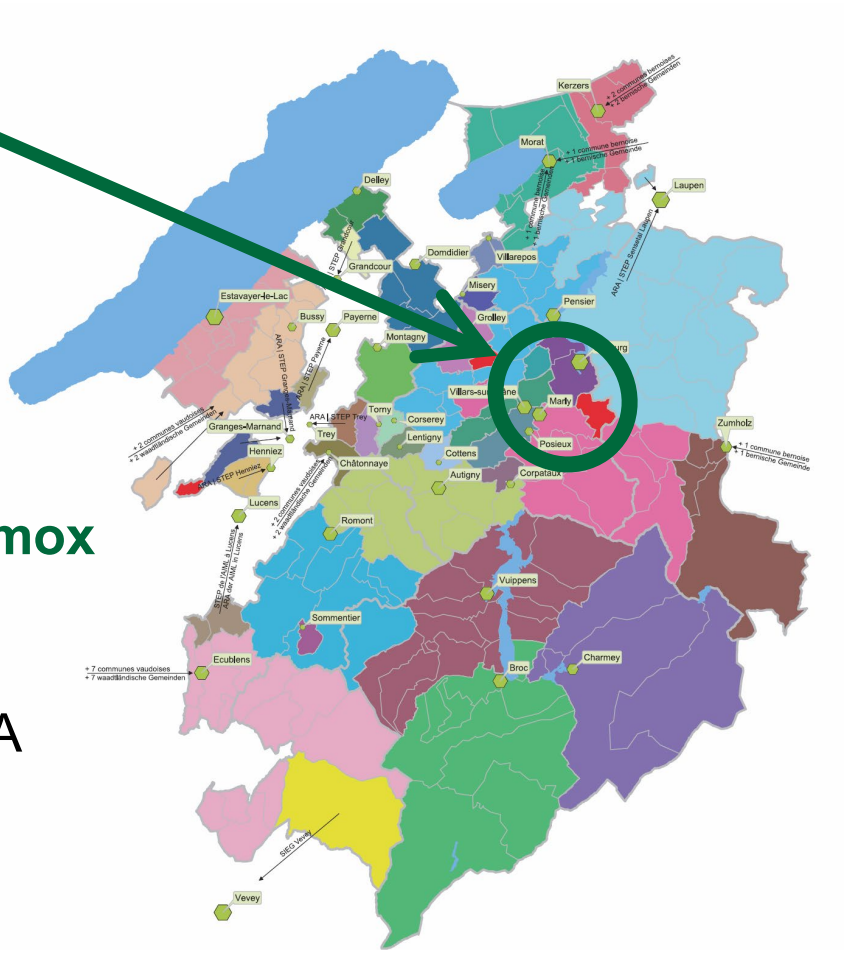
Region Seeland
ARA Kerzers, Murten, BE



Projekt **ARA Seeland Süd**:
- Ausbau: **82'000 EGW**
- Anschluss der ARA **Kerzers**
- **MV**-Behandlung mit **Ozonung und Zweischicht-Sandfiltration**

Kantonale Planung der Abwasserreinigung

Region Untere Saane
ARA Freiburg, Marly, Hauterive, Villars-s-G



ARA **Freiburg**:

- MV-Behandlung mit **Ozonung** und **Zweischicht-Sandfiltration**: Projekt in Arbeit – Bericht Voruntersuchung in Konsultation, Realisierung 2025
- Pilotversuche **Nitritation** und **Anammox**

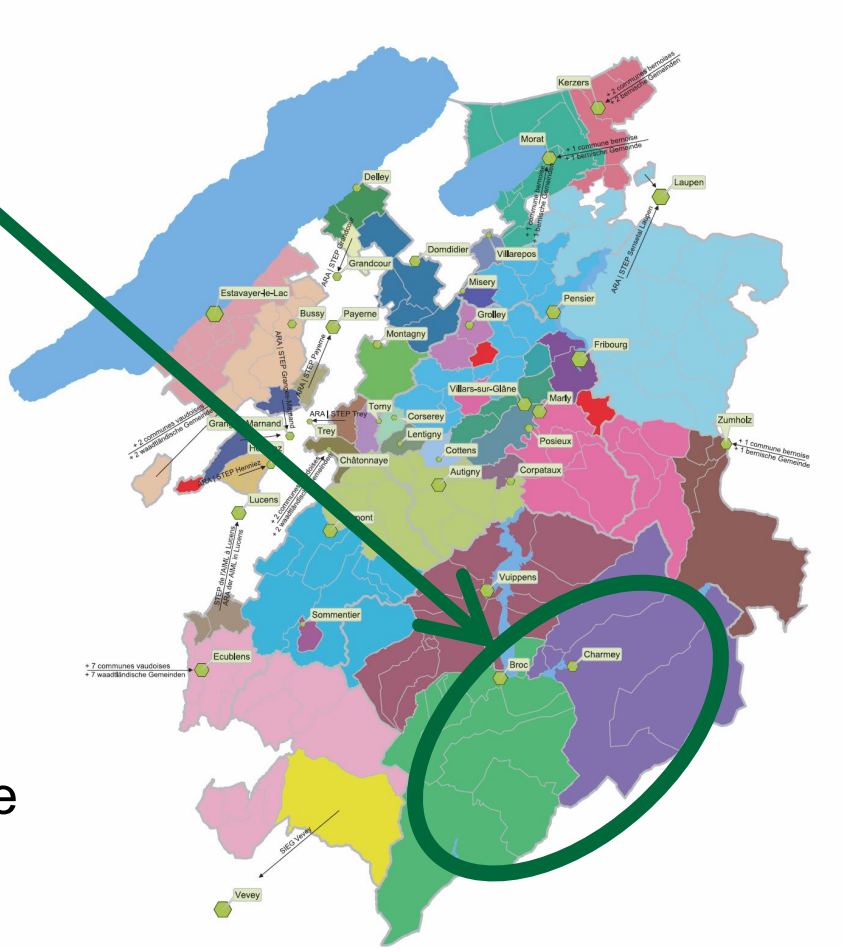
ARA **Villars-sur-Glâne**:

- Projekt **Ausbau und Sanierung** ARA 2045
- 50'000 EGW: Vorprojekt Ende 2021
- Anschluss der ARA **Posieux**: 2025

Kantonale Planung der Abwasserreinigung

Region Ober-Greyerz
ARA Broc, Charmey

- Die 2 betroffenen Verbände (AECE und AICG) prüfen **die bestmögliche Linienführung** für einen Anschluss.
- Ein neuer, für beide ARA gemeinsamer **Verteilerschlüssel**, wurde **festgelegt.**

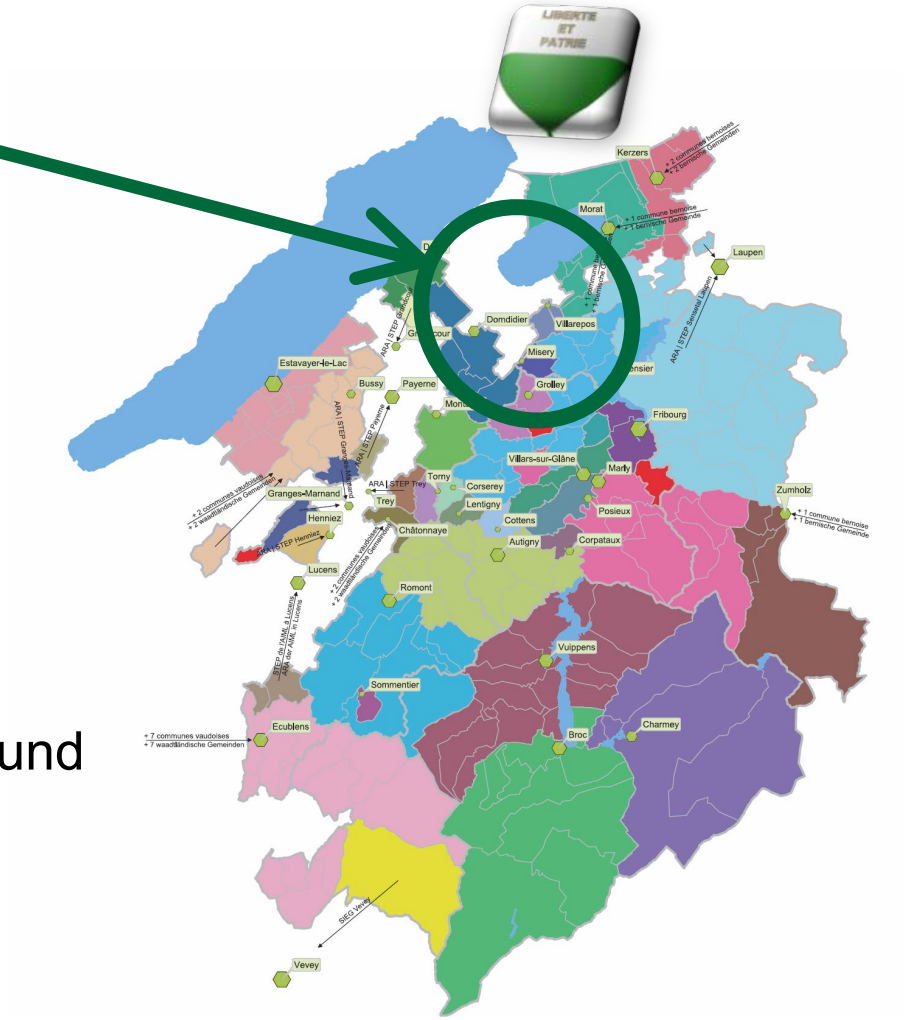


Planung:

- Gemäss Planung sollte die ARA Charmey bis **spätestens 2035** an die ARA Broc angeschlossen sein

Kantonale Planung der Abwasserreinigung

Region Avenches
ARA Belmont-Broye, Villarepos, Grolley, Delley-Portalban, + VD



Gründung **regionaler Lenkungsausschuss:**

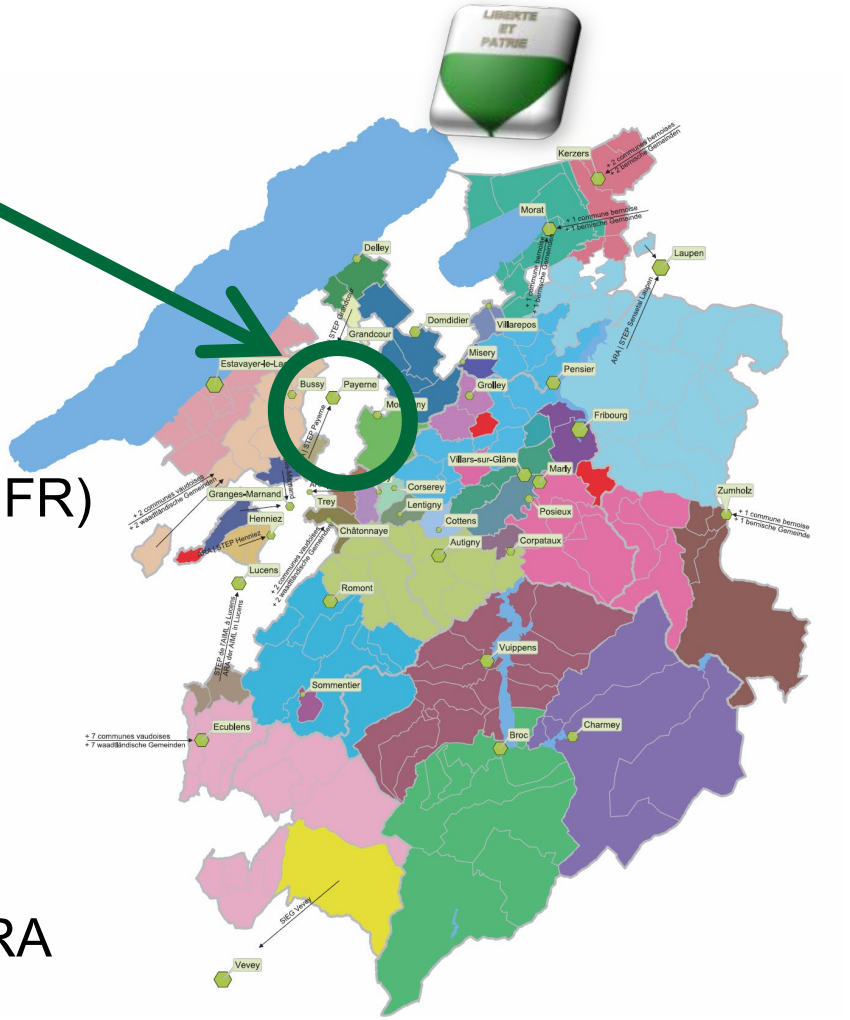
- Wahl einer **Baubegleitung**
- **Standort identifiziert**

Planung 2021-2022:

- Anpassung **Zonennutzungsplan** und weitere **technische Studien**
- Konstitutiver **politischer Prozess** (Statuten) bis **2022**

Kantonale Planung der Abwasserreinigung

Region Payerne –
ARA EPARSE (49’000 EGW)
ARA Bussy, Torny, Montagny, VD



Ab **2019:**

- **Neuer interkommunaler Verband "EPARSE"**: 16 Gemeinden (7 VD, 9 FR)
- Fortsetzung der technischen Studien unter der Führung eines **Leitungsausschusses**
- Wahl eines **Gesamtplaners**

Planung:

- «In **53 Monaten** soll die regionale ARA in Betrieb sein»

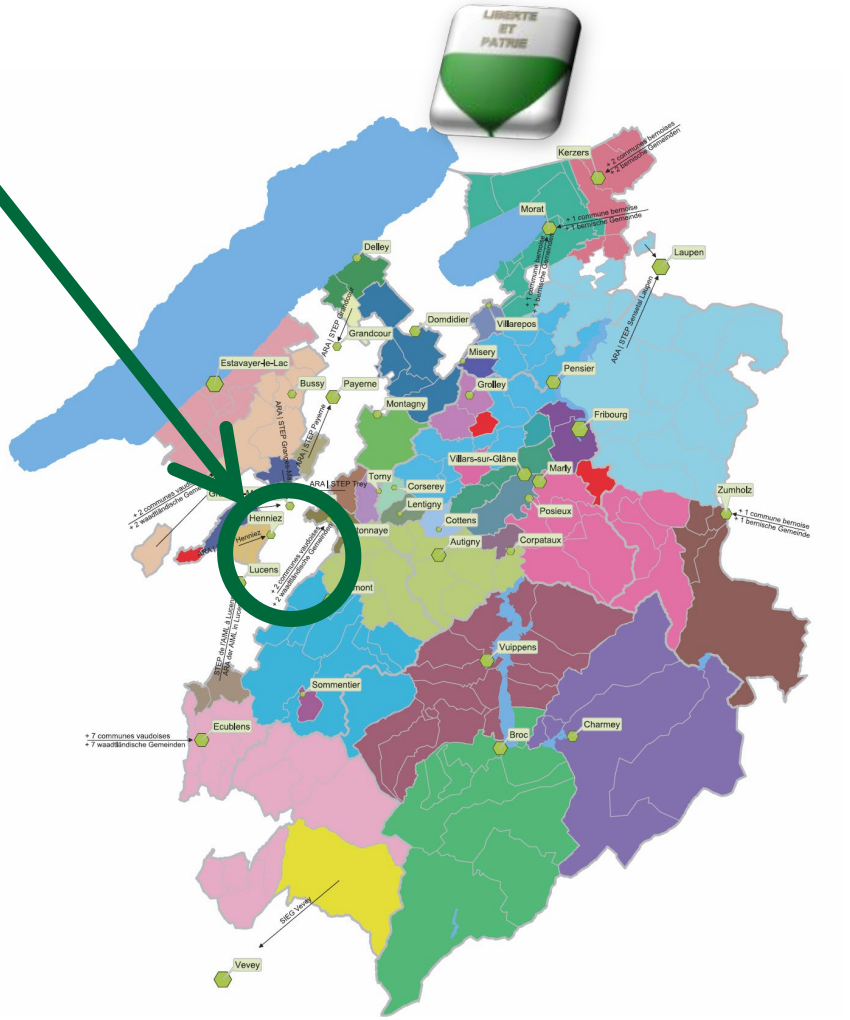
Kantonale Planung der Abwasserreinigung

Region Lucens (60'000 EGW),
ARA Châtonnaye + VD

Seit **2019:**

- **Neuer interkommunaler Verband "Eaux Moyenne Broye"**: 28 Gemeinden (22 VD, 6 FR)
- Fortsetzung der technischen Studien unter der Führung eines **Leitungsausschusses**
- Auswahl eines **Gesamtplaners**

Planung:
- Inbetriebnahme **Ende 2026**



Kantonale Planung der Abwasserreinigung

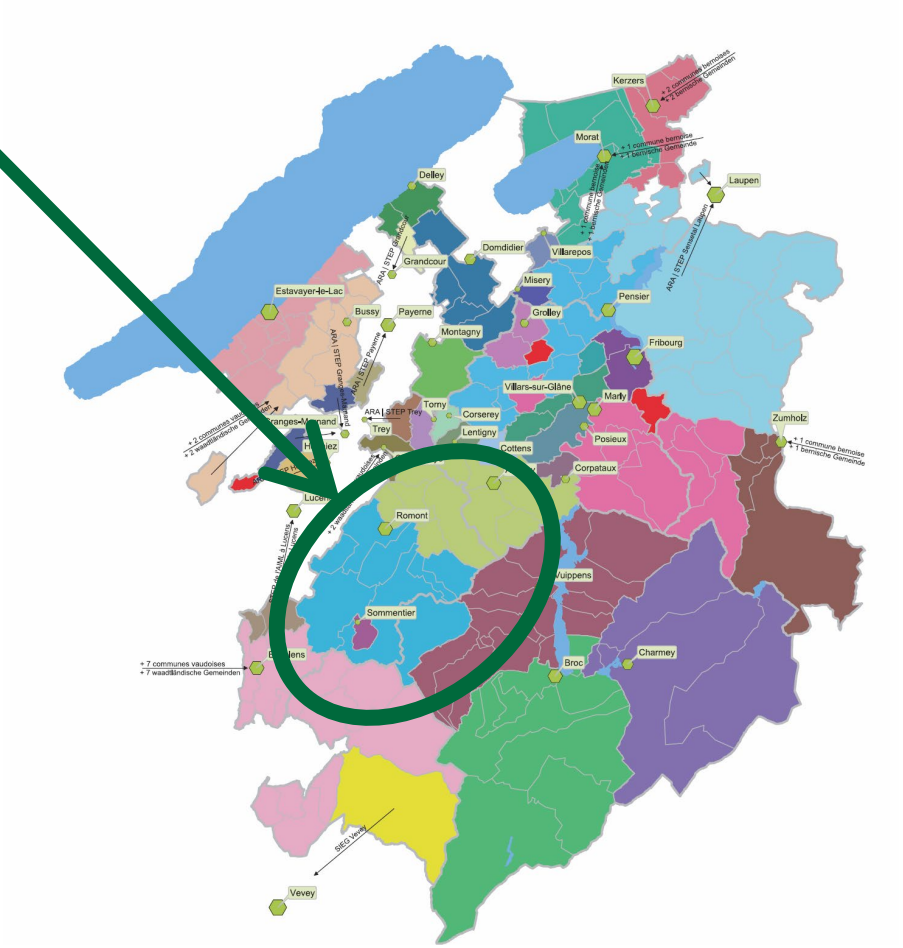
Region Glane
ARA Romont, Autigny

Grundlagenstudie abgeschlossen:

- ARA **64'000 EGW**

Im **2020/21**:

- Wahl **Baubegleitung**
- Ausarbeitung der **Statuten** des **neuen Verbands** (ABVGN)



Kantonale Planung der Abwasserreinigung

PoI regionaler Bedeutung
ARA AESC + Misery-Courtion + Corserey

Projekt **AESC 2045**:

- Studie **Ausbau** und **Anpassung an die Vorschriften** (**~50.000 EGW**)
- **Biologische** Behandlung mit **Biofiltern**
- **MV-Behandlung** mit **Ozonung** und **Sandfiltration**

Planung:

- Öffentliche Auflage im **Frühjahr 2022**
- Beginn der Arbeiten **Ende 2022**

Kantonale Planung der Abwasserreinigung

PoI regionaler Bedeutung
ARA ERES

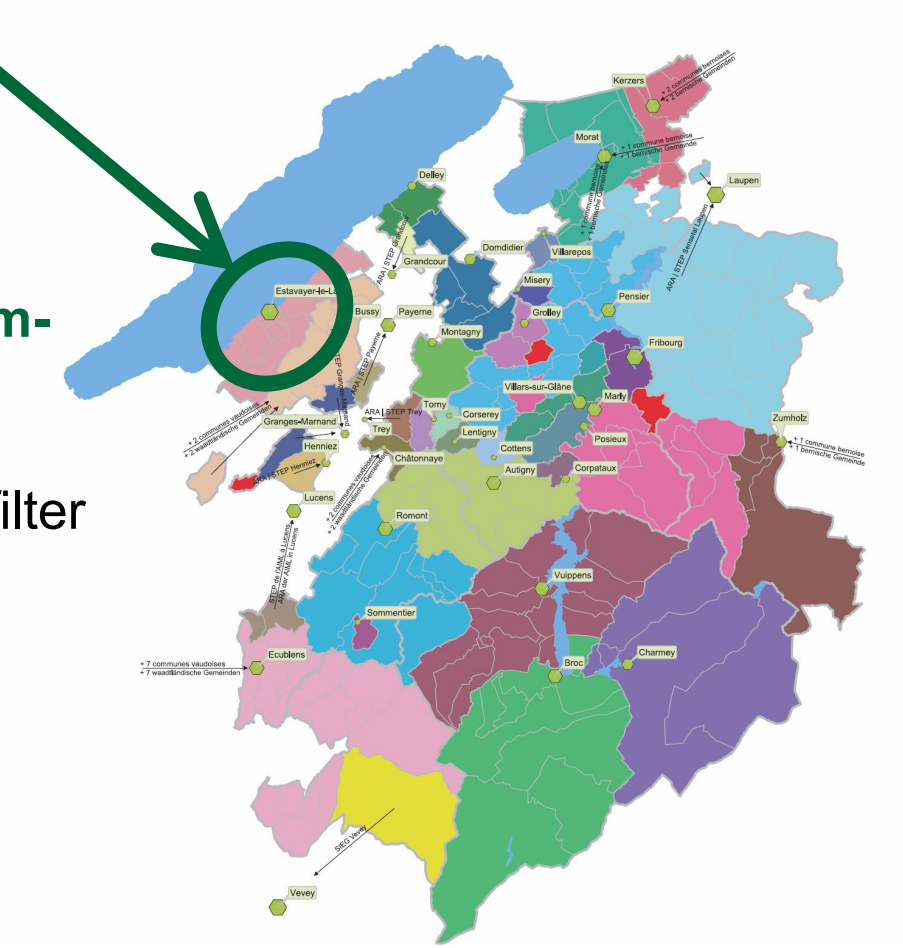
ARA Estavayer 2050 (80'000 EGW)

- Studie zur **Modernisierung** und **Sanierung** der **Biologie, Schlamm- und Gasbehandlung**

- Untersuchung von **Varianten** (Biofilter und hybride Verfahren)

Planung:

- **Abklärung** im Gange



Kantonale Planung der Abwasserreinigung

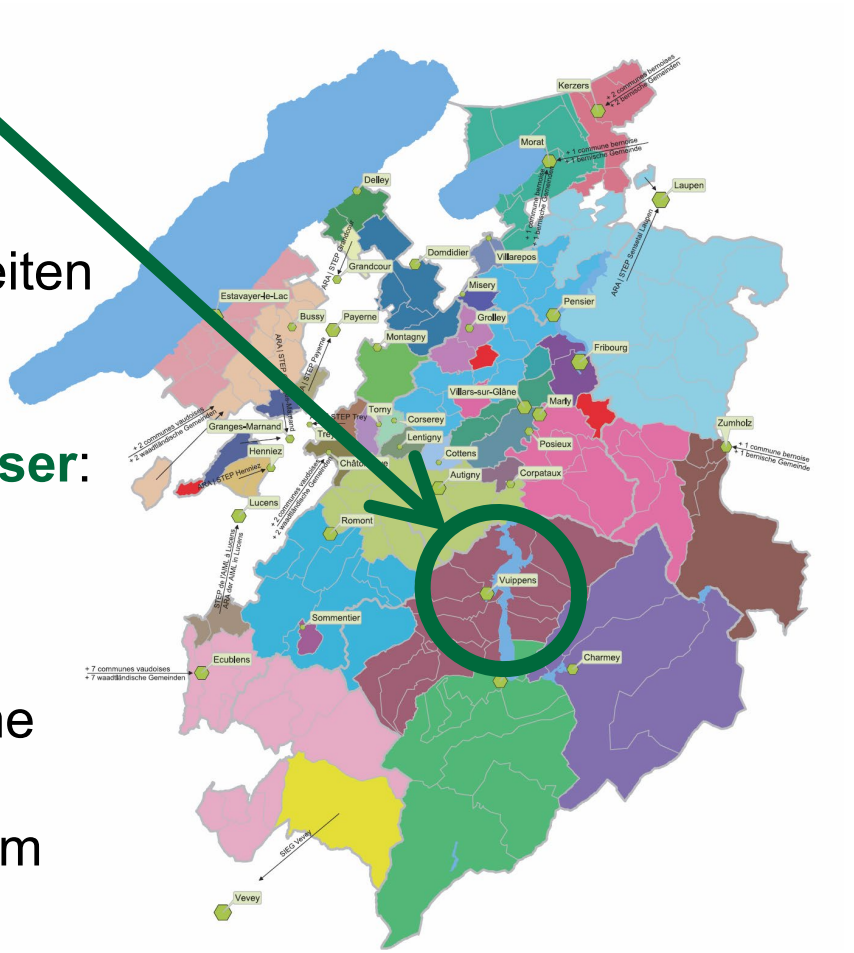
Pol regionaler Bedeutung
ARA AIS

ARA Vuippens (80'000 EW):

- Ausbau **Schlammbehandlung**: Arbeiten im Gange
- Wärmekraftwerk mit **Wärmerückgewinnung aus Abwasser**: erstes Projekt dieser Art im Kanton

Planung :

- Schlammbehandlung: Inbetriebnahme **Juni 2023**
- MV-Behandlung: **Variantenstudien** im Gange



Kantonale Planung der Abwasserreinigung

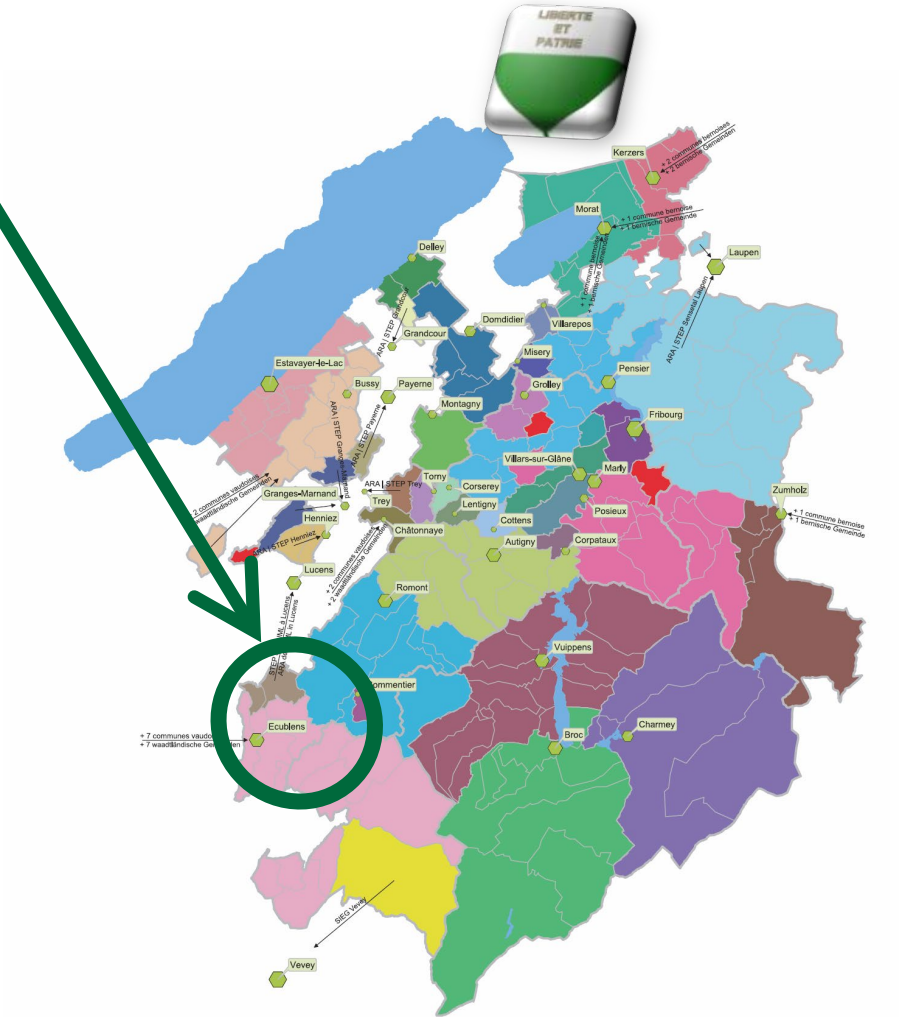
PoI regionaler Bedeutung
ARA VOG

Projekt VOG:

- Ausbau ARA **auf 48'750 EGW**

Planung:

- Erste ARA des Kantons **welche Mikroverunreinigungen** behandeln wird (Aktivkohle)
- Inbetriebnahme: Juni **2022**



Fragen?