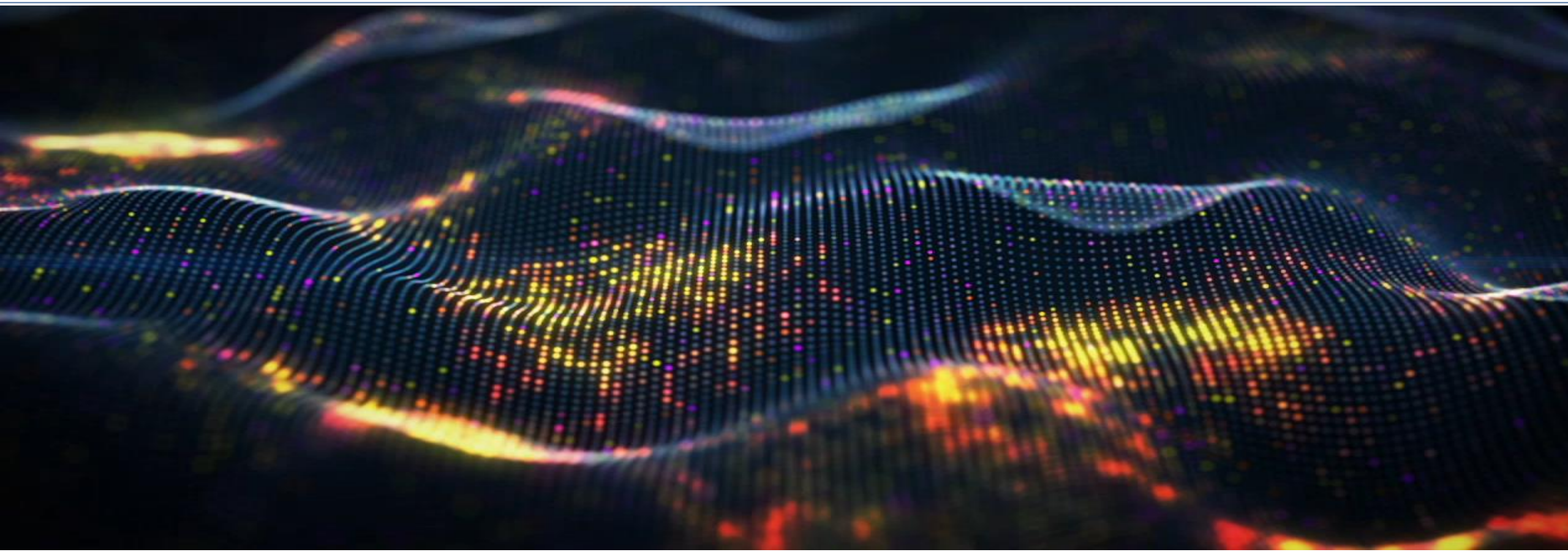
# SCHRAML Webinare – Informationssicherheit

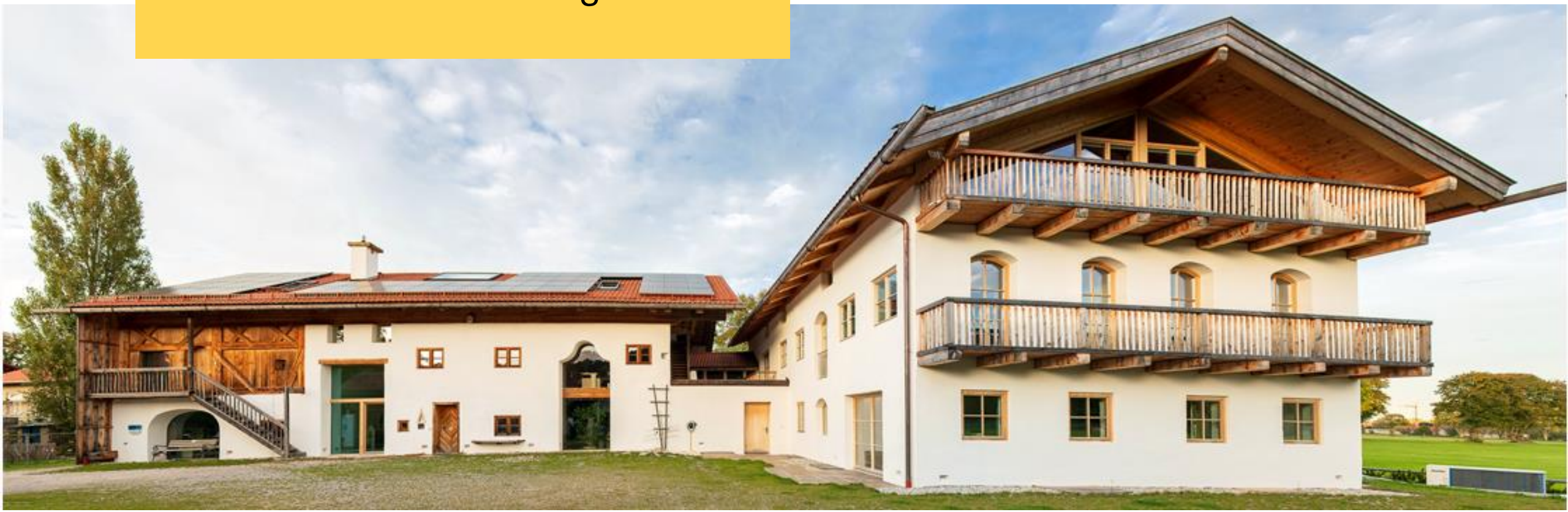


Prozessleittechnik

Fernwirktechnik

Automatisierungstechnik

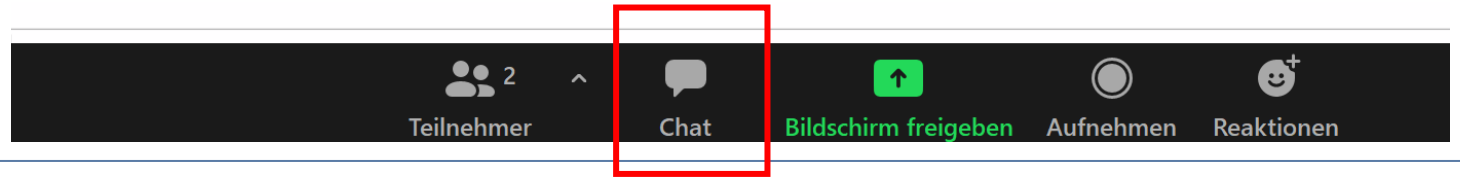
# Webinar aus Vagen



# Webinar – Orga-Basics


- Sie können uns und unseren Bildschirm sehen
- Sie können uns hören via Lautsprecher
  - oder Telefon einwählen (siehe Email-Einladung)
- Wir haben Sie alle stumm geschaltet

- Sie können uns über den **Chat** jederzeit Informationen, Fragen oder Wünsche mitteilen
- Fragen werden in den Themenblöcken dazu behandelt oder wir kommen im Nachgang direkt auf Sie zu



# Webinare

## Webinare AQASYS Prozessleitsystem via PC, Web, App und HMI

- **Mittwoch, 25. Januar 2023**
- **Mittwoch, 15. März 2023**

jeweils von 10.00 - 11.30 Uhr

## Webinare SCHRAML Fernwirktechnik, Automatisierung

- **Donnerstag, 26. Januar 2023**
- **Donnerstag, 16. März 2023**

jeweils von 10.00 - 11.30 Uhr

## NEU: Webinare IT-Sicherheit

- **Montag, 13. Februar 2023**
- **Dienstag, 28. März 2023**

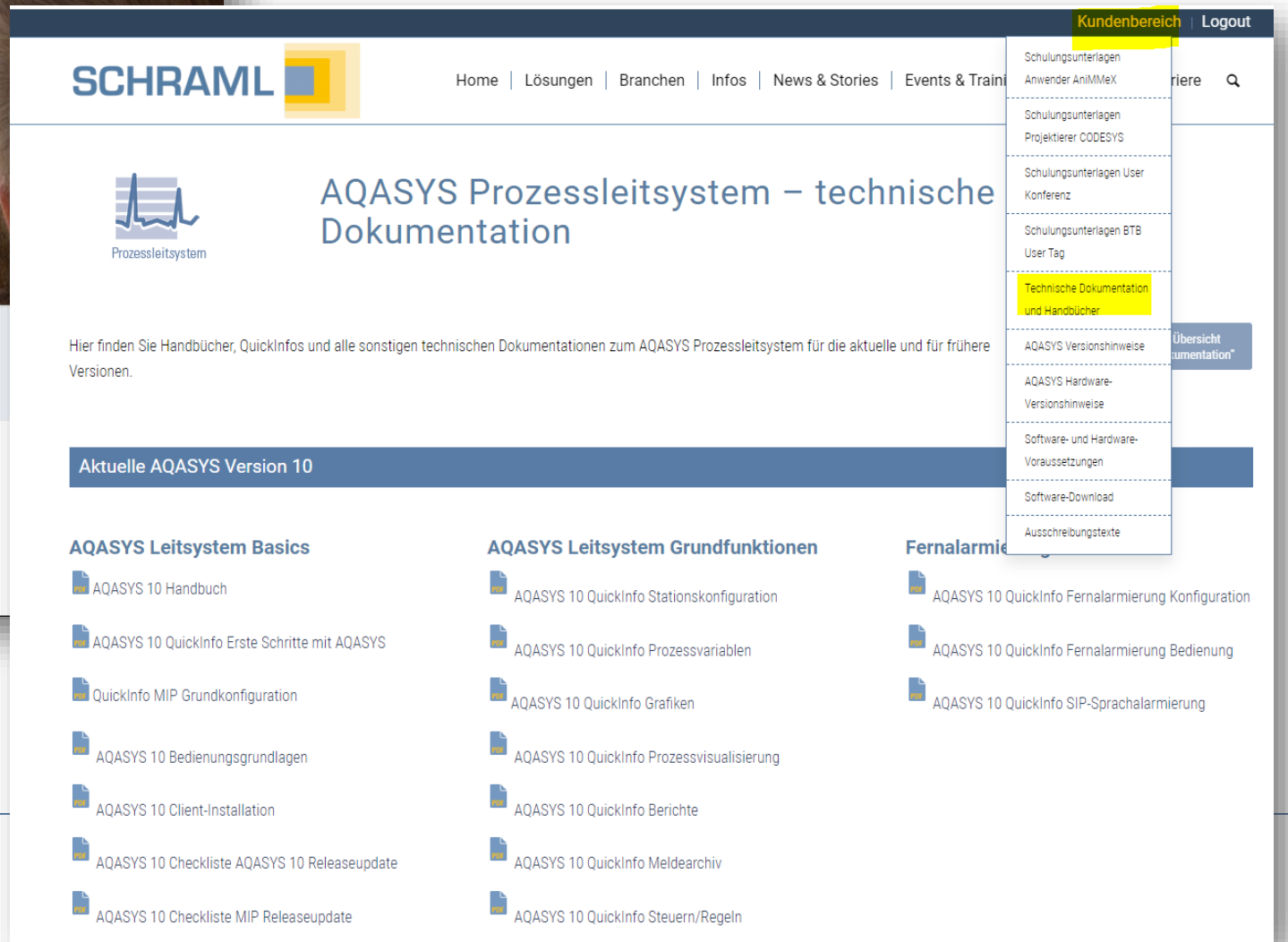
jeweils von 10.00 - 11.30 Uhr

## NEU: Webinare Kanalnetz und RÜB digital überwachen und optimieren

- **Donnerstag, 16. Februar 2023**
- **Mittwoch, 29. März 2023**

jeweils von 10.00 - 11.30 Uhr

# next stop: SCHRAML Website Kundenbereich für umfassende und schnelle Dokumentation und Infos

# Agenda

Motivation
Gesetzgebung
Richtlinien

BSI, KRITIS
DWA/DVGW

SCHRAML
Organisation

Security
„by design“


AQASYS
System

AQASYS
Web / App

Ausfall- &
Betriebs-
sicherheit

SCHRAML
Fernwirktechnik

# Agenda

Motivation
Gesetzgebung
Richtlinien

BSI, KRITIS
DWA/DVGW

SCHRAML
Organisation

Security
„by design“


AQASYS
System

AQASYS
Web / App

Ausfall- &
Betriebs-
sicherheit


SCHRAML
Fernwirktechnik

# Software & Hardware → Wir haben an vielen Stellen mit Informationssicherheit zu tun


# Grundlegende Ziele | Kontext der Informationssicherheit

# BSI – Die Lage der IT-Sicherheit in Deutschland 2021


## Die Lage der IT-Sicherheit in Deutschland 2021 im Überblick

**RANSOMWARE/DDOS**

Deutliche Ausweitung cyber-krimineller Erpressungsmethoden

Neuer Trend

+ 360 % Daten-Leak-Seiten

Schweigegeld-Erpressung

Lösegeld-Erpressung

Schutzgeld-Erpressung

**13 Tage** lang konnte ein Universitätsklinikum nach einem *Ransomware*-Angriff keine Notfall-Patienten aufnehmen.

**144 MIO.** neue Schadprogramm-Varianten

**+22 %** gegenüber 2020: **117,4 MIO.**

DURCHSCHNITTLICH **394.000** neue Schadprogramm-Varianten pro Tag (2020: 322.000)

IM HÖCHSTWERT **553.000** (2020: 470.000)

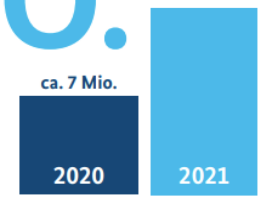
**DOPPELT SO VIELE** *BOT*-INFEKTIONEN DEUTSCHER SYSTEME pro Tag im Tagesspitzenwert

20.000 > **40.000**

**98 %** aller geprüften Systeme waren durch Schwachstellen in **MS Exchange** verwundbar.

**14,8 MIO.**

Meldungen zu Schadprogramm-Infektionen übermittelte das BSI an deutsche Netzbetreiber, mehr als **DOPPELT SO VIEL** wie im Jahr zuvor.




**44.000**

Mails mit Schadprogrammen wurden im Durchschnitt pro Monat in deutschen Regierungsnetzen abgefangen.

2020 35.000

**74.000**

Webseiten wurden wegen enthaltener Schadprogramme durch die Webfilter der Regierungsnetze gesperrt.

2020 52.000

BSI unter **TOP 3 NATIONEN** weltweit bei Common-Criteria-Zertifikaten.

**5.100** MITGLIEDER DER ALLIANZ FÜR CYBER-SICHERHEIT

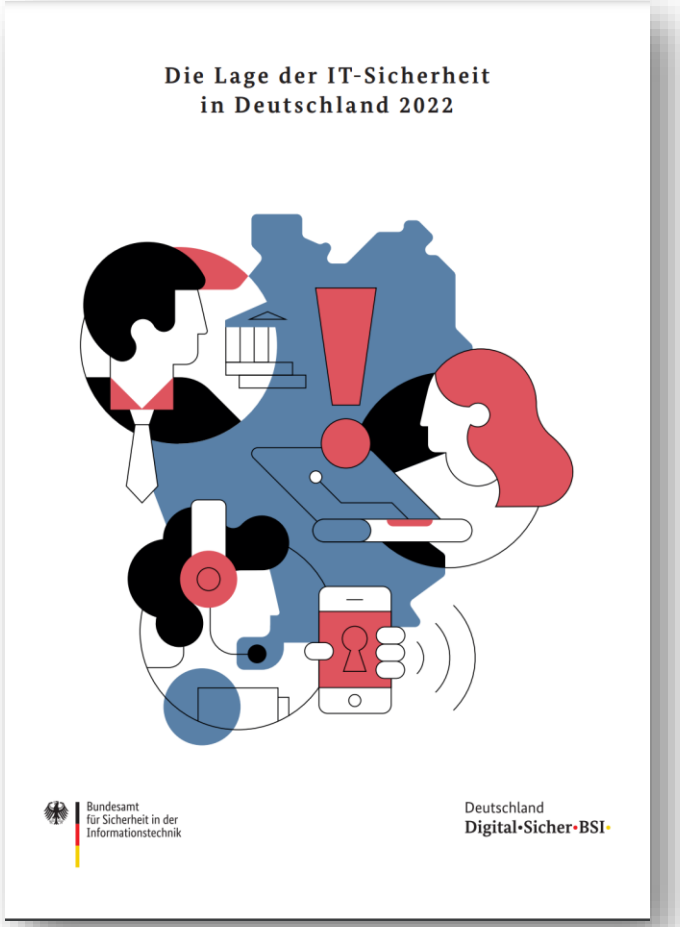
- 2020: 4.400
- 2019: 3.700
- 2018: 2.700

**< 10 %** waren nach Warnungen von BSI und Microsoft immer noch durch Schwachstellen in **MS Exchange** verwundbar.

Deutschland
Digital•Sicher•BSI•

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf;jsessionid=F54BD3FD9BFE90417377149E4091206F.internet081?__blob=publicationFile&v=3

# BSI – Die Lage der IT-Sicherheit in Deutschland 2022






Die Lage der IT-Sicherheit in Deutschland 2022
im Überblick

**Top 3-Bedrohungen je Zielgruppe:**

| Gesellschaft | Wirtschaft | Staat und Verwaltung |
|---|---|---|
| Identitätsdiebstahl<br>Sextortion<br>Fake-Shops im Internet | Ransomware<br>Schwachstellen, offene oder falsch konfigurierte Online-Server<br>IT-Supply-Chain: Abhängigkeiten und Sicherheit | Ransomware<br>APT<br>Schwachstellen, offene oder falsch konfigurierte Online-Server |

**Erster digitaler Katastrophenfall in Deutschland**

**207** Tage Katastrophenfall

Nach Ransomware-Angriff konnten Elterngeld, Arbeitslosen- und Sozialgeld, KfZ-Zulassungen und andere bürgernahe Dienstleistungen nicht erbracht werden.

**Die Anzahl der Schadprogramme steigt stetig.**
Die Anzahl neuer Schadprogramm-Varianten hat im aktuellen Berichtszeitraum um rund
**116,6** Millionen zugenommen.

**Hacktivismus im Kontext des russischen Krieges:**
Mineralöl-Unternehmen in Deutschland muss kritische Dienstleistung einschränken.

**Kollateralschaden**
nach Angriff auf Satelliten-kommunikation

**20.174**

Schwachstellen in Software-Produkten (13 % davon kritisch) wurden im Jahr 2021 bekannt. Das entspricht einem **Zuwachs von 10 %** gegenüber dem Vorjahr.



**15** Millionen Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

**34.000**
Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

**78.000**
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.

**69%**
aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z. B. Phishing-Mails und Mail-Erpressung.

**90%**
des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d. h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

BSI ist weltweit der führende Dienstleister im Bereich Common-Criteria-Zertifikate.

5.100 2021
4.400 2020

Zehn Jahre Allianz für Cyber-Sicherheit:
2022 sind wir bereits
**6.220** Teilnehmer.

Deutschland
Digital•Sicher•BSI•

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lagebericht/Lagebericht2022.pdf?__blob=publicationFile&v=6

# BSI Info: „Unzureichende Absicherung von Prozessleittechnik im KRITIS-Sektor Wasser“

TLP:GREEN

Bundesamt für Sicherheit in der Informationstechnik

Nationales IT-Lagezentrum BSI

SCHWACHSTELLE | **GEFÄHRDUNG** | VORFALL | IT-ASSETS

## Unzureichende Absicherung von Prozessleittechnik im KRITIS-Sektor Wasser

*Nr. 2018-226761-1023, Version 1.0, 18.09.2018*

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

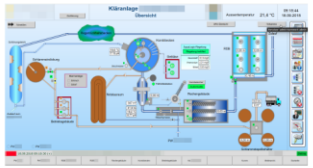
**TLP:GREEN: Organisationsübergreifende Weitergabe**

Informationen dieser Stufe dürfen innerhalb der Organisation und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

### Sachverhalt

Dem BSI liegen wiederholt Erkenntnisse vor, dass Prozessleittechnik mit Fernwartungszugang und unzureichender Authentifizierung an das Internet angebunden ist. In den aktuellen Fällen handelt es sich um vorausgefüllte Benutzernamen im Login-Formular in Kombination mit trivialen Passwörtern. Betroffen waren Pumpwerke und Kläranlagen.



* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.



BSI IT-Sicherheitsinformation



Die betroffenen Betreiber wurden durch das zuständige Landes-CERT informiert.

### Bewertung

Bei den beschriebenen Fällen handelt es sich um Implementierungsfehler. Selbst wenn Prozessleitsysteme so konfiguriert sind, dass keine Änderungen und keine physischen Schäden möglich sind und das Autorisierungskonzept sicher umgesetzt ist, können interne Informationen durch eine unsichere Authentifizierung offengelegt werden und der Betreiber möglicherweise einen Reputationsverlust erleiden.

### Maßnahmen

Prozessleittechnik sollte nicht mit unzureichender Authentifizierung offen über das Internet erreichbar sein. Falls eine Fernwartung unumgänglich ist, finden Sie in dem BSI Dokument "Fernwartung im industriellen Umfeld v2.0" [1] Hinweise zu einer sicheren Implementierung (z. B. Netzsegmentierung, Zugang via VPN etc.). Des Weiteren sind im Informationsangebot der Allianz für Cyber-Sicherheit Empfehlungen für den sicheren Einsatz von ICS-spezifischen Apps v2.0 [2], Erfahrungen aus der industriellen Sicherheitsberatung v2.0 [3], Fallbeispiele [4], [5] sowie Anforderungen an netzwerkfähige Industriekomponenten v2.0 [6] zu finden.

### Links

[1] Fernwartung im industriellen Umfeld v2.0 - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.html

[2] Sicherer Einsatz von ICS-spezifischen Apps v2.0 - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_103.html

[3] Erfahrungen aus der industriellen Sicherheitsberatung v2.0 - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_122.html

[4] ICS-Fallbeispiel: Servicetechniker - Der Virus kommt zu Fuß! v2.0 - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_095c.html

[5] ICS-Fallbeispiel: Schwimmbad - Ab heute ist jeden Tag Warmbadetag! v2.0 - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_095a.html

[6] Anforderungen an netzwerkfähige Industriekomponenten v2.0 - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_067.html





## Anlagen

### Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs) welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

### Erklärungen zum Traffic Light Protokoll (TLP)

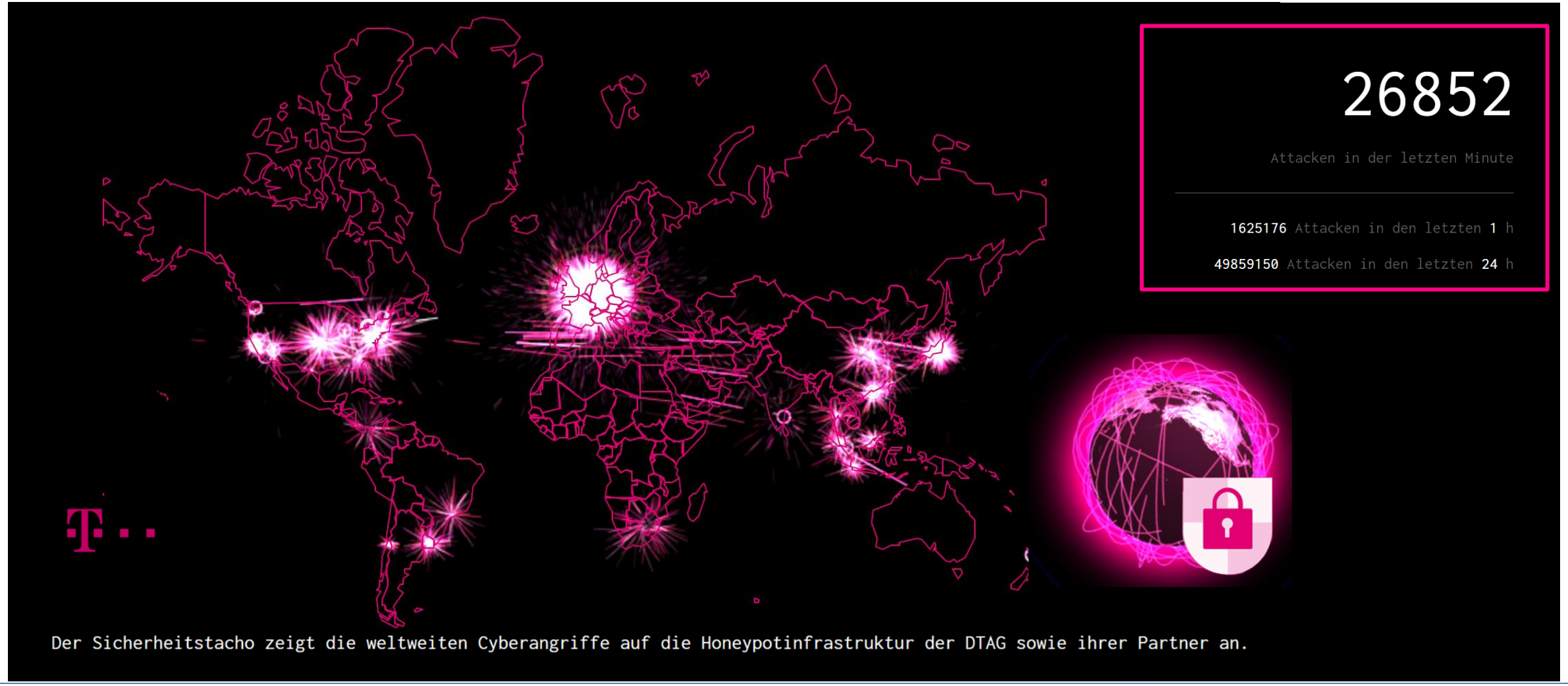
Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?
   Das TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.
2) Welche Einstufungen existieren?
   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.
3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4) Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.



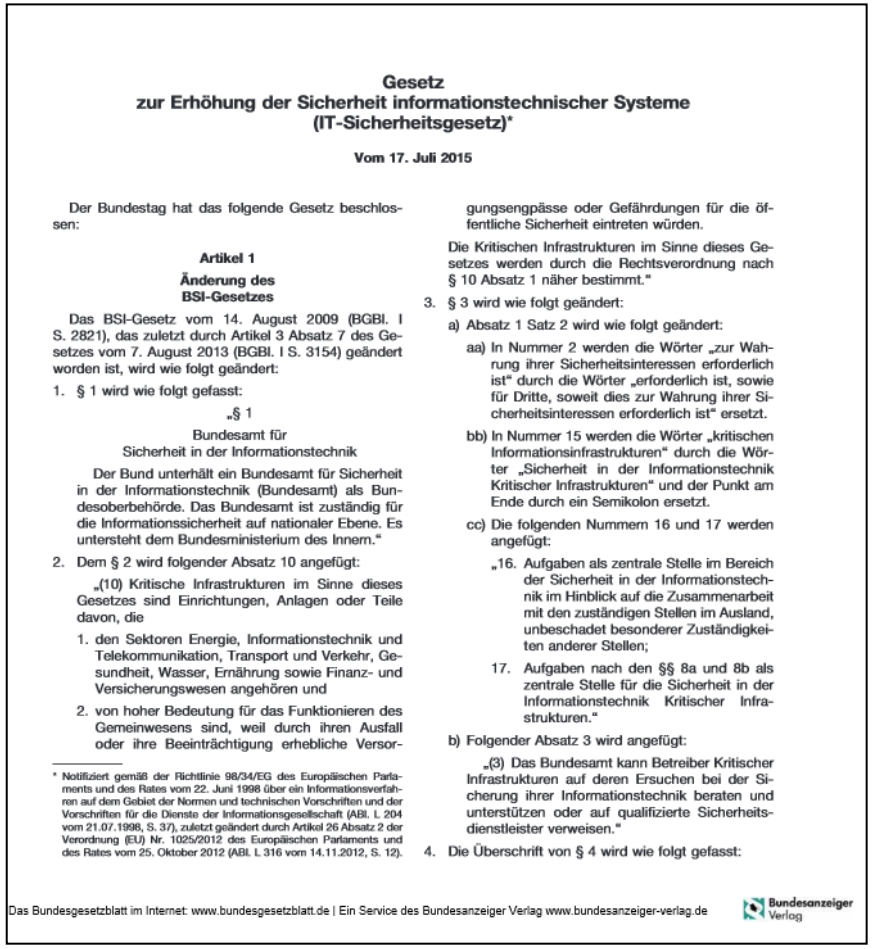
BSI-MgmtInfo-2018-226761_v1.0_VCV_TLPGREEN-1.pdf

# Live-Beispiel „Cyberangriffe“ – sicherheitstacho.eu




https://sicherheitstacho.eu/start/main

# Gesetz zur Erhöhung der Sicherheit informations-technischer Systeme (IT-Sicherheitsgesetz), 17.07.2015



**Gesetz**
**zur Erhöhung der Sicherheit informationstechnischer Systeme**
**(IT-Sicherheitsgesetz)***

**Vom 17. Juli 2015**

Der Bundestag hat das folgende Gesetz beschlossen:

**Artikel 1**

**Änderung des BSI-Gesetzes**

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„§ 1

Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern."

2. Dem § 2 wird folgender Absatz 10 angefügt:

„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt."

3. § 3 wird wie folgt geändert:

a) Absatz 1 Satz 2 wird wie folgt geändert:

aa) In Nummer 2 werden die Wörter „zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" durch die Wörter „erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist" ersetzt.

bb) In Nummer 15 werden die Wörter „kritischen Informationsinfrastrukturen" durch die Wörter „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" und der Punkt am Ende durch ein Semikolon ersetzt.

cc) Die folgenden Nummern 16 und 17 werden angefügt:

„16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen."

b) Folgender Absatz 3 wird angefügt:

„(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen."

4. Die Überschrift von § 4 wird wie folgt gefasst:

* Notifiziert gemäß der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204 vom 21.07.1998, S. 37), zuletzt geändert durch Artikel 26 Absatz 2 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 (ABl. L 316 vom 14.11.2012, S. 12).

Das Bundesgesetzblatt im Internet: www.bundesgesetzblatt.de | Ein Service des Bundesanzeiger Verlag www.bundesanzeiger-verlag.de

(§ 8a) Sicherheit in der Informationstechnik Kritischer Infrastrukturen

„Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind."

Quelle:
http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl115s1324.pdf%27%255D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1442404198243

# KA und WV | Relevante KRITIS-Anlagen

**Teil 3 Anlagenkategorien und Schwellenwerte**

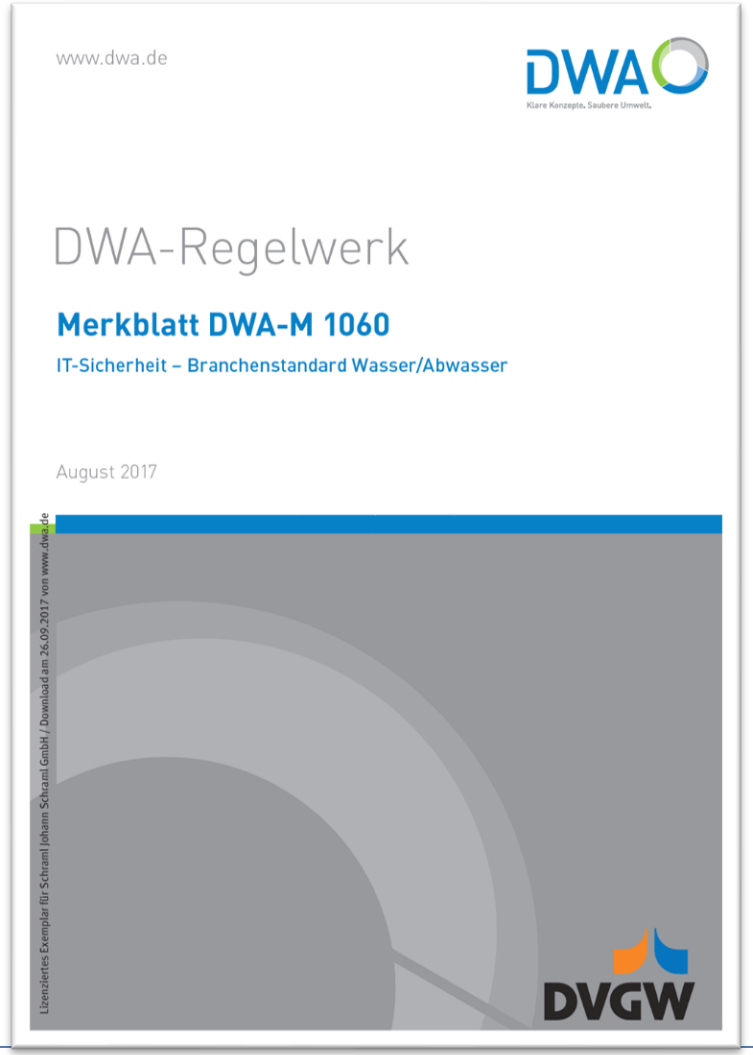
| Spalte A | Spalte B | Spalte C | Spalte D |
|---|---|---|---|
| **Nr.** | **Anlagenbezeichnung** | **Bemessungskriterium** | **Schwellenwert** |
| **1.** | **Abwasserbeseitigung** | | |
| 1.1 | Siedlungsentwässerung | | |
| 1.1.1 | Kanalisation | Angeschlossene Einwohner | 500 000 |
| 1.2 | Abwasserbehandlung und Gewässereinleitung | | |
| 1.2.1 | Kläranlage | Ausbaugröße in Einwohnergleichwerten | 500 000 |
| 1.2.2 | Leiteinrichtung | Ausbaugrößen der ge- | 500 000 |

| | | | |
|---|---|---|---|
| **2.** | **Trinkwasserversorgung** | | |
| 2.1 | Gewinnung | | |
| 2.1.1 | Gewinnungsanlage | Gewonnene Wassermenge in Mio. m³/Jahr | 21,9 |
| 2.1.2 | Wasserwerk | Wasseraufkommen in Mio. m³/Jahr | 21,9 |
| 2.2 | Aufbereitung | | |
| 2.2.1 | Aufbereitungsanlage | Aufbereitete Trinkwassermenge in Mio. m³/Jahr | 21,9 |
| 2.2.2 | Wasserwerk | Wasseraufkommen in Mio. m³/Jahr | 21,9 |
| 2.3 | Verteilung | | |
| 2.3.1 | Wasserverteilungssystem | Verteilte Wassermenge in Mio. m³/Jahr | 21,9 |
| 2.3.2 | Leiteinrichtung | Von den gesteuerten/überwachten Anlagen gewonnene, transportierte oder aufbereitete Menge Wasser in Mio. m³/Jahr | 21,9 |

Europäische Richtlinie **NIS 2 (Schutz von Netzwerk und Informationssystemen)** zum 16.01.2023 in Kraft getreten.
**Wasser und Abwasser** als einer von 11 wesentlichen (essential) Sektoren gekennzeichnet.
NIS 2 gilt für >50 Mitarbeiter, >€10 Mio. Jahresbilanz oder Umsatz, d.h. mittlere/große Unternehmen, regionale, zentrale, öffentliche Verwaltung.
Risiko- und Vorfallmanagement werden gestärkt.

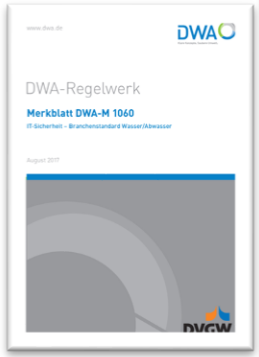
Quelle: Auszug aus Referentenentwurf 01/2016

# DWA / DVGW Merkblatt (DWA-M 1060, DVGW W 1060 IT-Sicherheit – Branchenstandard Wasser/Abwasser (B3S)




„Der **IT-Sicherheitsstandard für den Sektor Wasser** dient als Grundlage für die Risikoabschätzung und die Durchführung von Maßnahmen zum Schutz der informationstechnischen Systeme, Komponenten oder Prozesse von Wasserversorgungs- und Abwasserentsorgungsanlagen, unabhängig davon, ob eine Anlage gemäß BSI-Kritisverordnung (BSI-KritisV) als Kritische Infrastruktur eingestuft ist.“

# DWA / DVGW Merkblatt
# IT-Schutzziele




## 4.2 IT-Schutzziele

Der Schutz der informationstechnischen Systeme, Komponenten oder Prozesse verfolgt primär die allgemeinen IT-Schutzziele:

- Verfügbarkeit,
- Integrität,
- Authentizität,
- Vertraulichkeit.

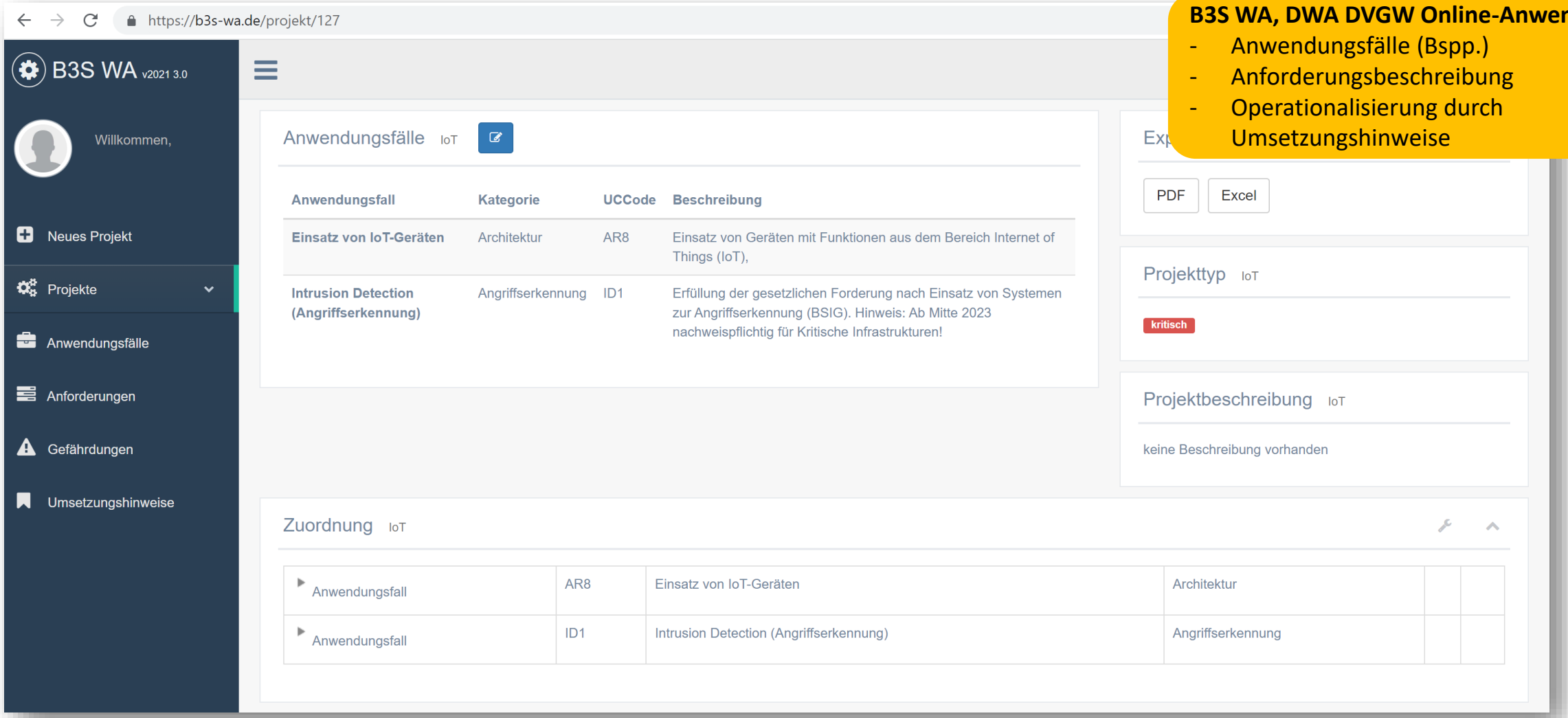
Von den allgemeinen IT-Schutzzielen differierende branchenspezifische IT-Schutzziele bestehen nicht.

Im Einzelnen bedeutet dies, dass

- Ausfälle/Ausfallzeiten der informationstechnischen Systeme, Komponenten oder Prozesse vermieden werden und ein Zugriff auf die relevanten Daten jederzeit möglich ist,
- die unautorisierte Modifikation der informationstechnischen Systeme, Komponenten oder Prozesse und ihrer Daten verhindert wird (korrekte Funktion der Systeme und Unversehrtheit der Daten),
- die Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit der Daten und ihrer Herkunft gewährleistet wird,
- die Informationen vor unbefugter Preisgabe geschützt sind.

# DWA / DVGW Merkblatt
# IT-Sicherheitsleitfaden (Online-Anwendung)

**B3S WA, DWA DVGW Online-Anwendung**
- Anwendungsfälle (Bspp.)
- Anforderungsbeschreibung
- Operationalisierung durch Umsetzungshinweise



# Operationalisierung | Bsp. DWA IT-Sicherheitsleitfaden

## Was leistet das Programm?

- Auswahl zwischen 23 Anwendungsfällen, mit denen die grundsätzliche Infrastrukturkonfiguration der IT-Systeme von Wasserver- und Abwasserentsorgungsanlagen beschrieben wird
- Generierung des dazugehörigen Anforderungskatalogs in Bezug auf die IT-Sicherheit
- Erstellung der darauf aufbauenden IT-Schutzmaßnahmen, die Sie ergreifen sollten
- Die Möglichkeit auf allen Ebenen (Anwendungsfall, Gefährdung, Maßnahme) Ergänzungen oder Modifikationen zu erstellen

## Was ist neu in der Version 3.0?

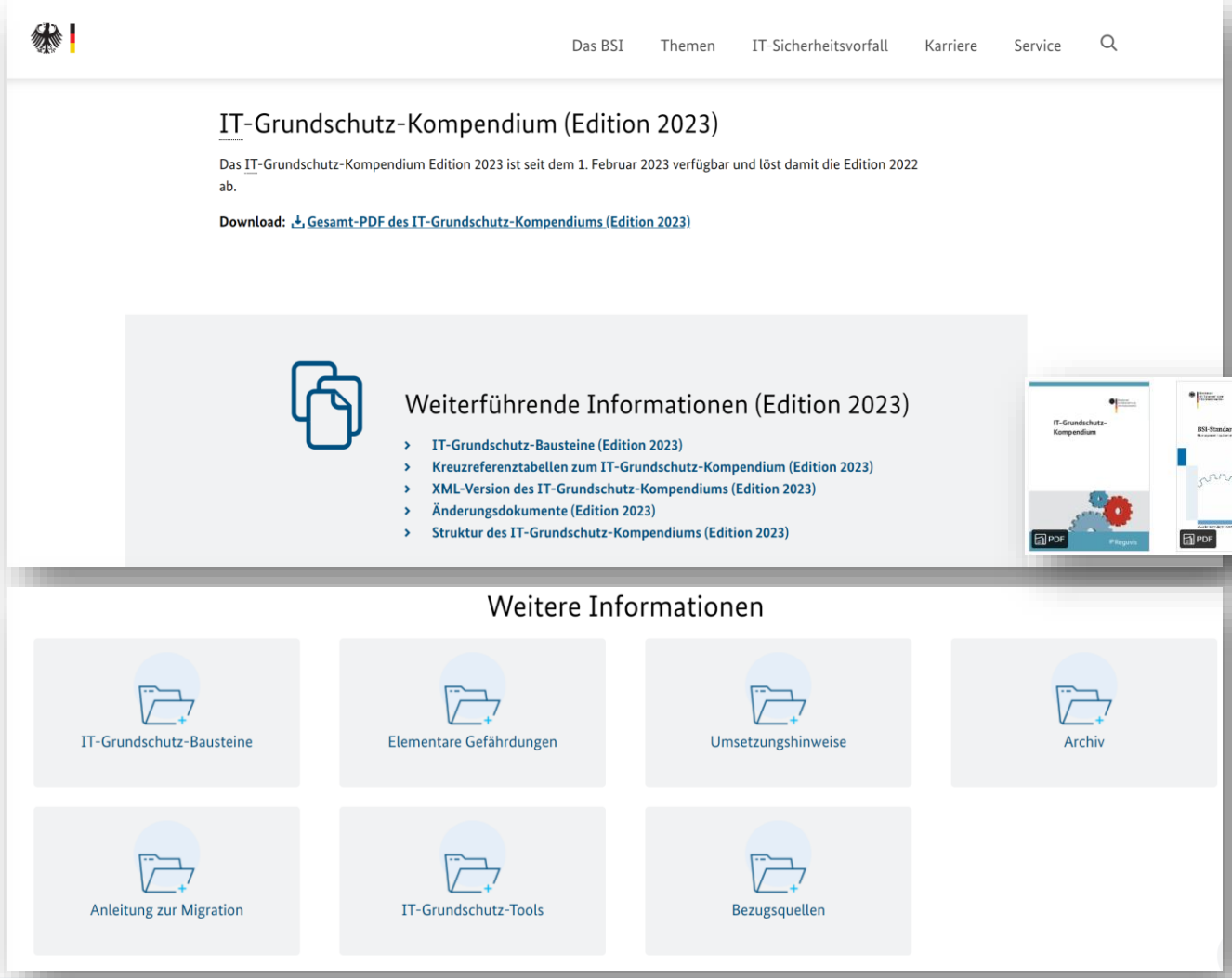
- Strukturelle Änderung, da nunmehr ausschließlich das IT- Grundschutz-Kompendium als Grundlage dient
- 4 neue Anwendungsfälle:
  - AR6 – Datenverbindung über öffentliche Netze
  - AR7 – Virtualisierung der ICS-Infrastruktur
  - AR8 – Einsatz von IoT-Geräte
  - ID1 – Intrusion Detection (Angriffserkennung)
- Ergänzung des Anwendungsfalls OM1 um Cloud-Computing
- Aktualisierung der Themen „Risikobetrachtung“ und „Restrisikobewertung“.

**B3S WA, DWA DVGW Online-Anwendung**

- Kostenpflichtiges Werkzeug
- Verpflichtender Software-Pflegevertrag
- Vergünstigungen für DWA/DVGW Mitglieder

Quelle: http://de.dwa.de/de/it-sicherheitsleitfaden.html

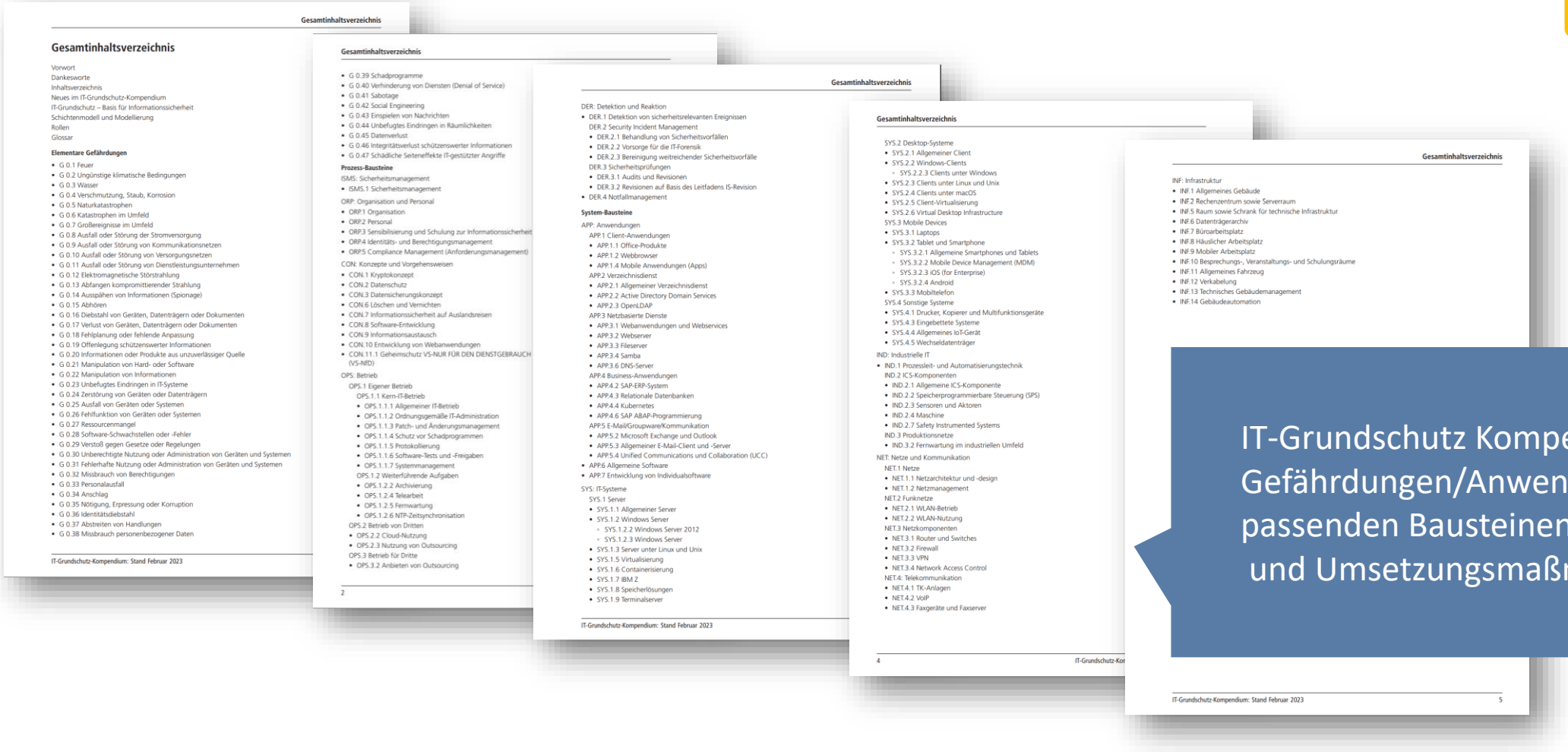
# BSI – IT-Grundschutz Kompendium


https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

# BSI – IT-Grundschutz Kompendium mit Gefährdungen, Bausteine mit Anforderungen

2023 Edition



Gesamtinhaltsverzeichnis

Vorwort
Dankesworte
Inhaltsverzeichnis
Neues im IT-Grundschutz-Kompendium
IT-Grundschutz – Basis für Informationssicherheit
Schichtenmodell und Modellierung
Rollen
Glossar

**Elementare Gefährdungen**

- G 0.1 Feuer
- G 0.2 Ungünstige klimatische Bedingungen
- G 0.3 Wasser
- G 0.4 Verschmutzung, Staub, Korrosion
- G 0.5 Naturkatastrophen
- G 0.6 Katastrophen im Umfeld
- G 0.7 Großereignisse im Umfeld
- G 0.8 Ausfall oder Störung der Stromversorgung
- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.10 Ausfall oder Störung von Versorgungsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistungsunternehmen
- G 0.12 Elektromagnetische Störstrahlung
- G 0.13 Abfangen kompromittierender Strahlung
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.33 Personalausfall
- G 0.34 Anschlag
- G 0.35 Nötigung, Erpressung oder Korruption
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten

IT-Grundschutz-Kompendium: Stand Februar 2023

Gesamtinhaltsverzeichnis

- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.43 Einspielen von Nachrichten
- G 0.44 Unbefugtes Eindringen in Räumlichkeiten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen
- G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

**Prozess-Bausteine**

ISMS: Sicherheitsmanagement
- ISMS.1 Sicherheitsmanagement

ORP: Organisation und Personal
- ORP.1 Organisation
- ORP.2 Personal
- ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
- ORP.4 Identitäts- und Berechtigungsmanagement
- ORP.5 Compliance Management (Anforderungsmanagement)

CON: Konzepte und Vorgehensweisen
- CON.1 Kryptokonzept
- CON.2 Datenschutz
- CON.3 Datensicherungskonzept
- CON.6 Löschen und Vernichten
- CON.7 Informationssicherheit auf Auslandsreisen
- CON.8 Software-Entwicklung
- CON.9 Informationsaustausch
- CON.10 Entwicklung von Webanwendungen
- CON.11.1 Geheimschutz VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD)

OPS: Betrieb
- OPS.1 Eigener Betrieb
  - OPS.1.1 Kern-IT-Betrieb
    - OPS.1.1.1 Allgemeiner IT-Betrieb
    - OPS.1.1.2 Ordnungsgemäße IT-Administration
    - OPS.1.1.3 Patch- und Änderungsmanagement
    - OPS.1.1.4 Schutz vor Schadprogrammen
    - OPS.1.1.5 Protokollierung
    - OPS.1.1.6 Software-Tests und -Freigaben
    - OPS.1.1.7 Systemmanagement
  - OPS.1.2 Weiterführende Aufgaben
    - OPS.1.2.2 Archivierung
    - OPS.1.2.4 Telearbeit
    - OPS.1.2.5 Fernwartung
    - OPS.1.2.6 NTP-Zeitsynchronisation
- OPS.2 Betrieb von Dritten
  - OPS.2.2 Cloud-Nutzung
  - OPS.2.3 Nutzung von Outsourcing
- OPS.3 Betrieb für Dritte
  - OPS.3.2 Anbieten von Outsourcing

2

Gesamtinhaltsverzeichnis

DER: Detektion und Reaktion
- DER.1 Detektion von sicherheitsrelevanten Ereignissen

DER.2 Security Incident Management
- DER.2.1 Behandlung von Sicherheitsvorfällen
- DER.2.2 Vorsorge für die IT-Forensik
- DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle

DER.3 Sicherheitsprüfungen
- DER.3.1 Audits und Revisionen
- DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision
- DER.4 Notfallmanagement

**System-Bausteine**

APP: Anwendungen

APP.1 Client-Anwendungen
- APP.1.1 Office-Produkte
- APP.1.2 Webbrowser
- APP.1.4 Mobile Anwendungen (Apps)

APP.2 Verzeichnisdienst
- APP.2.1 Allgemeiner Verzeichnisdienst
- APP.2.2 Active Directory Domain Services
- APP.2.3 OpenLDAP

APP.3 Netzbasierte Dienste
- APP.3.1 Webanwendungen und Webservices
- APP.3.2 Webserver
- APP.3.3 Fileserver
- APP.3.4 Samba
- APP.3.6 DNS-Server

APP.4 Business-Anwendungen
- APP.4.2 SAP-ERP-System
- APP.4.3 Relationale Datenbanken
- APP.4.4 Kubernetes
- APP.4.6 SAP ABAP-Programmierung

APP.5 E-Mail/Groupware/Kommunikation
- APP.5.2 Microsoft Exchange und Outlook
- APP.5.3 Allgemeiner E-Mail-Client und -Server
- APP.5.4 Unified Communications und Collaboration (UCC)
- APP.6 Allgemeine Software
- APP.7 Entwicklung von Individualsoftware

SYS: IT-Systeme

SYS.1 Server
- SYS.1.1 Allgemeiner Server
- SYS.1.2 Windows Server
  - SYS.1.2.2 Windows Server 2012
  - SYS.1.2.3 Windows Server
- SYS.1.3 Server unter Linux und Unix
- SYS.1.5 Virtualisierung
- SYS.1.6 Containerisierung
- SYS.1.7 IBM Z
- SYS.1.8 Speicherlösungen
- SYS.1.9 Terminalserver

IT-Grundschutz-Kompendium: Stand Februar 2023

Gesamtinhaltsverzeichnis

SYS.2 Desktop-Systeme
- SYS.2.1 Allgemeiner Client
- SYS.2.2 Windows-Clients
  - SYS.2.2.3 Clients unter Windows
- SYS.2.3 Clients unter Linux und Unix
- SYS.2.4 Clients unter macOS
- SYS.2.5 Client-Virtualisierung
- SYS.2.6 Virtual Desktop Infrastructure

SYS.3 Mobile Devices
- SYS.3.1 Laptops
- SYS.3.2 Tablet und Smartphone
  - SYS.3.2.1 Allgemeine Smartphones und Tablets
  - SYS.3.2.2 Mobile Device Management (MDM)
  - SYS.3.2.3 iOS (for Enterprise)
  - SYS.3.2.4 Android
- SYS.3.3 Mobiltelefon

SYS.4 Sonstige Systeme
- SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
- SYS.4.3 Eingebettete Systeme
- SYS.4.4 Allgemeines IoT-Gerät
- SYS.4.5 Wechseldatenträger

IND: Industrielle IT
- IND.1 Prozessleit- und Automatisierungstechnik

IND.2 ICS-Komponenten
- IND.2.1 Allgemeine ICS-Komponente
- IND.2.2 Speicherprogrammierbare Steuerung (SPS)
- IND.2.3 Sensoren und Aktoren
- IND.2.4 Maschine
- IND.2.7 Safety Instrumented Systems

IND.3 Produktionsnetze
- IND.3.2 Fernwartung im industriellen Umfeld

NET: Netze und Kommunikation

NET.1 Netze
- NET.1.1 Netzarchitektur und -design
- NET.1.2 Netzmanagement

NET.2 Funknetze
- NET.2.1 WLAN-Betrieb
- NET.2.2 WLAN-Nutzung

NET.3 Netzkomponenten
- NET.3.1 Router und Switches
- NET.3.2 Firewall
- NET.3.3 VPN
- NET.3.4 Network Access Control

NET.4: Telekommunikation
- NET.4.1 TK-Anlagen
- NET.4.2 VoIP
- NET.4.3 Faxgeräte und Faxserver

4

Gesamtinhaltsverzeichnis

INF: Infrastruktur
- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.5 Raum sowie Schrank für technische Infrastruktur
- INF.6 Datenträgerarchiv
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume
- INF.11 Allgemeines Fahrzeug
- INF.12 Verkabelung
- INF.13 Technisches Gebäudemanagement
- INF.14 Gebäudeautomation

IT-Grundschutz-Kompendium: Stand Februar 2023 5

IT-Grundschutz Kompendium
Gefährdungen/Anwendungsfälle mit passenden Bausteinen, Anforderungen und Umsetzungsmaßnahmen

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf?__blob=publicationFile&v=5
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzDownloads/itgrundschutzDownloads_node.html;jsessionid=F32F65D00DDC6F7F4965E3BD7CD240F0.1_cid341

# Umsetzungshilfen im KRITIS Sektor | Bsp. LSI Bayern

1

Landesamt für Sicherheit in der Informationstechnik

**"IT-Sicherheit in der Trinkwasserversorgung in Bayern"**

- Checkliste zur Mindestabsicherung -


**Landesamt für Sicherheit in der Informationstechnik**
Referat Beratung öffentlicher KRITIS-Betreiber
Keßlerstraße 1
90489 Nürnberg
Telefon: 0911 21549-525
Mail: beratung-kritis@lsi.bayern.de
Web: lsi.bayern.de

2

**Information**

Die Bedeutung einer abgesicherten IT-Landschaft wächst mit jedem Tag und jeder Bedrohung. Mit dieser Checkliste ist es einfach möglich, den aktuellen Stand Ihrer bestehenden Absicherung grundlegend zu überprüfen. Sie können dadurch eventuelles Verbesserungspotential erkennen oder auch Ergebnisse als Argumentationshilfe gegenüber Entscheidungsträgern nutzen. Sollten Sie Aufgabengebiete nach extern ausgelagert haben, so müssen Sie sicherstellen, dass Ihr / Ihre Dienstleister die Sicherheitsanforderungen ebenfalls einhält / einhalten. Hier kann die Checkliste helfen, die wichtigsten Anforderungen im Blick zu behalten. Es empfiehlt sich, sofern vorhanden, die Checkliste gemeinsam mit Ihrem Dienstleister zu bearbeiten und die Resultate mit den/m verantwortlichen Wassermeister/n sowie der Geschäftsleitung durchzusprechen. Wir beraten Sie gerne zu den einzelnen Punkten und hoffen mit Ihnen zusammen und mit unseren modular aufbauenden Konzepten Schritt für Schritt in eine sichere Zukunft zu starten.
Nach Umsetzung der Mindestabsicherung empfehlen wir zum weiteren Ausbau der Informationssicherheit z.B. mit der LSI-Handlungsempfehlung "IT-Sicherheit in der Trinkwasserversorgung in Bayern", ISIS12, ISO 27001, BSI IT-Grundschutz oder dem branchenspezifischen Sicherheitsstandard Wasser/Abwasser weiterzuarbeiten.

3

**Zielgruppe**

Kleine Trinkwasserversorger in Bayern.

**Schutzziele**

Das oberste Gebot im Rahmen dieses Werks stellt die Versorgungssicherheit der Bevölkerung mit Trinkwasser dar.
Besonders berücksichtigt werden weiterhin die folgenden übergeordneten Schutzziele: Verfügbarkeit, Integrität und Vertraulichkeit.

4

**Inhalt**

| Status | |
|---|---|
| | **1. Dokumentation** |
| | 1.1 Dokumentation |
| | **2. Technische Vorgehensweise** |
| | 2.1 Netztrennung des Leittechniknetzes |
| | 2.2 Fernzugänge für eigene Mitarbeiter |
| | 2.3 Fernwartung durch externe Dienstleister |
| | 2.4 Bei Auslagerung der Prozessleit- und Steuerungstechnik (nur falls erfolgt) |
| | 2.5 Schutz vor physischen Schäden |
| | 2.6 Datensicherung |
| | 2.7 Systemverfügbarkeit |
| | 2.8 Autorisierung der Zugriffe |
| | 2.9 Lokaler Manipulationsschutz |
| | 2.10 Koordinierte und geprüfte Konfigurations- und Update-Prozeduren |
| | 2.11 Regelmäßige Systemüberprüfungen |
| | **3. Organisatorische und personelle Maßnahmen** |
| | 3.1 Organisation / ISMS |
| | 3.2 Vorgehen bei einem Verdacht auf einen IT-Sicherheitsvorfall |
| | 3.3 Personelle Maßnahmen |

Quelle: https://www.lsi.bayern.de/mam/aktuelles/checkliste_zur_mindestabsicherung_trinkwasserversorgung_v1.0.xlsx

# Agenda

Motivation
Gesetzgebung
Richtlinien

BSI, KRITIS
DWA/DVGW

SCHRAML
Organisation

Security
„by design“

AQASYS
System

AQASYS
Web / App

Ausfall- &
Betriebs-
sicherheit

SCHRAML
Fernwirktechnik

# SCHRAML | Informationssicherheit Umfangreiche organisatorische u. technische Maßnahmen, Mitgliedschaften, etc.

QZV
Verein zur Qualitätssicherung und Zertifizierung für den Mittelstand e.V.

QZV DIN ISO/IEC 27001:2017

**ZERTIFIKAT**

Der Verein zur Qualitätssicherung und Zertifizierung für den Mittelstand e.V. bescheinigt, dass das Unternehmen

**SCHRAML GMBH**
**Herxheimer Str. 7**
**D - 83620 Vagen**

ein Informationssicherheits-Management-System entsprechend der DIN ISO/IEC 27001:2017 eingerichtet hat und unterhält. Der Nachweis wurde in einem Audit erbracht.

Prüfbericht-Nummer: **04619331**

erstellt durch: Prof. Dr.-Ing. Dieter Deublein

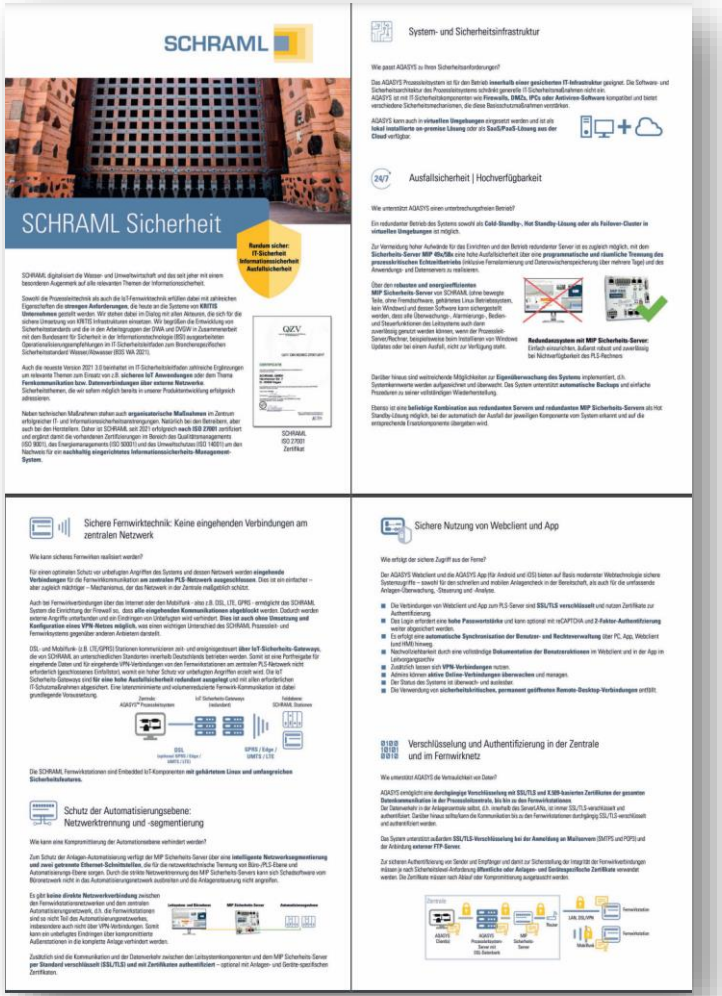
Dieses Zertifikat wurde ausgestellt am: 17.12.2021 und gilt bis zum: 16.12.2024
Zertifikat-Registernummer: **04519331**

für den QZV Prof.Dr.-Ing. Gerhard Knauer

QZV e.V. Schlierseestr. 46, 81539 München
Registrierungsnummer 33150102 (AICB e.V.)

ACB

Allianz für Cyber-Sicherheit

SCHRAML

SCHRAML Sicherheit

System- und Sicherheitsinfrastruktur

Ausfallsicherheit | Hochverfügbarkeit

Sichere Fernwirktechnik: Keine eingehenden Verbindungen am zentralen Netzwerk

Sichere Nutzung von Webclient und App

Schutz der Automatisierungsebene: Netzwerktrennung und -segmentierung

Verschlüsselung und Authentifizierung in der Zentrale und im Fernwirknetz

# Ext. Prüfung | Penetrationstest “Pen Test“durch SySS im Betreiberauftrag

ZERTIFIKAT
PENETRATIONSTEST

SySS THE PENTEST EXPERTS.

Die

**SySS GmbH**
**Schaffhausenstraße 77**
**72072 Tübingen**

bestätigt hiermit, dass sie für das Unternehmen

[redacted]
**Wasser- und Abwasserbetriebe gKU**
[redacted]

einen Penetrationstest durchgeführt hat.

**Prüfgegenstand:**

- Prozessleittechnik-Webanwendung der Abwasserentsorgung
- Prozessleittechnik-Webanwendung der Wasserversorgung

inklusive zugrunde liegender Systeme

**Prüfzeitraum:** 14. bis 28. Juli 2022

**Prüftiefe/Widerstandszeit:** Der simulierte Angriff dauerte fünf Personentage (reine Testzeit).

**Zusammenfassende Prüfergebnisse:** Nach Abschluss aller Testaktivitäten bestätigt die SySS GmbH, dass die identifizierten, relevanten Schwachstellen erfolgreich beseitigt wurden.

**Empfehlung:** Die SySS GmbH empfiehlt, den Prüfgegenstand nach jeder signifikanten Änderung oder spätestens nach einem Jahr einer erneuten Prüfung zu unterziehen.

Tübingen, den 22. September 2022

Sebastian Schreiber
(Geschäftsführer)

Florian Kock
(Projektleiter)

Erfolgreicher Pen-Test
von zwei AQASYS Anlagen
(Web, Desktop, HMI, etc.).

1x in der SCHRAML Cloud
1x „on Premise“, lokal vor Ort,
administriert durch den Betreiber

# Agenda

Motivation
Gesetzgebung
Richtlinien

BSI, KRITIS
DWA/DVGW

SCHRAML
Organisation

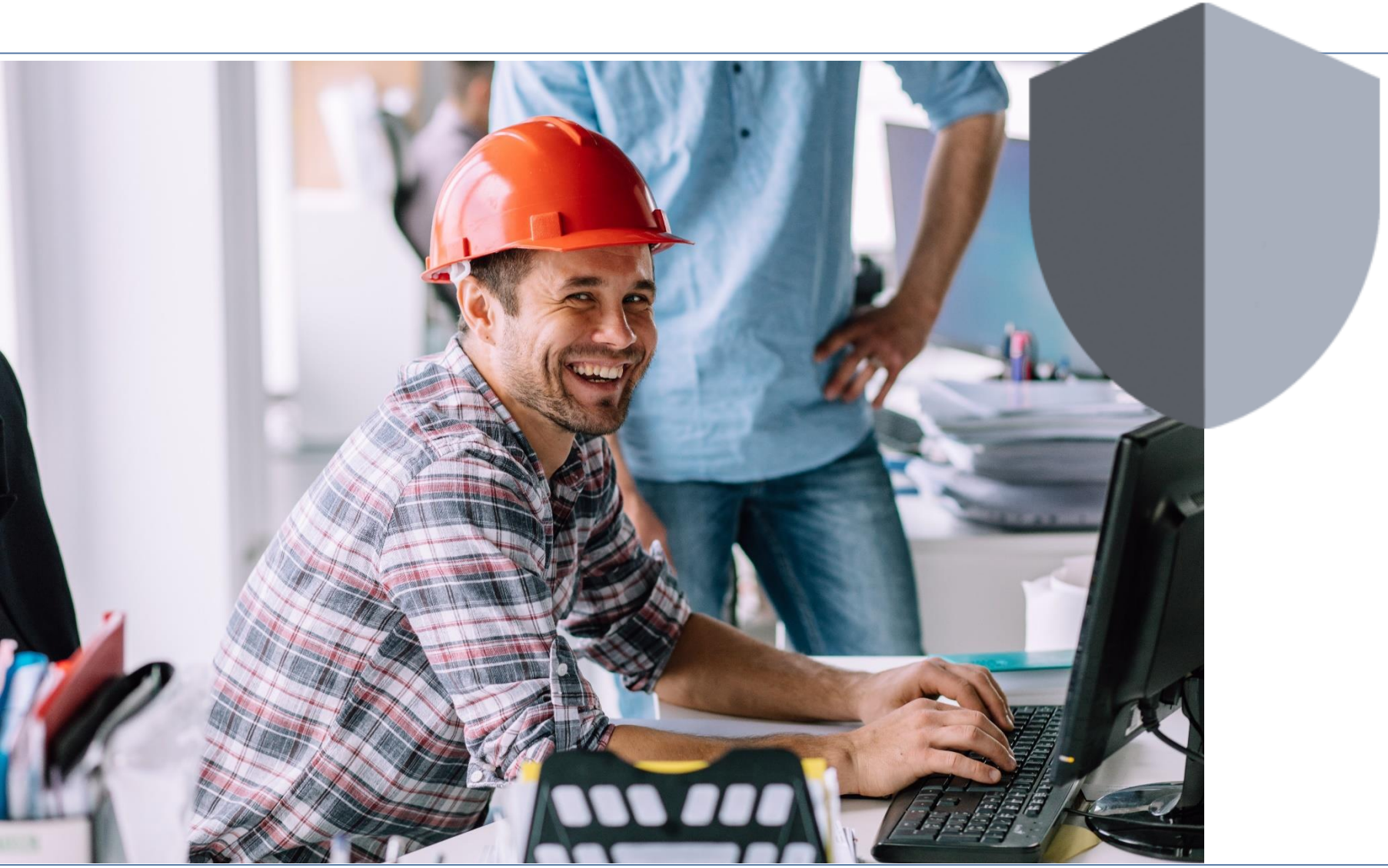
Security
„by design“


AQASYS
System

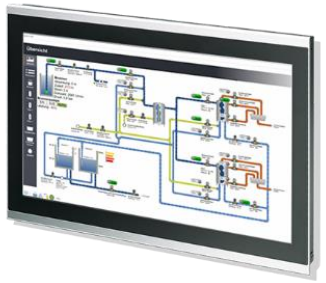
AQASYS
Web / App

Ausfall- &
Betriebs-
sicherheit

SCHRAML
Fernwirktechnik




MIP 588
SCHRAML



# AQASYS in vielfältigen Integrations-Szenarien lauffähig (mit entsprechenden Anforderungen)

## Einzel-/Mehrplatz, Client/Server (on premise)

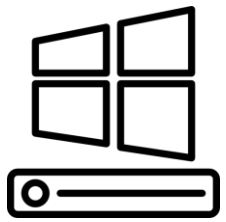
## SCHRAML Cloud

## Virtuelle Umgebung


## „by Design“

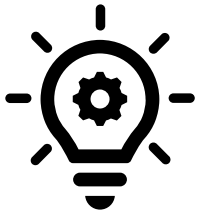
- AQASYS = unterstützt vielfältige Integrations-Szenarien
- AQASYS = kompatibel mit aktuellen IT-Standards u. Sicherheitskomponenten wie **aktuellen Betriebssystemen, SQL-Datenbanken, virtuellen Servern, Firewalls, DMZs, IPCs, Antiviren-Software, HTML5-Browsern, mobilen Endgeräten**

# System- und Sicherheitsinfrastruktur
# Betriebssystem, Datenbank, ohne Windows-Admin-Rechte



- **Gesicherte Client-Server-Architektur**
- **Aktuelle Betriebssysteme** bzw. Patches verwenden (AQASYS aktuell halten)*
- **Durchgängig verschlüsselte u. authentifizierte Kommunikation** zwischen Clients, Server, Sicherheitsserver MIP, HMI, etc. (SSL/TLS Verschlüsselung/Authentifizierung mit Zertifikaten)


- AQASYS arbeitet mit einer **SQL Datenbank**
- **Sichere, performante Datenbankzugriffe** (Sicherheitsrichtlinien einhalten, Patches, etc.)
- **Automatische Backup-Unterstützung aus AQASYS**

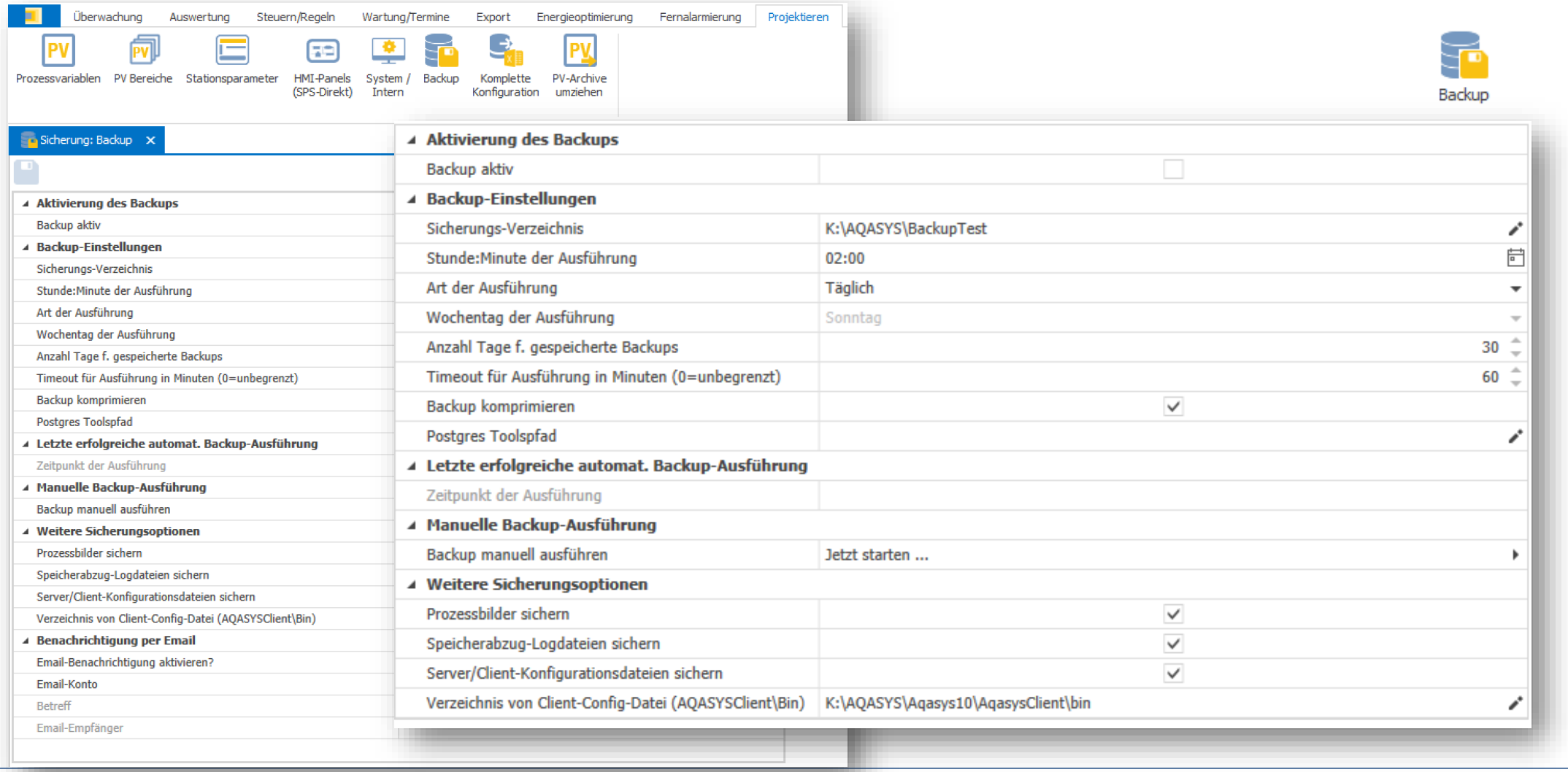


AQASYS Leitsystem auch

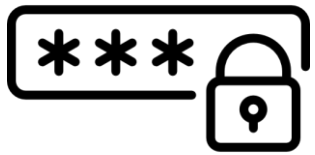
- ohne aktive Windows-Anmeldung eines Nutzers **als Dienst lauffähig**
- Benötigt zur Ausführung im Betrieb **keine administrativen Rechte**
- **Windows-Nutzer mit Standardrechten** kann sicher in AQASYS konfigurieren und bedienen

* AQASYS Versionskompatibilitäten sind im registrierten Kundenbereich abrufbar

# Automatische Backups in AQASYS 10



# AQASYS Loginverfahren
# Unauthorisierte Logins werden über wirksam Schutzkonzepte vermieden



AQASYS Benutzer + PW

Domäne
(Active Directory)

RFID Chip

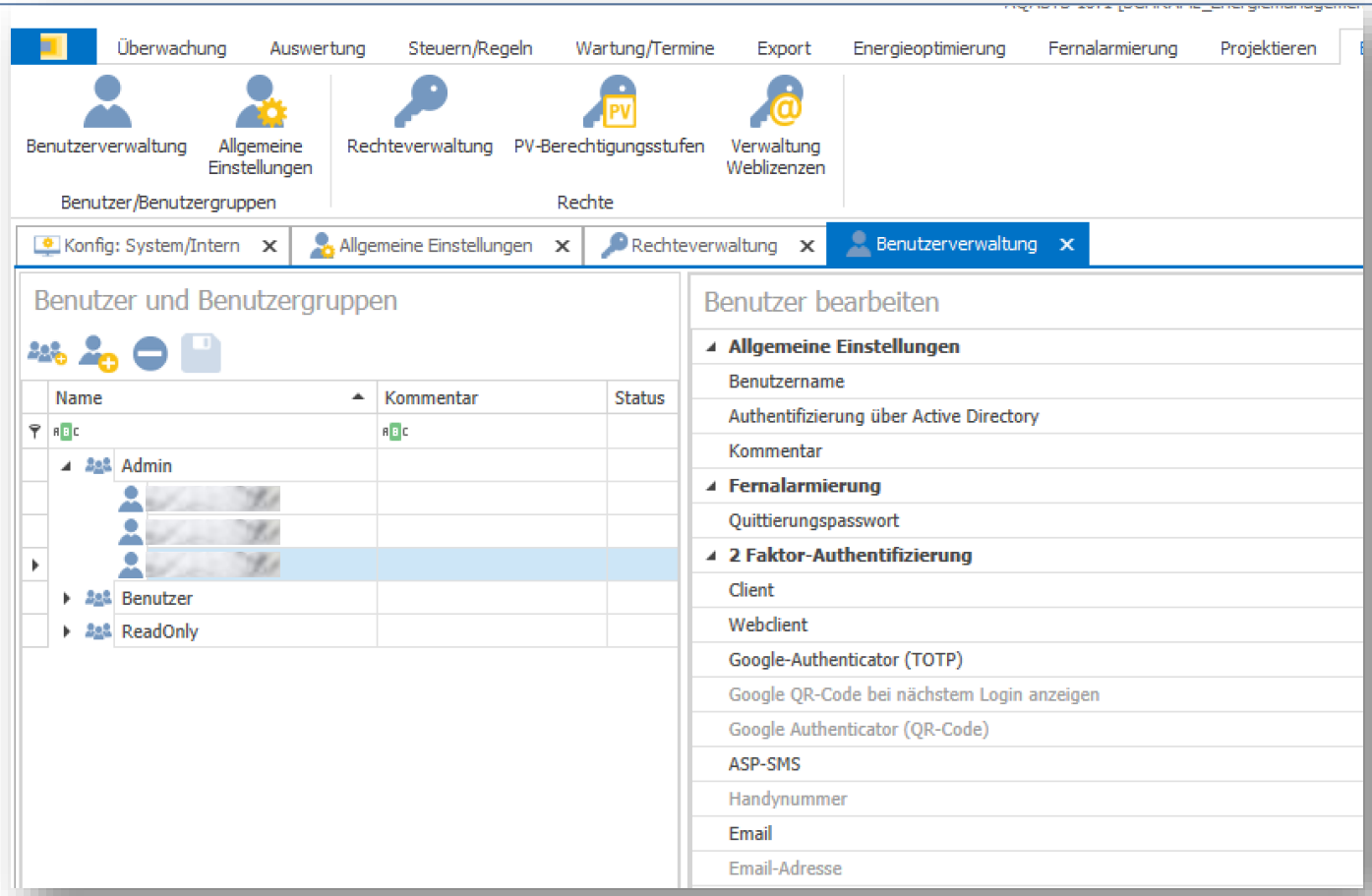
- **SHA-512 Algorithmus** zur Login-Verschlüsselung – durch Hashing kein Zurücklesen/Kopieren möglich
- **Mindestpasswortlänge und Zeichenzusammensetzung** zu definieren
- **Passwort-Erneuerungszyklus** festlegbar
- **Schutz vor Brute-Force-Login-Attacken und Denial-of-Service-Attacken (bei Webserver)** durch temporäre Login-Sperre bei zu vielen Fehlversuchen
- Anmeldungen und Anmeldeversuche durchgängig aufgezeichnet
- Keine Backdoors

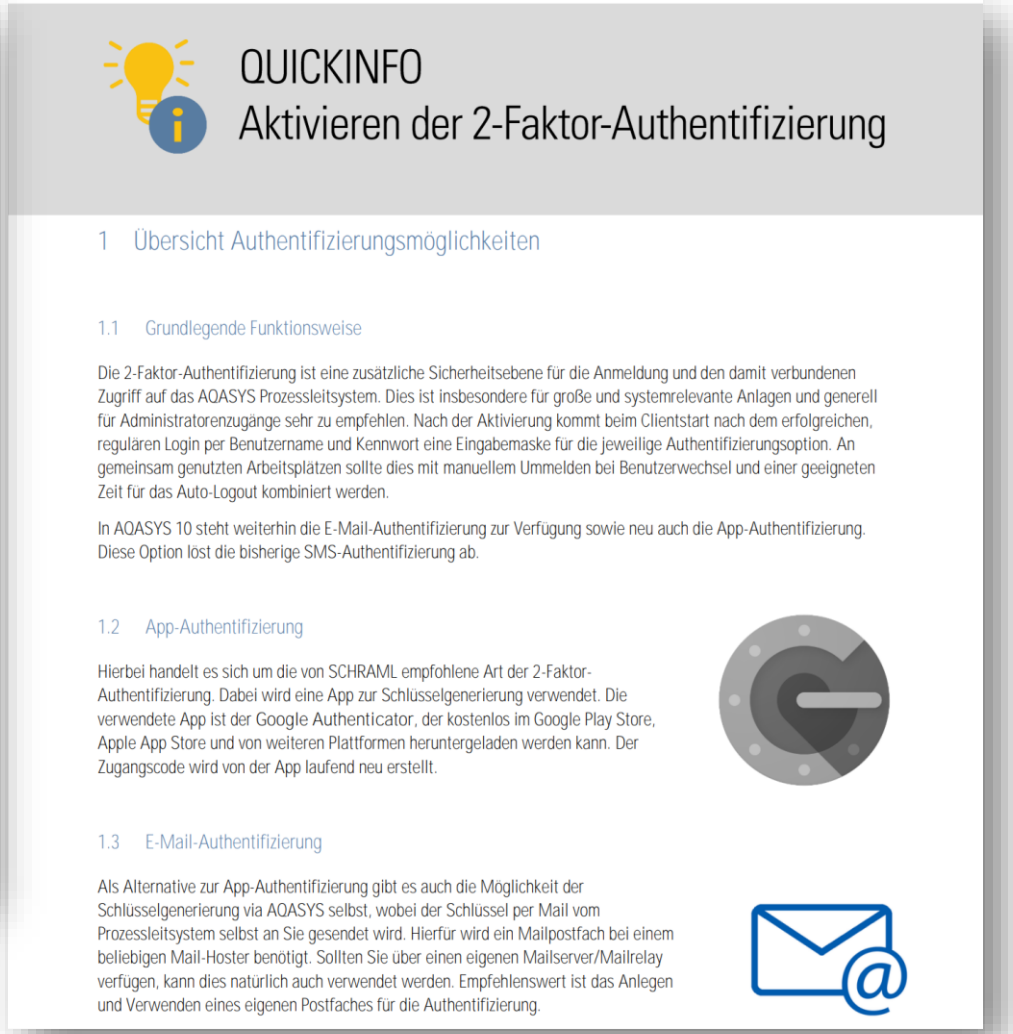
Option: 2-Faktor-Authentifizierung

weiteres, erzeugtes Einmal-Passwort via
TTOP Verfahren – Time-based One-time Password-Algorithmus

Authenticator (Google, Microsoft), Email, ASP-SMS

# 2-Faktor-Authentifizierung mit TOTP, Email, ASP-SMS



QUICKINFO
Aktivieren der 2-Faktor-Authentifizierung

1 Übersicht Authentifizierungsmöglichkeiten

1.1 Grundlegende Funktionsweise

Die 2-Faktor-Authentifizierung ist eine zusätzliche Sicherheitsebene für die Anmeldung und den damit verbundenen Zugriff auf das AQASYS Prozessleitsystem. Dies ist insbesondere für große und systemrelevante Anlagen und generell für Administratorenzugänge sehr zu empfehlen. Nach der Aktivierung kommt beim Clientstart nach dem erfolgreichen, regulären Login per Benutzername und Kennwort eine Eingabemaske für die jeweilige Authentifizierungsoption. An gemeinsam genutzten Arbeitsplätzen sollte dies mit manuellem Ummelden bei Benutzerwechsel und einer geeigneten Zeit für das Auto-Logout kombiniert werden.

In AQASYS 10 steht weiterhin die E-Mail-Authentifizierung zur Verfügung sowie neu auch die App-Authentifizierung. Diese Option löst die bisherige SMS-Authentifizierung ab.

1.2 App-Authentifizierung

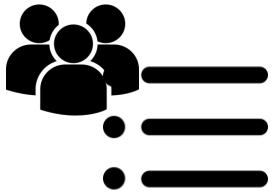
Hierbei handelt es sich um die von SCHRAML empfohlene Art der 2-Faktor-Authentifizierung. Dabei wird eine App zur Schlüsselgenerierung verwendet. Die verwendete App ist der Google Authenticator, der kostenlos im Google Play Store, Apple App Store und von weiteren Plattformen heruntergeladen werden kann. Der Zugangscode wird von der App laufend neu erstellt.

1.3 E-Mail-Authentifizierung

Als Alternative zur App-Authentifizierung gibt es auch die Möglichkeit der Schlüsselgenerierung via AQASYS selbst, wobei der Schlüssel per Mail vom Prozessleitsystem selbst an Sie gesendet wird. Hierfür wird ein Mailpostfach bei einem beliebigen Mail-Hoster benötigt. Sollten Sie über einen eigenen Mailserver/Mailrelay verfügen, kann dies natürlich auch verwendet werden. Empfehlenswert ist das Anlegen und Verwenden eines eigenen Postfaches für die Authentifizierung.

# Benutzer- und Rechtemanagement

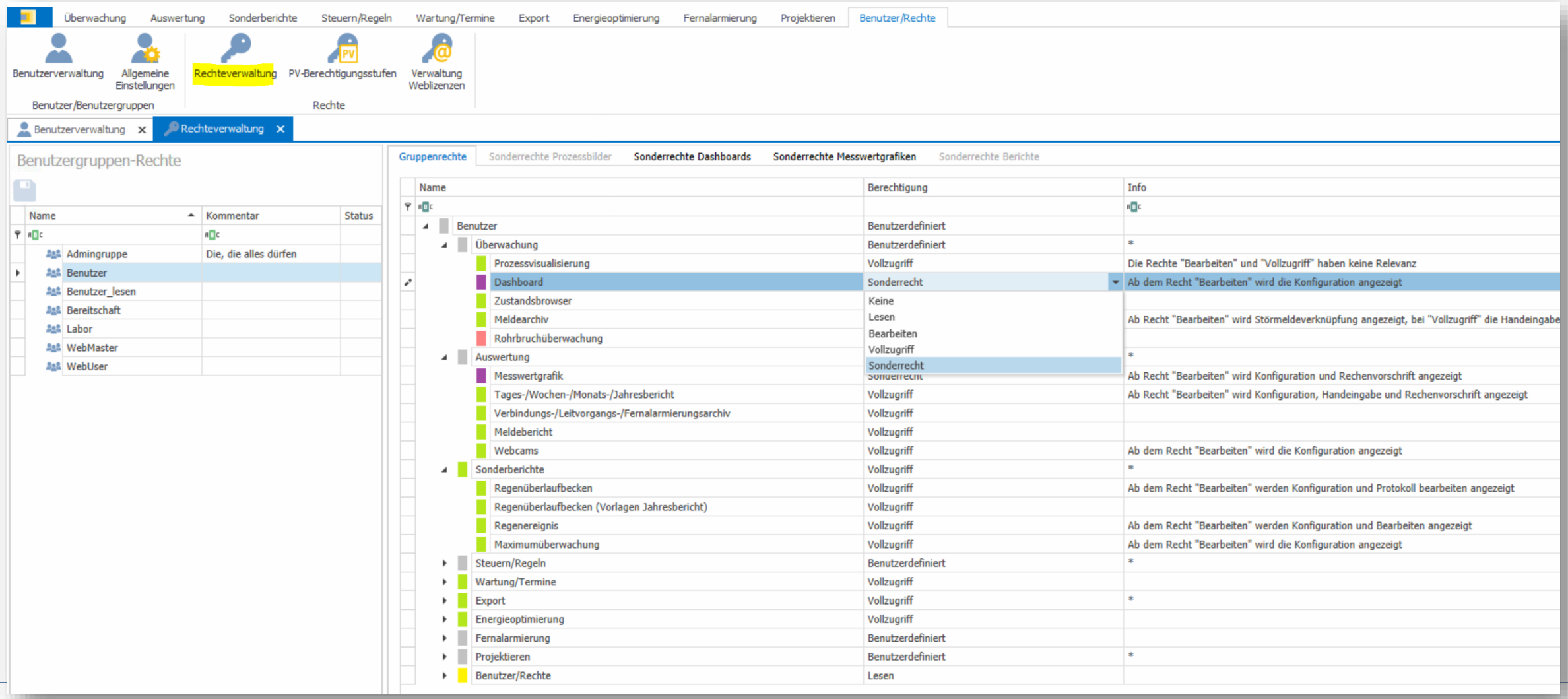
- AQASYS hat ein umfassendes Rechte- und Rollenkonzept mit Benutzern und Benutzergruppen (Menü-Rechte, Sonderrechte, usw.)
- Optional: Mandantenmanagement für z.B. Verbundsysteme



- Alle Vorgänge (Logins, Abmeldungen, Konfigänderungen, Schalthandlungen, etc.) werden benutzerbezogen im Leitvorgangsarchiv protokolliert – gilt für AQASYS PC, Web & App,
- ab AQ 10 auch die Aktionen am AQ HMI

- Sicher: hartcodierte aktive Zugänge für Servicezwecke sind z.B. nicht erlaubt

# Rechteverwaltung auf Basis der Benutzergruppen: Vollzugriff, Bearbeiten, Lesen, Keine, Sonderrecht



# Agenda

Motivation
Gesetzgebung
Richtlinien

BSI, KRITIS
DWA/DVGW

SCHRAML
Organisation

Security
„by design“

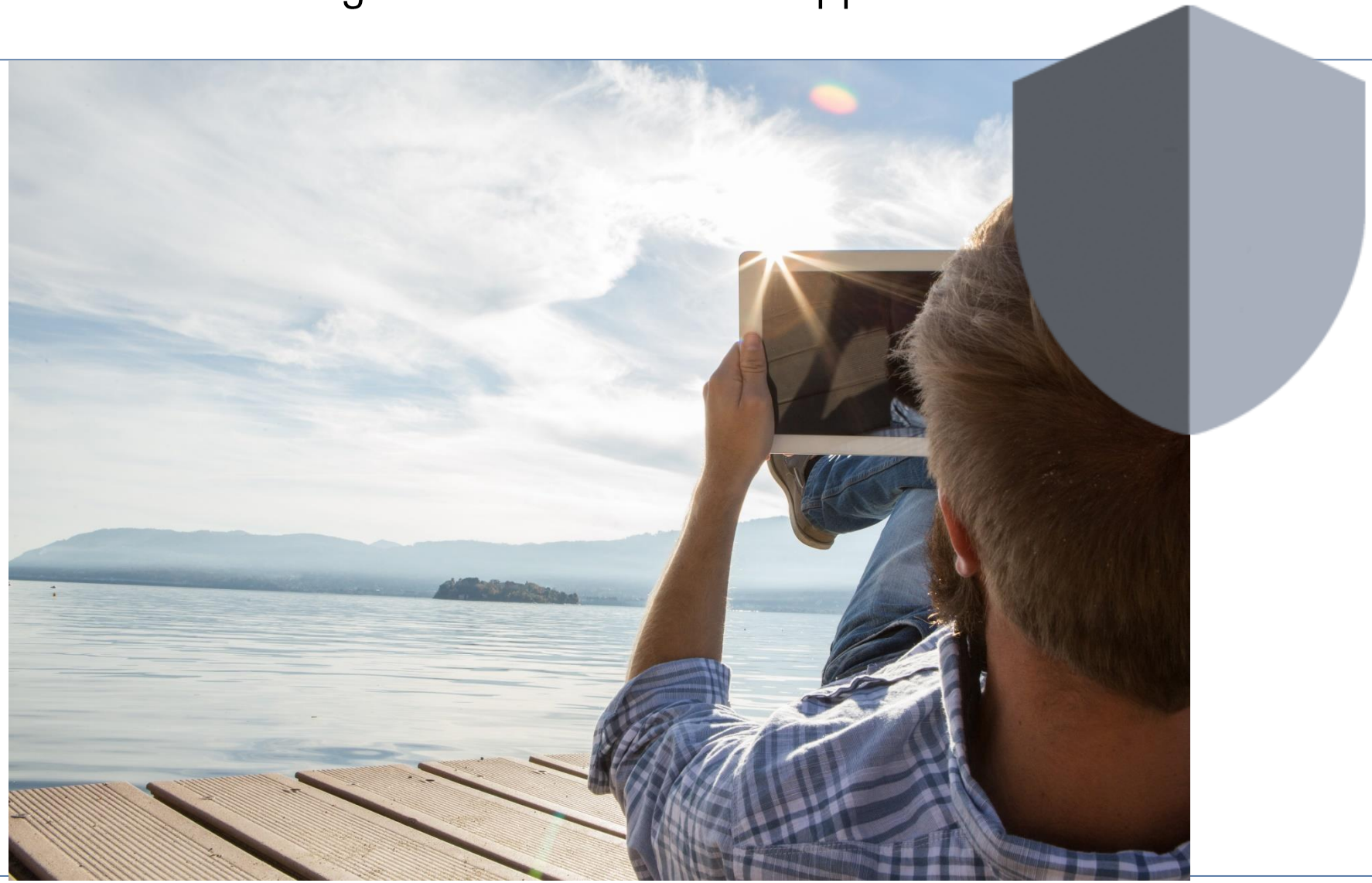
AQASYS
System

AQASYS
Web / App

Ausfall- &
Betriebs-
sicherheit

SCHRAML
Fernwirktechnik

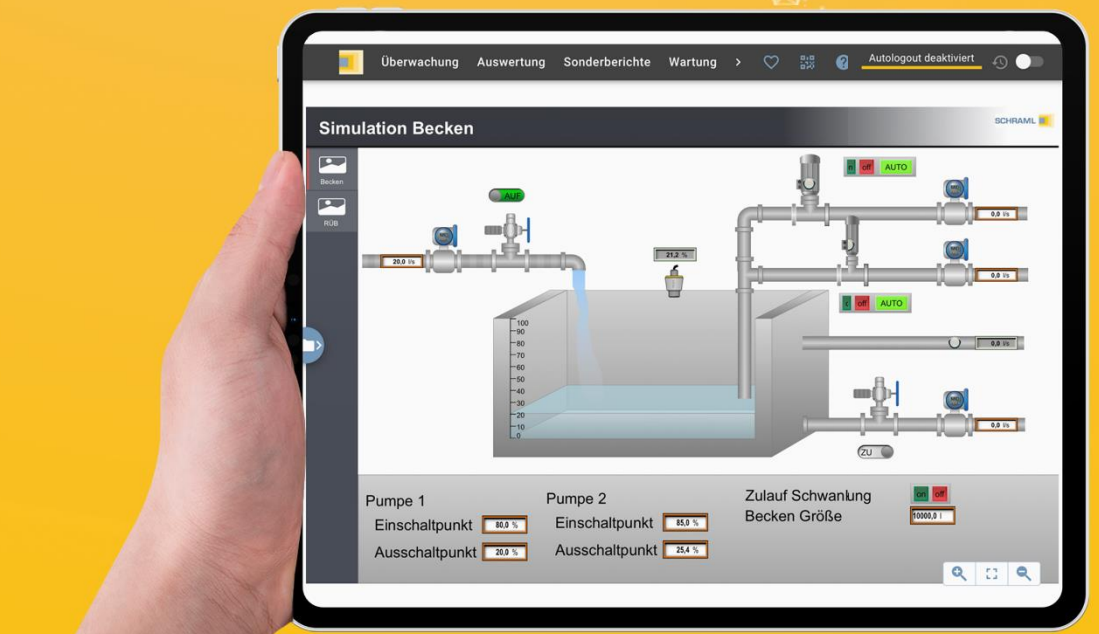
# Sichere Nutzung von Webclient und App



SCHRAML

# WASSER INTELLIGENT MANAGEN.

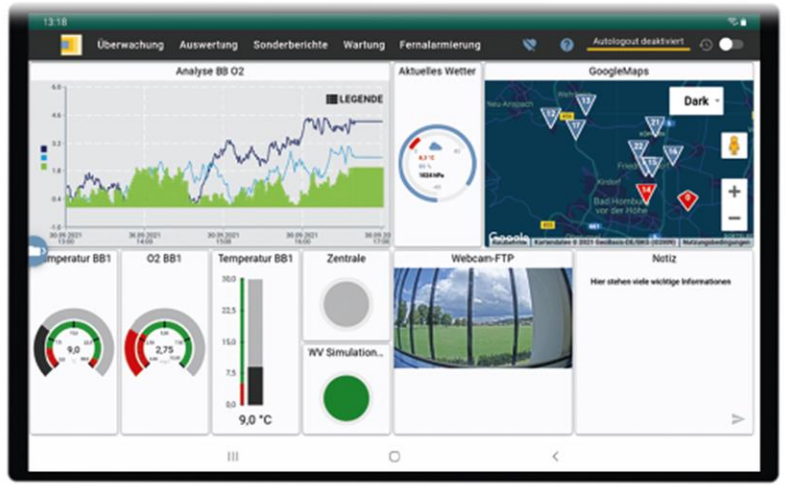
## PROZESSLEITEN FERNWIRKEN AUTOMATISIEREN





iOS

# Alles in der AQASYS App:
# Visualisierung | Dashboard | Ganglinien | Berichte | Wartung | Alarmierung






JETZT BEI Google Play

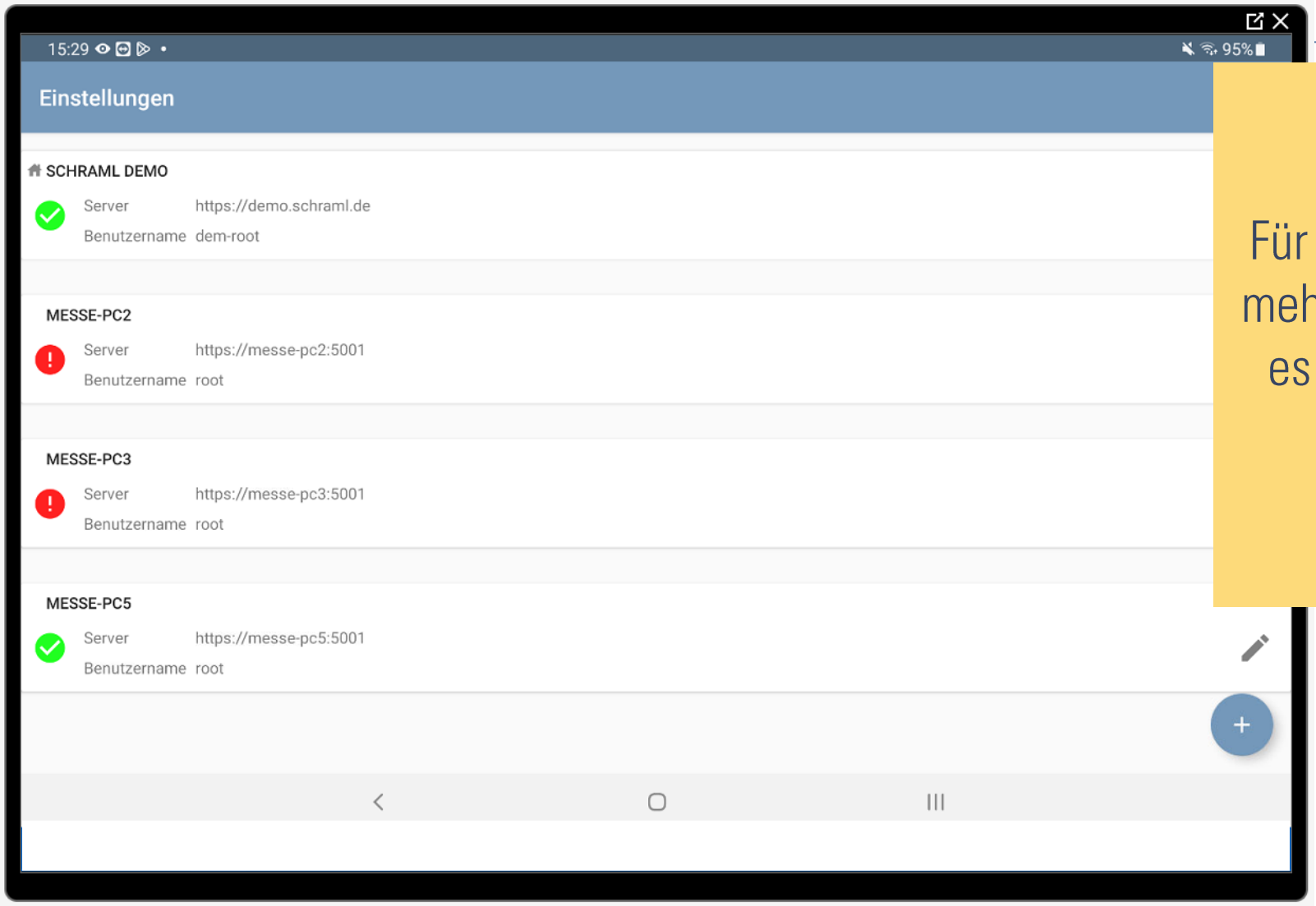
Laden im App Store

**Intuitive und optimierte Bedienung** für mobile Endgeräte (Responsive Design) inklusive Favoritenliste, kürzlich besuchte Seiten, gleiche Menüstruktur und Icons wie Webclient und Desktop

**Sichere und einfache Anmeldung** über AQASYS Benutzerkonten für den schnellen Zugriff auf Ihre Anlagenüberwachung und -steuerung (optional mit reCAPTCHA oder 2-Faktor-Authentifizierung)

Verwaltung **mehrerer Anlagen in einer App** inklusive einfachem Zugriffswechsel zwischen den Anlagen, z.B. auf Kanalnetz und Kläranlage oder von Verbundanlagen

# Verwaltung von mehreren Anlagen (Projekten) in der App




Für Integratoren oder Betreiber mehrerer AQASYS Projekte gibt es eine Verwaltung mehrerer Anlagen in der App!

# AQASYS **Webclient** – greifen Sie sicher mobil auf ihre Anlage zu

## Sicherheitsaspekte bei Verwendung des Webclients





Keine permanent geöffneten Fernzugriffe ohne Dokumentations-/Überwachungsfunktion (siehe Remote Applikationen wie z.B. TeamViewer, Anydesk, etc.)

Idealerweise durchgängige, gehärtete Lösung aus einer Hand (möglichst keine Drittsoftware „dazwischen“, Methoden zur Vermeidung von Schadsoftware wie XSS, SQL Injection, Brute Force Login und DDoS Atacken)

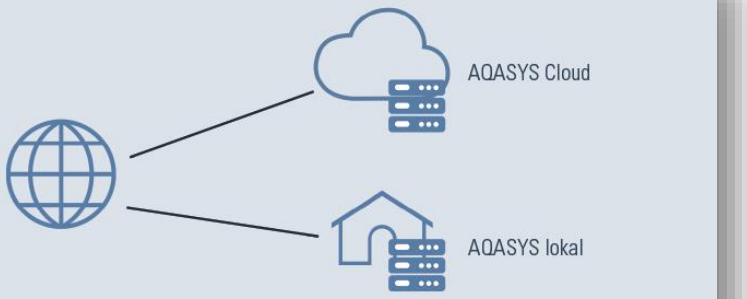
Keine sicherheitskritischen Plugins wie z.B. Java, Flash → HTML5 / pure Webtechnologie

Einsatz spezieller Passwortstärken, Web-Rechte, reCAPTCHA möglich,
(Optional: 2-Faktor-Authentifizierung)

Verschlüsselte und authentifizierte https-Verbindung (TLS/SSL)

Nutzung VPN-Verbindung möglich, VPN-Clients für Smartphones etc. verfügbar

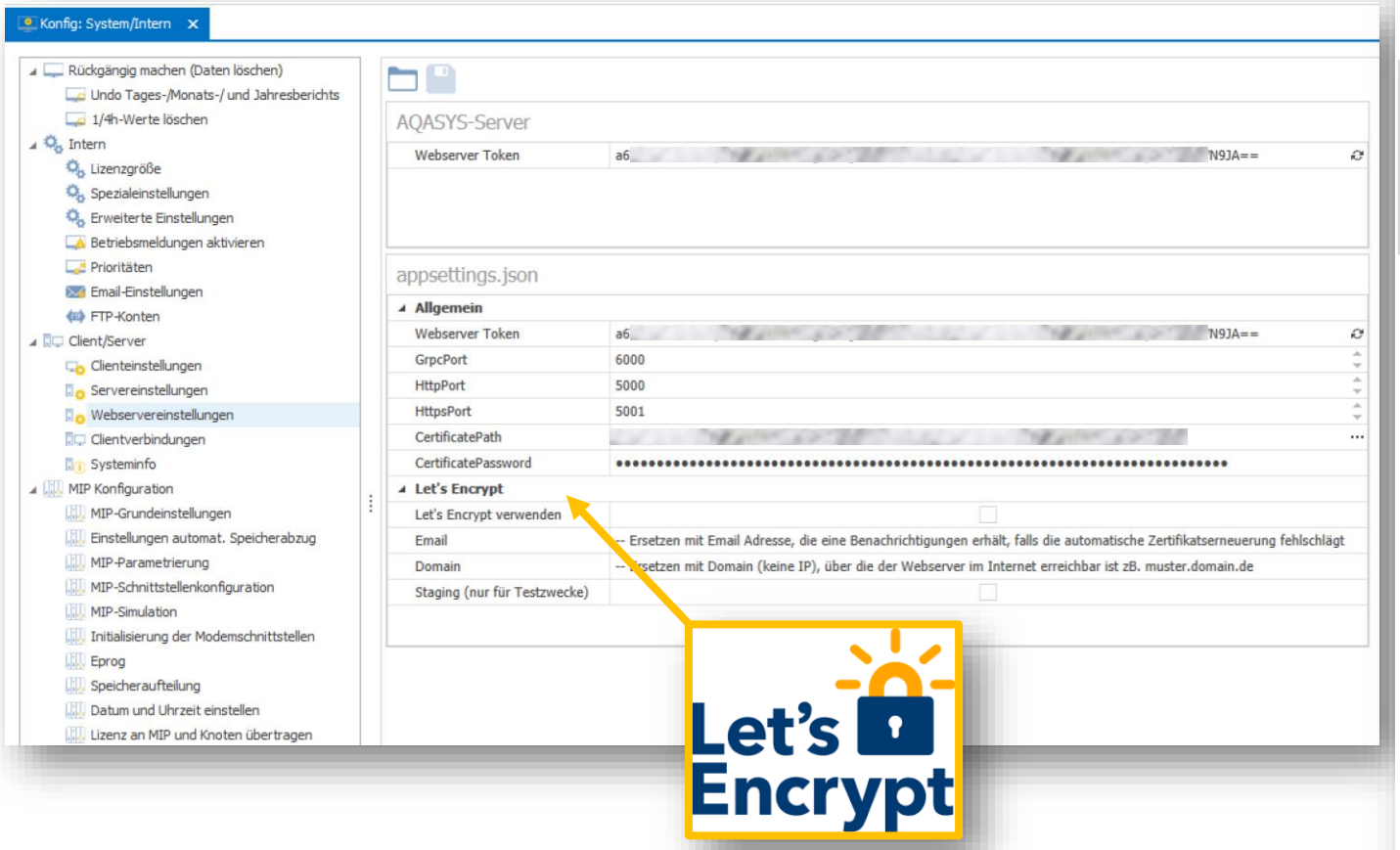
# AQASYS App - Flexibler und sicherer Zugriff auf Ihre Anlage

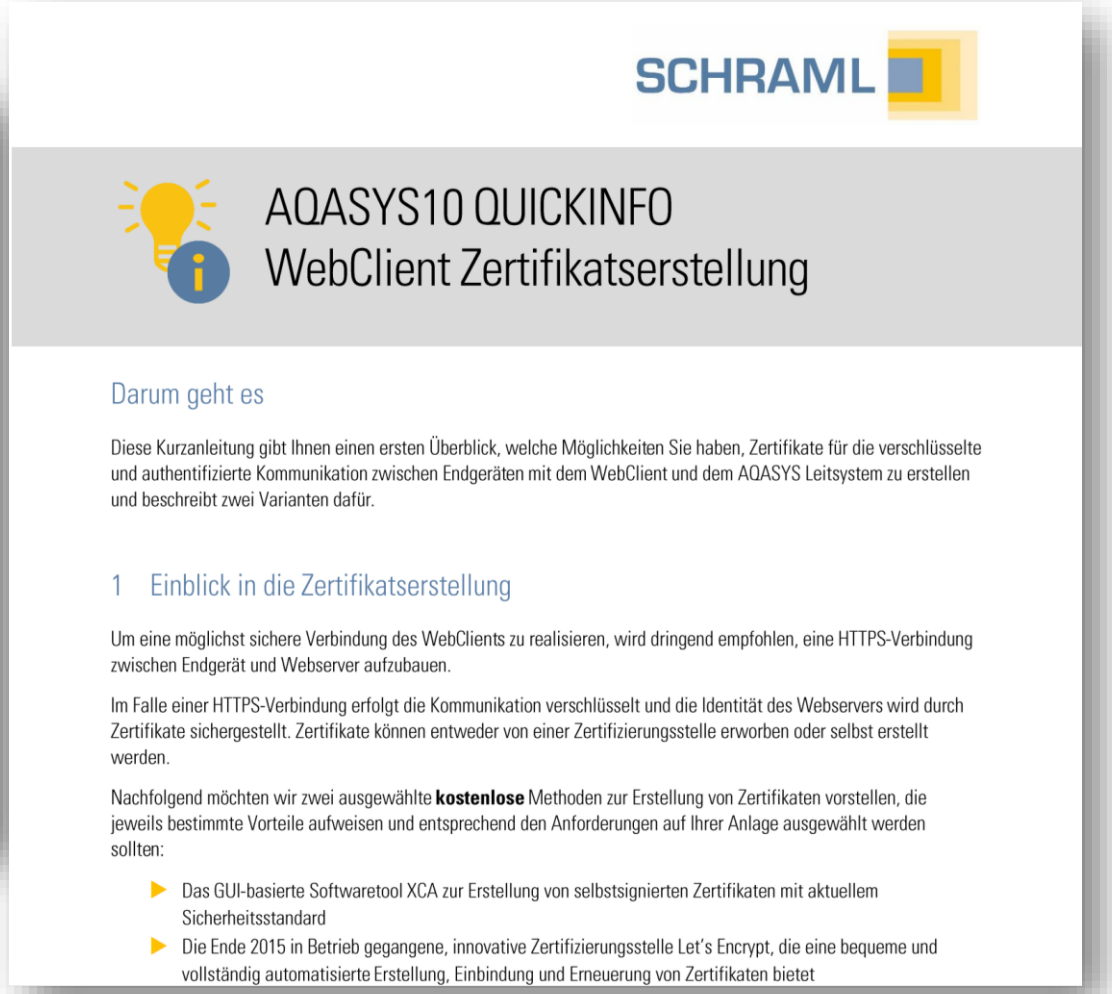




## Volle Sicherheit in der App-Anwendung

- SSL/TLS Verschlüsselung und authentifizierte Zertifkate
- Login mit reCAPTCHA und 2-Faktor-Authentifizierung (optional)
- automatische Synchronisation der Benutzer- und Rechteverwaltung über PC, App, Webclient (und HMI) hinweg
- vollständige Dokumentation der Benutzeraktionen in der App im Leitvorgangsarchiv
- VPN-Verbindungen möglich
- Einsetzbar in demilitarisierter Zone
- Admins managen und überwachen aktive Online-Verbindungen

# AQASYS kann mit allen Zertifikaten umgehen | Let's encrypt vs. erworbener vs. selbsterstellter Zertifikate



SCHRAML

AQASYS10 QUICKINFO
WebClient Zertifikatserstellung

## Darum geht es

Diese Kurzanleitung gibt Ihnen einen ersten Überblick, welche Möglichkeiten Sie haben, Zertifikate für die verschlüsselte und authentifizierte Kommunikation zwischen Endgeräten mit dem WebClient und dem AQASYS Leitsystem zu erstellen und beschreibt zwei Varianten dafür.

## 1 Einblick in die Zertifikatserstellung

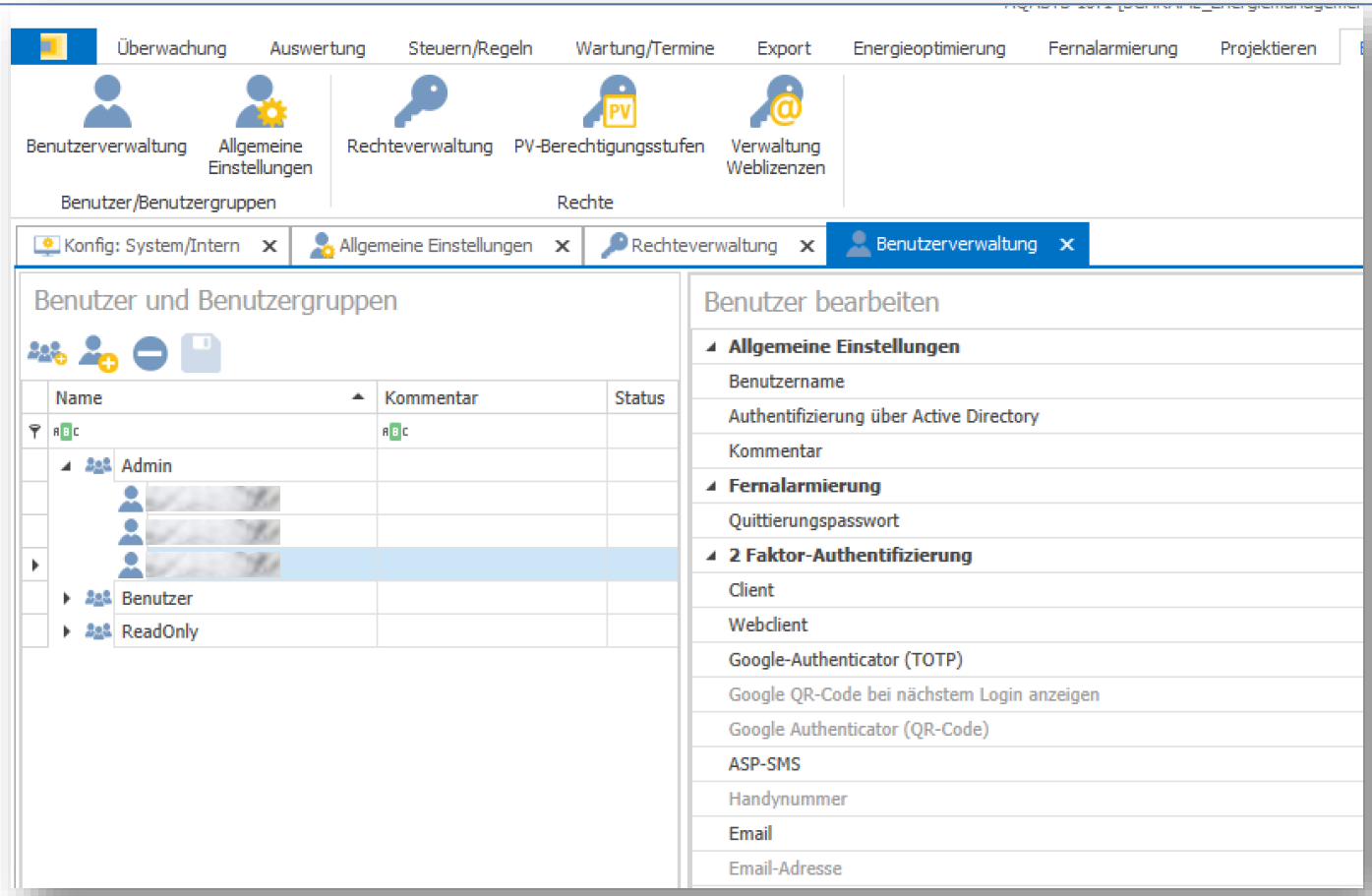
Um eine möglichst sichere Verbindung des WebClients zu realisieren, wird dringend empfohlen, eine HTTPS-Verbindung zwischen Endgerät und Webserver aufzubauen.

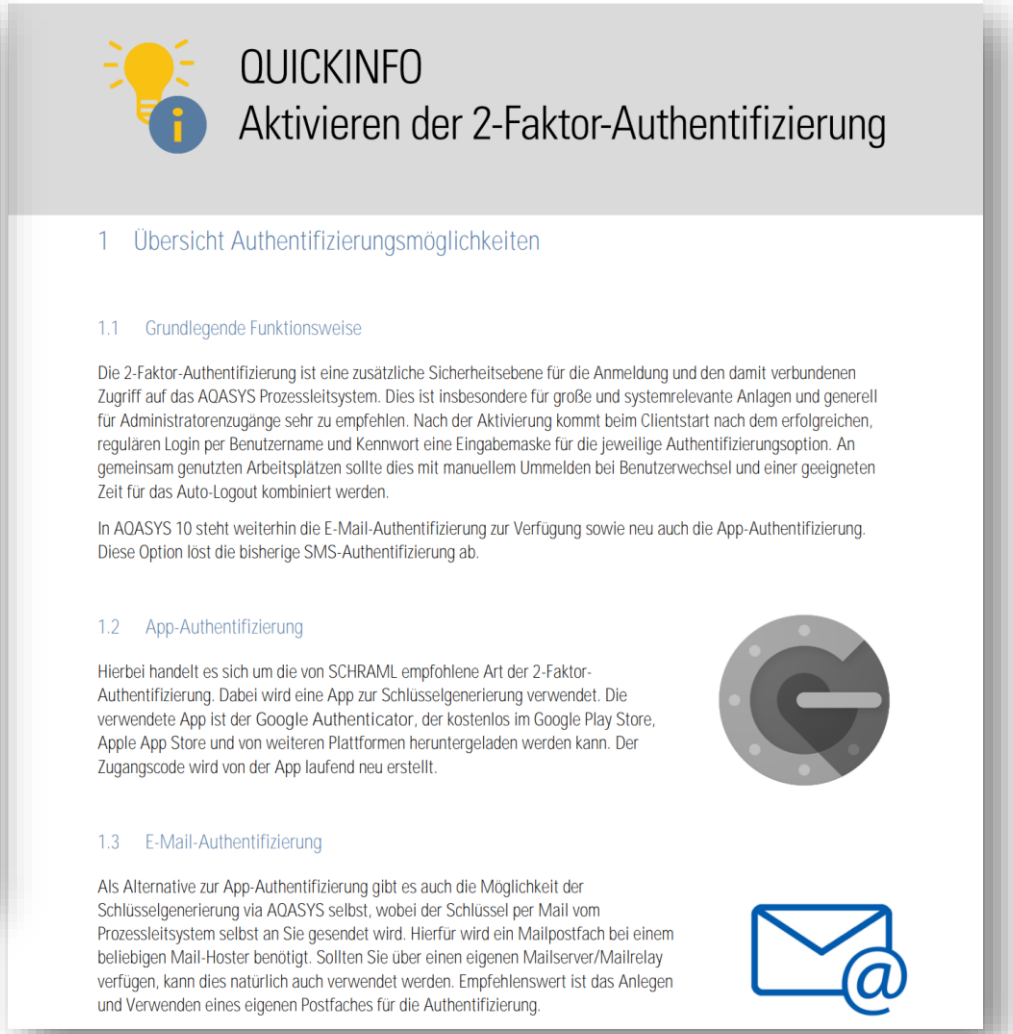
Im Falle einer HTTPS-Verbindung erfolgt die Kommunikation verschlüsselt und die Identität des Webservers wird durch Zertifikate sichergestellt. Zertifikate können entweder von einer Zertifizierungsstelle erworben oder selbst erstellt werden.

Nachfolgend möchten wir zwei ausgewählte **kostenlose** Methoden zur Erstellung von Zertifikaten vorstellen, die jeweils bestimmte Vorteile aufweisen und entsprechend den Anforderungen auf Ihrer Anlage ausgewählt werden sollten:

- Das GUI-basierte Softwaretool XCA zur Erstellung von selbstsignierten Zertifikaten mit aktuellem Sicherheitsstandard
- Die Ende 2015 in Betrieb gegangene, innovative Zertifizierungsstelle Let's Encrypt, die eine bequeme und vollständig automatisierte Erstellung, Einbindung und Erneuerung von Zertifikaten bietet

# 2-Faktor-Authentifizierung mit TOTP, Email, ASP-SMS



QUICKINFO
Aktivieren der 2-Faktor-Authentifizierung

1 Übersicht Authentifizierungsmöglichkeiten

1.1 Grundlegende Funktionsweise

Die 2-Faktor-Authentifizierung ist eine zusätzliche Sicherheitsebene für die Anmeldung und den damit verbundenen Zugriff auf das AQASYS Prozessleitsystem. Dies ist insbesondere für große und systemrelevante Anlagen und generell für Administratorenzugänge sehr zu empfehlen. Nach der Aktivierung kommt beim Clientstart nach dem erfolgreichen, regulären Login per Benutzername und Kennwort eine Eingabemaske für die jeweilige Authentifizierungsoption. An gemeinsam genutzten Arbeitsplätzen sollte dies mit manuellem Ummelden bei Benutzerwechsel und einer geeigneten Zeit für das Auto-Logout kombiniert werden.

In AQASYS 10 steht weiterhin die E-Mail-Authentifizierung zur Verfügung sowie neu auch die App-Authentifizierung. Diese Option löst die bisherige SMS-Authentifizierung ab.

1.2 App-Authentifizierung

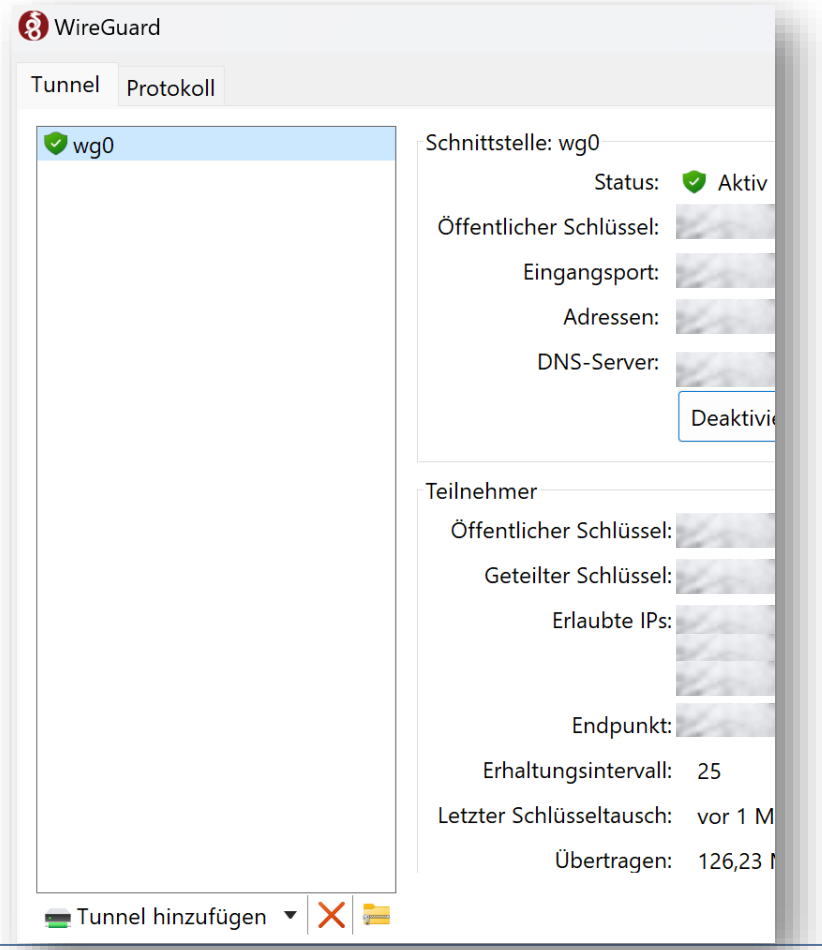
Hierbei handelt es sich um die von SCHRAML empfohlene Art der 2-Faktor-Authentifizierung. Dabei wird eine App zur Schlüsselgenerierung verwendet. Die verwendete App ist der Google Authenticator, der kostenlos im Google Play Store, Apple App Store und von weiteren Plattformen heruntergeladen werden kann. Der Zugangscode wird von der App laufend neu erstellt.

1.3 E-Mail-Authentifizierung

Als Alternative zur App-Authentifizierung gibt es auch die Möglichkeit der Schlüsselgenerierung via AQASYS selbst, wobei der Schlüssel per Mail vom Prozessleitsystem selbst an Sie gesendet wird. Hierfür wird ein Mailpostfach bei einem beliebigen Mail-Hoster benötigt. Sollten Sie über einen eigenen Mailserver/Mailrelay verfügen, kann dies natürlich auch verwendet werden. Empfehlenswert ist das Anlegen und Verwenden eines eigenen Postfaches für die Authentifizierung.

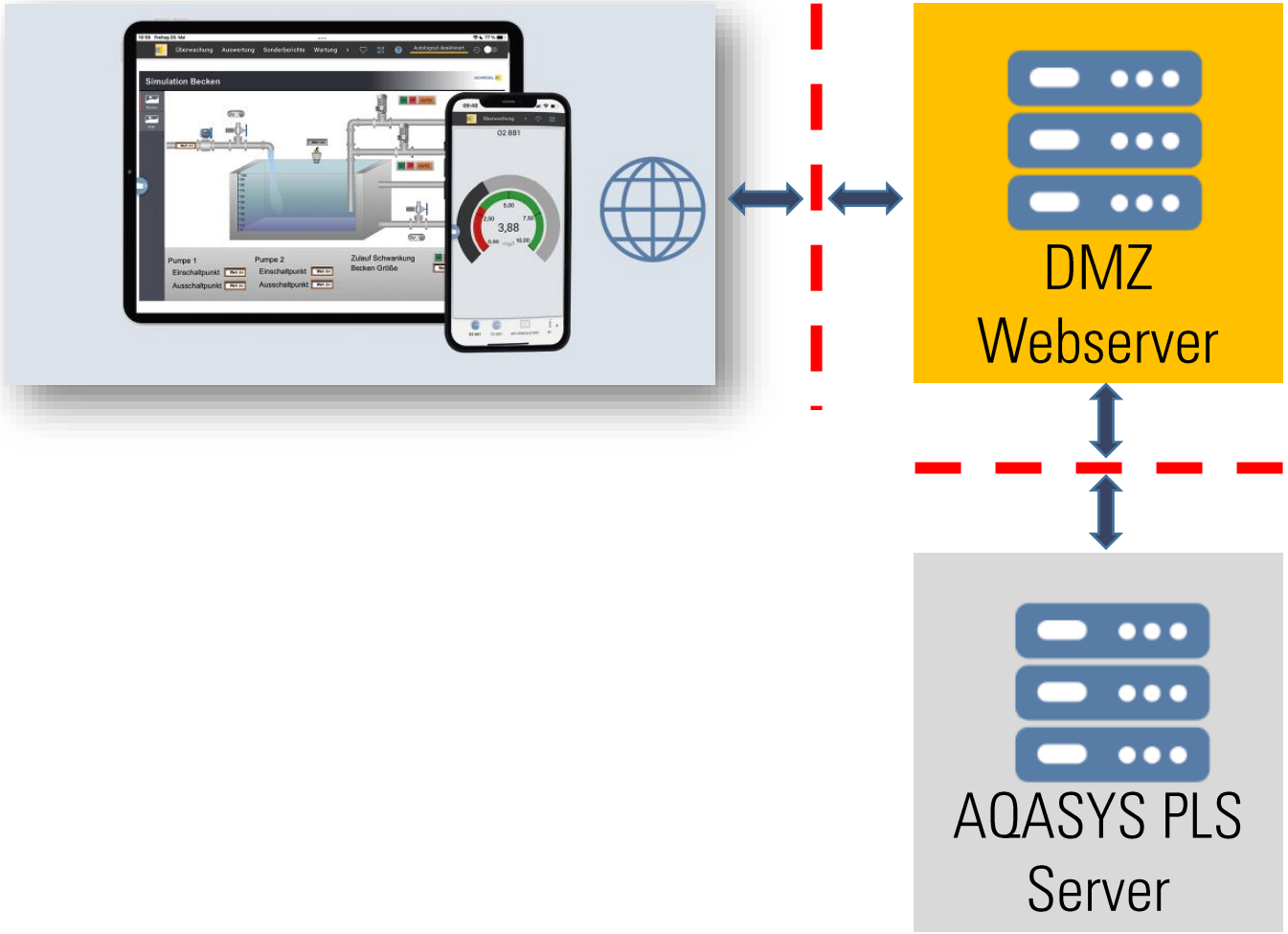
# AQASYS Webclient oder App auch mit VPN nutzbar

## Windows VPN Client

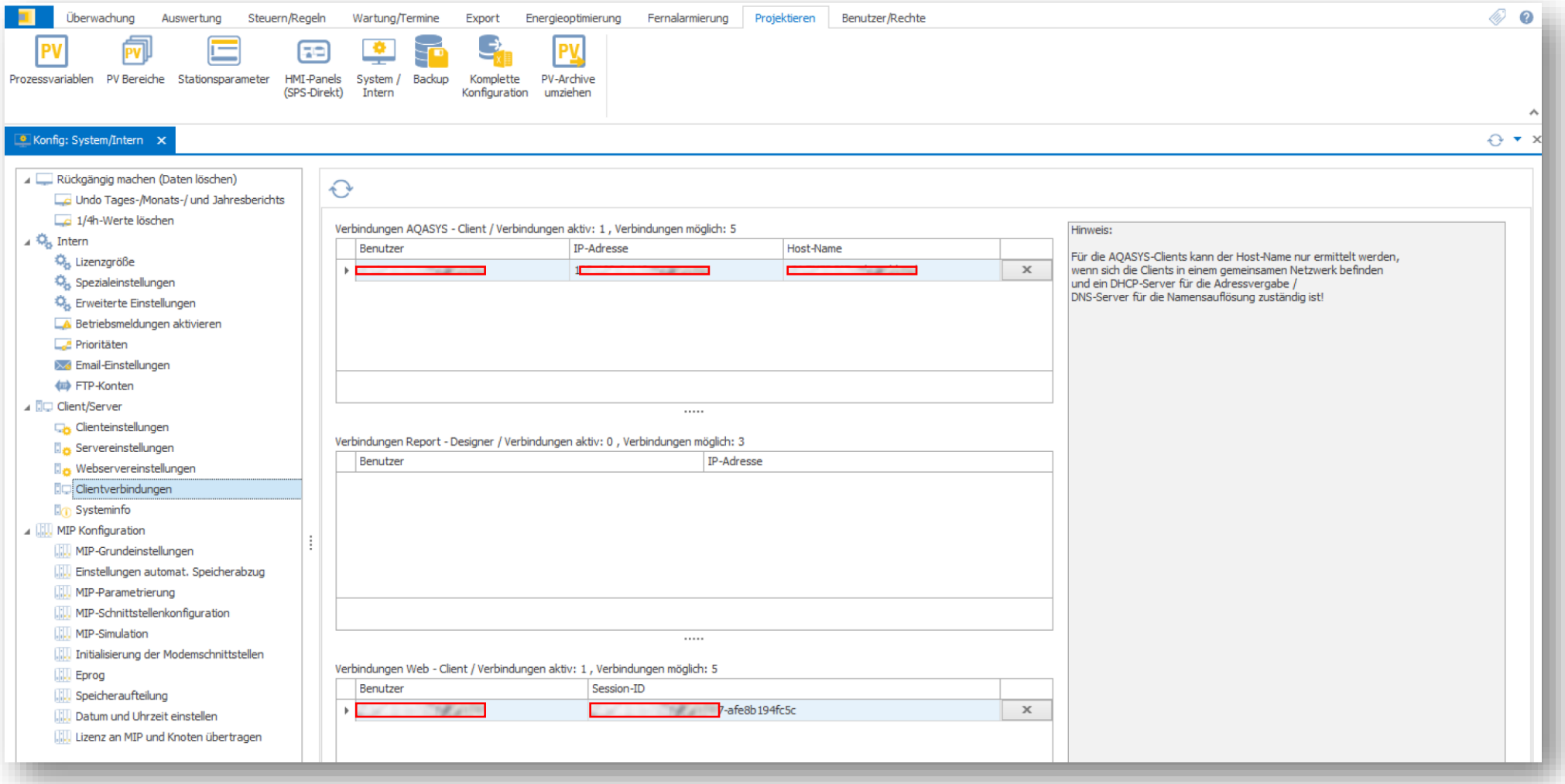



## VPN App (iOS; auch für Android)

# DMZ – Demilitarisierte Zone für gesicherte Webzugriffe




# AQASYS Admin-Monitoring eingehender Client-Verbindungen



# Agenda

Motivation
Gesetzgebung
Richtlinien

BSI, KRITIS
DWA/DVGW

SCHRAML
Organisation

Security
„by design“

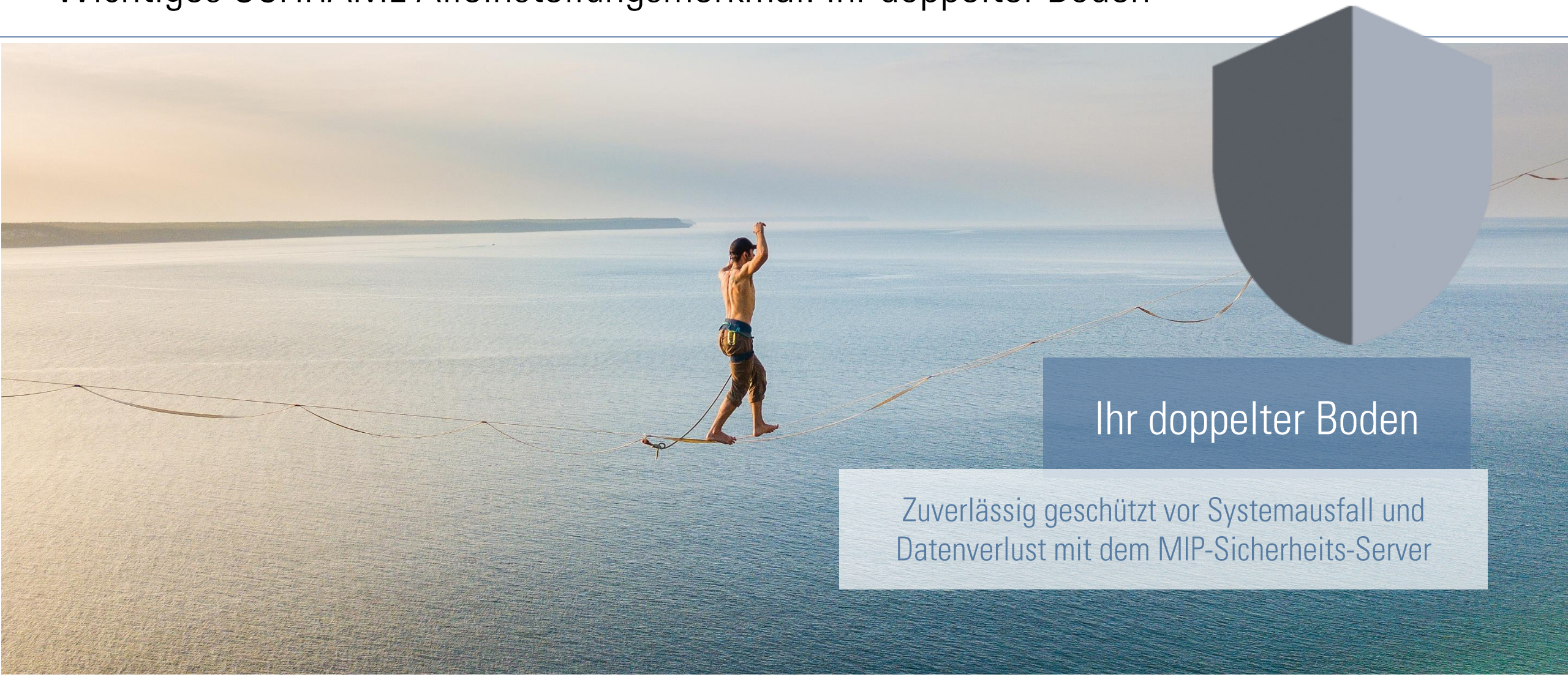
AQASYS
System

AQASYS
Web / App

Ausfall- &
Betriebs-
sicherheit

SCHRAML
Fernwirktechnik

# Wichtiges SCHRAML Alleinstellungsmerkmal: Ihr doppelter Boden



# Ausfall-Sicherheit | Hochverfügbarkeit

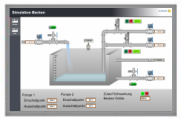
- Grundsätzlich ist Betrieb des Systems als Cold-Standby, Hot-Standby oder Failover-Cluster in virtuellen Umgebungen möglich – mit IT-Know-How und Aufwand verbunden (bei IB und im Alltag)

- MIP Sicherheits-Server ermöglicht hohe Ausfall-, Betriebs- und IT-Sicherheit

  - Räumliche und programmatische Trennung des prozesskritischen Echtzeitbetriebs und des Anwendungs- / Datenserver
  - Leitsystem-PC / Server = „schwächste Glied“ in der SCADA-Automatisierungskette – erhält durch MIP Sicherheits-Server einen hochperformanten doppelten Boden


  - Hoch robust, gehärtetes Linux Betriebssystem, keine bewegten Teile, sehr energiesparsam

Sicherstellung prozesskritischer Funktionen – auch wenn PLS-Rechner nicht verfügbar
**Alarmierung | (Quer-)Steuerung | Bedienung (HMI) | Datenspeicherung | IT-Sicherheit**

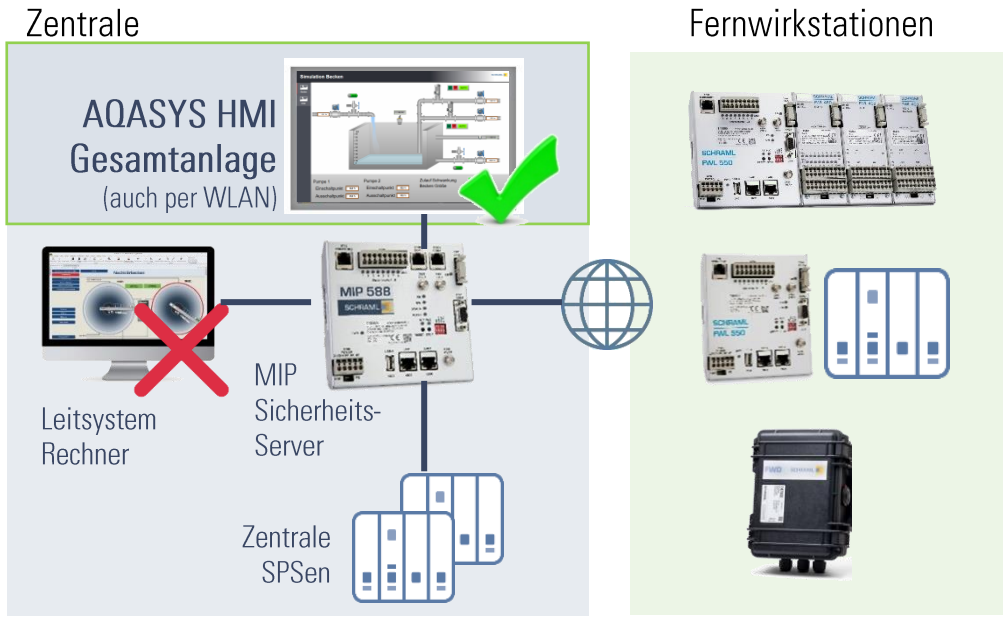




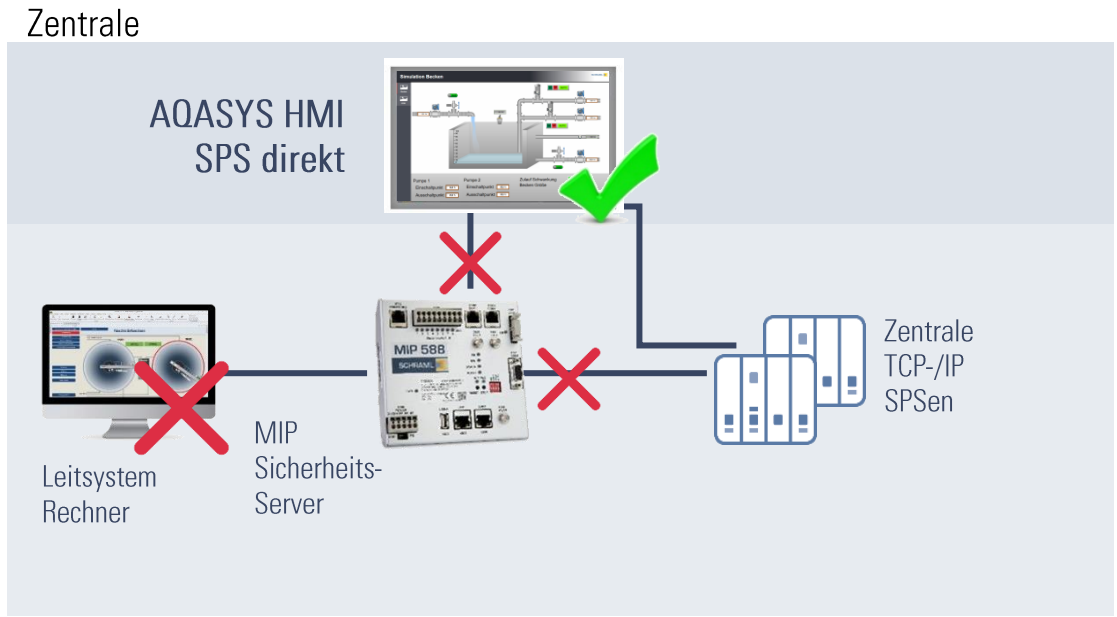
MIP-Sicherheits-Server auch als Hot-Standby Konzept verfügbar

# AQASYS HMI:
# ausfallsicher und durchgängig Überwachen und Steuern - in der Zentrale

## AQASYS HMI Gesamtanlage



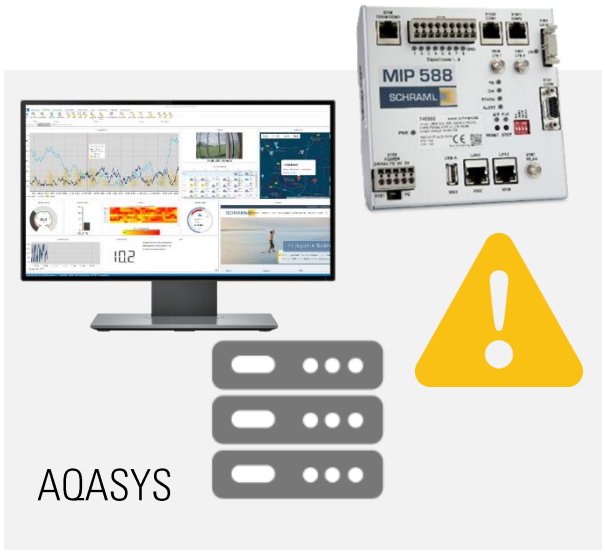

## AQASYS HMI SPS direkt




Ausfallsicheres Überwachen und Steuern (je nach Benutzerrechte)

- in der Zentrale (z.B. in der Warte),
- auf dem zentralen Anlagengelände (z.B. Schaltschrank oder mobil am WLAN-Tablet)
- auch als Ersatz eines Störmeldedruckers (mit Zusatzfunktionen) geeignet

# AQASYS Fernalarmierung – geht auf Nummer sicher




bis zu **4 Alarmierungslinien = Wege**
→ Redundanz, Ausfallsicherheit, Präferenzen

bis zu **100 Rufgruppen mit bis zu**
**20 Empfänger pro Rufgruppe**

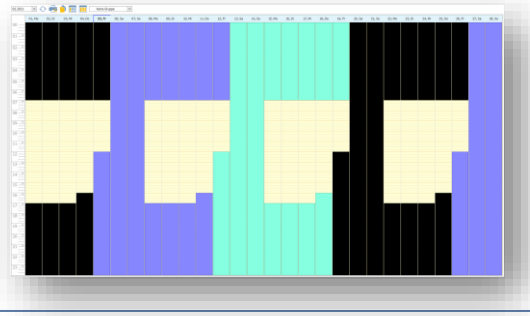
**Gruppe: Kanal**
1. Hr. Huber | 0171-12345 - SMS
2. Hr. Huber | 0171 – 12345 - Sprache
3. Fr. Muster | 0152-14563027 - Sprache
4. …..

bis zu **200 Rufnummern**
→ verschiedene Personen, Endgeräte, usw..

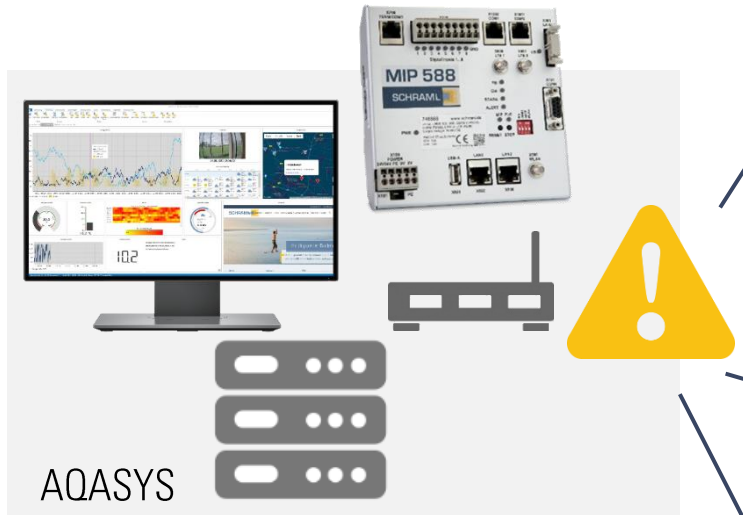
**Gruppe Trinkwasser**
1. Fr. Müller | 08062-12345 - SMS
2. Hr. Huber | ….
…

**9 Störmelde-Prioritäten**
Fokussierung, Relevanz

bis zu **100 Alarmierungspläne**
→ flexible Zuordnungen von Zeiten, Verantwortlichkeiten, Dringlichkeiten etc.



# AQASYS **Fernalarmierungswege / - Linien**
## volle Auswahl an bewährten und neuen Diensten




via (integriertes) LTE-Modem

- SMS über GSM Netz

via DSL

- E-Mail via DSL & eigene Domäne

Über ihre(n) SIP Account/ SIP Telefonanlage

- Sprachausgabe Text-to-Speech via SIP

via Web-Fernalarmierungs-dienst

- Sprachausgabe Text-to-Speech via Web
- SMS über Web
- Telegram App
- Cityruf über Web

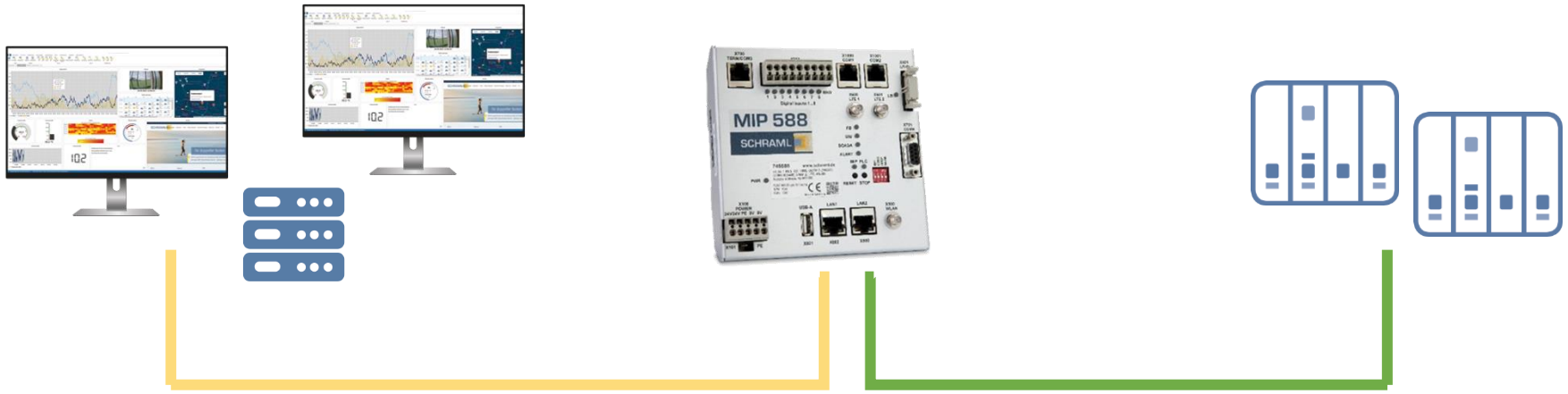
Achtung: Verfügbarkeit Festnetzdienste
- Eplus, D1, Vodafone und O2 haben Festnetz-Dienst weitgehend eingestellt
- Die Datenübertragung per Analogmodem funktioniert bei VoIP-Telefonanschlüssen nur mangelhaft

# Schutz der Automatisierungsebene
# Netzwerktrennung und -segmentierung

AQASYS
Büro- & Leitsystemebene

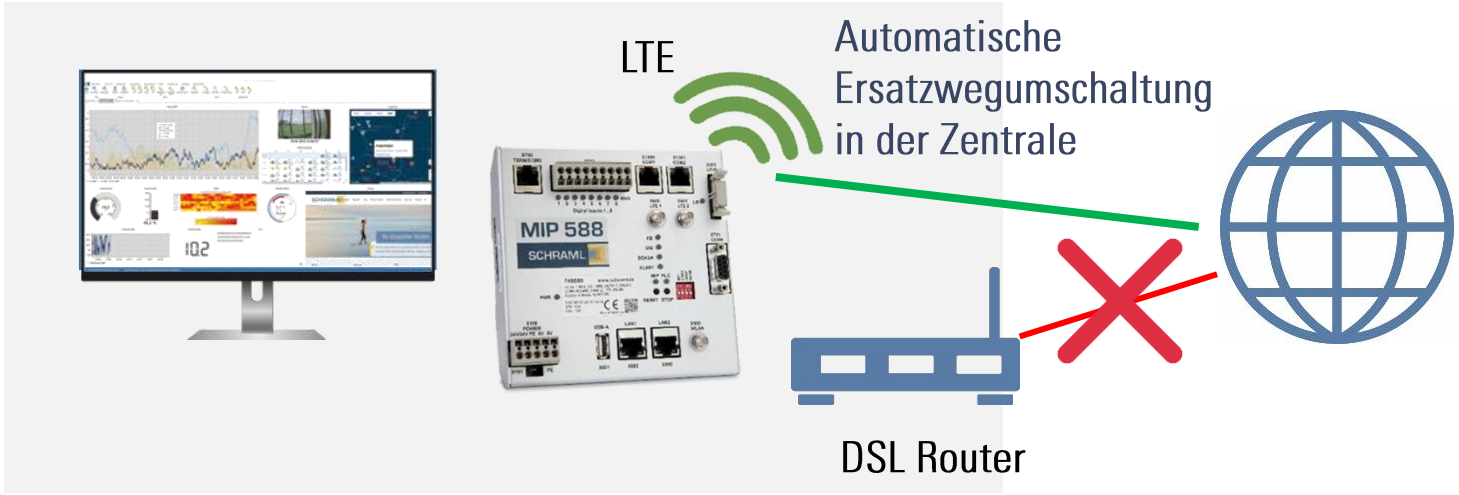
**MIP Sicherheits-Server**

Automatisierungs-ebene / SPSen




Segmentierung von PC- und Automatisierungsnetzwerk im MIP Sicherheits-Server

# Exkurs: doppelter Boden beim Fernwirken mit MIP 58x automatische **Ersatzwegschaltung** DSL <–> LTE in der Zentrale





- Verfügbarkeit des Fernwirk-Übertragungsweges in der Zentrale (DSL über DSL-Router) wird kontinuierlich geprüft
- bei Nicht-Verfügbarkeit wird automatisch auf den Ersatzweg LTE/GPRS via integriertem LTE-Modem im MIP umgeschaltet → Fernwirkstationen und Zentrale können weiterhin kommunizieren für Störmeldungen, Steuerbefehle, Datenübertragung
- Ist der Standardweg wieder verfügbar, wird automatisch wieder auf ihn zurückgeschaltet.

# Agenda

Motivation
Gesetzgebung
Richtlinien

BSI, KRITIS
DWA/DVGW

SCHRAML
Organisation

Security
„by design“

AQASYS
System

AQASYS
Web / App

Ausfall- &
Betriebs-
sicherheit

SCHRAML
Fernwirktechnik

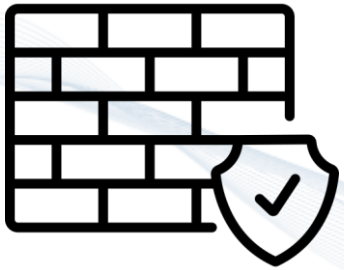
# Sichere Fernwirktechnik
# Vielfältige Übertragungswege für „den Weg ins Leitsystem“

# Sichere Fernwirktechnik
# keine eingehenden Verbindungen am zentralen Netzwerk

# Sichere Mobilfunk und Internet Datenübertragung (4G, 2G, DSL)

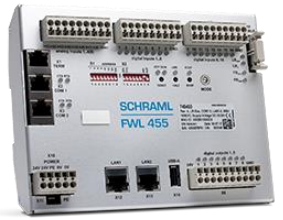
**Security by Design**
**simpel und revolutionär**

SCHRAML Architektur ermöglicht Fernwirktechnik via Internet (DSL, Mobilfunk)
bei gleichzeitigem Verbot eingehender Verbindungen in der Zentrale



Keine feste
IP-Adresse notwendig

Hochwirksame Portfreigaben:
**keine eingehende**
Verbindungen

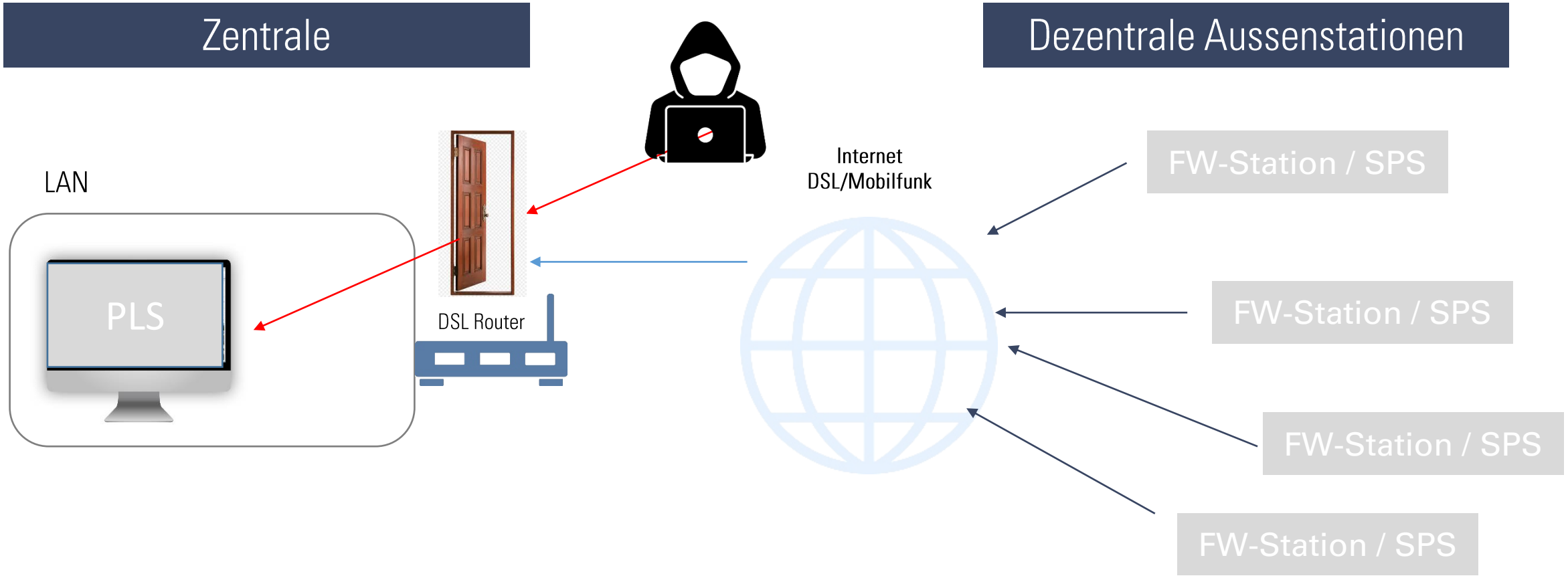




gehärtetes Linux,
geräteindividuelle
Passworte
(keine Speicherung
bei SCHRAML,
keine Backdoors)


Keine VPN-Verbindungen notwendig
Keine speziellen M2M-Verträge notwendig

# andere Fernwirk-Lösungen auf dem Markt benötigen eingehende Verbindungen (offene Ports) = „geöffnete Türen“ in der Zentrale



# „Ihr geschlossenes Tor ist der wirksamste Schutz vor Angriffen – wer von Ihnen kann/will schon ein offenes Tor im Internet überwachen?!"

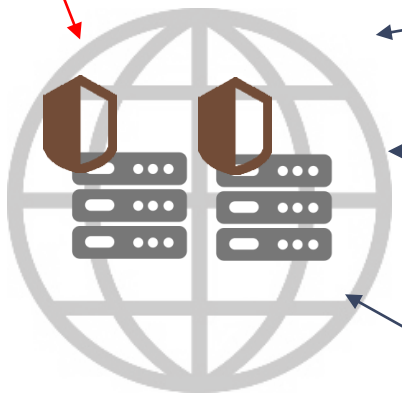
## Zentrale

LAN




DSL Router

Internet
DSL/Mobilfunk



Redundante IoT-Sicherheits-Gateways übernehmen die „Schutz- & Abwehr-Arbeit" für Sie

## Dezentrale Aussenstationen

SCHRAML Fernwirkstationen sind Embedded IoT-Komponenten mit gehärtetem Linux und umfangreichen Sicherheitsfeatures

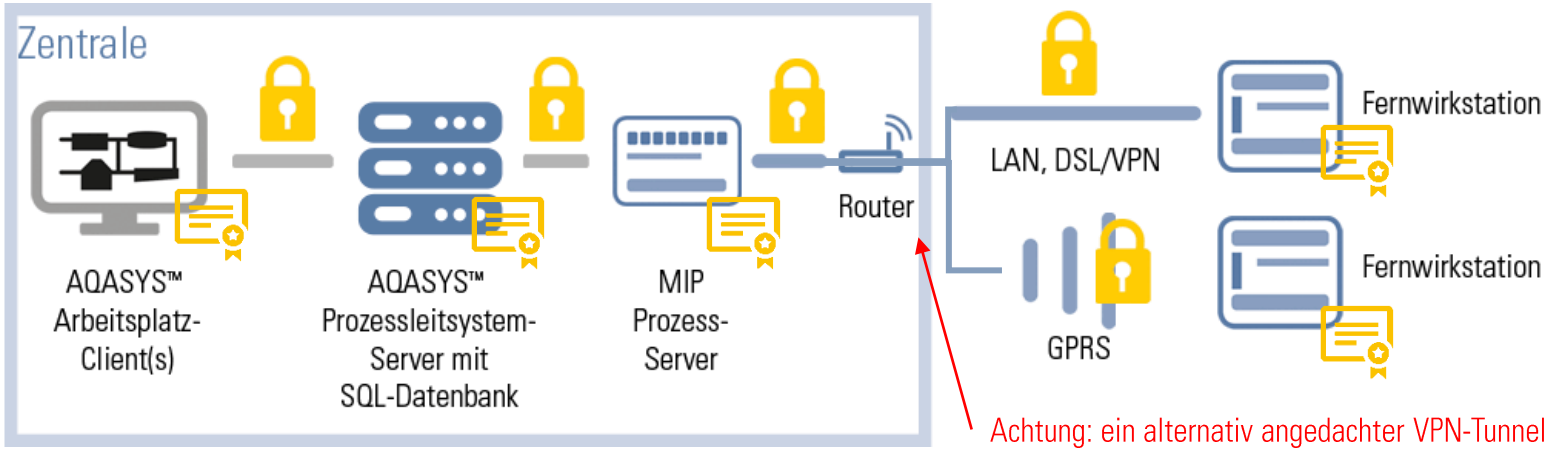
# Zusätzliche Option: Erhöhte IT-Sicherheit
# Schutz vor Manipulation der Datenkommunikation und Steuerbefehle

## Durchgängige **SSL/TLS Verschlüsselung**

der Datenkommunikation zum Schutz der kommunizierten Daten und Steuerbefehle (vor Mitlesen und Manipulation) zwischen allen (!) Komponenten eines Prozessleit- und Fernwirksystems

## Anlagen- und gerätespezifische Zertifikate

zur Sicherstellung der Authentifizierung (wer bist du *tatsächlich*? Akzeptiert dich das System?) von Sender und Empfänger von Daten und Steuerbefehlen




Achtung: ein alternativ angedachter VPN-Tunnel würde hier am Router enden – die Kommunikation im zentralen Netzwerk ist ungeschützt aber für Manipulation hoch interessant

# Anlagen- und gerätespezifische Zertifikate


- Der Kunde (die Anlage) erhält von SCHRAML einen **Sicherheits-USB-Stick**, mit dem die individuellen, anlagen- und gerätespezifische Zertifikate erzeugt und auf die Geräte übertragen werden.

- Der Sicherheits-USB-Stick ist FIPS Security 140-2 Level 3 zertifiziert und verfügt über eine AES 256-bit Hardware-Verschlüsselung, so dass der Stick nicht ausgelesen werden kann.
- Die Zertifikate werden für **keine andere** Anlage genutzt. Das heißt: Ausschließlich die Geräte mit den von diesem Dongle erstellten Zertifikaten vertrauen sich.

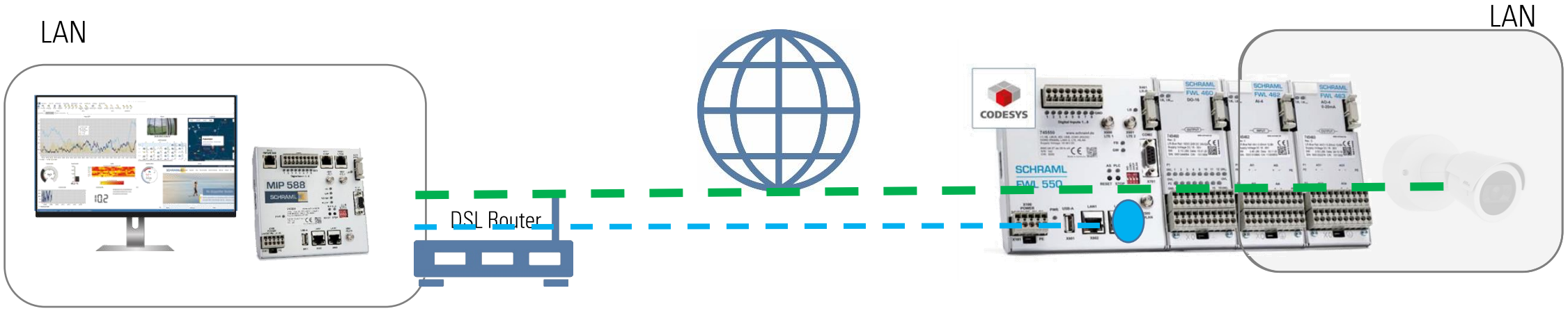
▶ Für die verschlüsselte und sicher authentifizierte Kommunikation müssen somit alle Komponenten des Prozessleit- und Fernwirksystems mit einem entsprechenden Zertifikat ausgestattet werden:
alle Clients, alle Server, alle Stationen

▶ Der Stick geht ab Auslieferung in das Eigentum der Anlage über. Die Anlage entscheidet, wer (intern/extern) diesen Stick verwenden darf, d.h. anlagen- und gerätespezifische Zertifikate damit erstellen kann.
→ die Anlage trägt die Verantwortung für ihre spezifischen Zertifikate und damit auch für ihre eigene IT-Sicherheit.

# Fernprogrammierung der SPSen – komfortabel & sicher
# VPN und VPN Forwarding: permanent oder temporär

## Zentrale

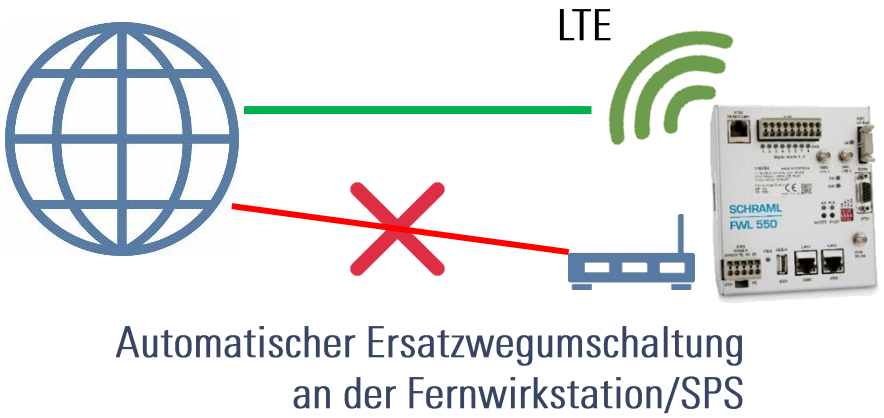
## Dezentrale Aussenstation




- **VPN-Dienste**: TOP flexibel da unterschiedliche und moderne VPN-Dienste wählbar (Vorgaben durch zentralen Router
  → OpenVPN | IPSec | Wireguard

- **VPN Tunnel permanent oder temporär (aus AQASYS aktivierbar für frei definierbare Zeit)**
- temporär aktivierbar (statt permanent) hilfreich, wenn man z.B. die SPS aus der Ferne programmieren will und sonst den Durchgriff auf die SPS schützen will und Datenrate reduzieren möchte

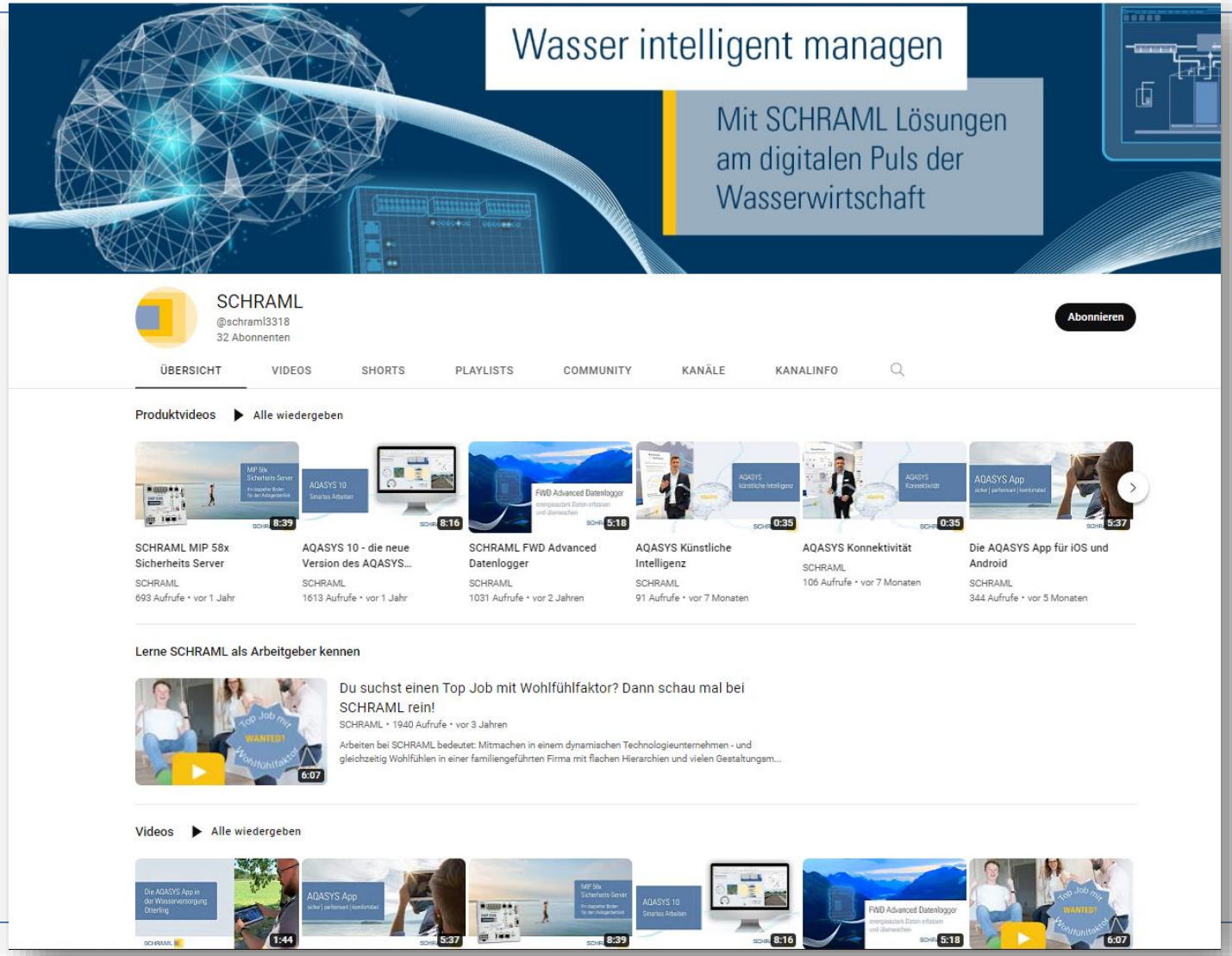
# FWL 550 Option – automatische Ersatzwegschaltung DSL <–> LTE


- Verfügbarkeit des Standard-Übertragungsweges (DSL über DSL-Router) wird kontinuierlich geprüft
- bei Nicht-Verfügbarkeit wird automatisch auf den Ersatzweg LTE/GPRS (integriertes LTE-Modem) umgeschaltet. Ist der Standardweg wieder verfügbar, wird automatisch wieder auf ihn zurückgeschaltet.
- Eine potentielle VPN Verbindung ist auch nach der automatischen Umschaltung des Übertragungswegs sichergestellt.


Zeit für Ihre Fragen

# SCHRAML YouTube – Produkt Videos



SCHRAML

Bis zum nächsten Webinar
z.B. Donnerstag, 16.01.
Kanalnetz & RÜB-Management

# Agenda

- Motivation: Gesetzgeber/NIS2, BSI/LSI, KRITIS & Verbände (DWA, DVGW)
- ZIELE und MASSNAHMEN
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität (z.B. Netzwerkkommunikation, Netzwerksicherheit), u. weitere
  - → siehe auch Anforderungen DWA-Tool (z.B. Brandschutz, Ersatzregelungen, Notfallpläne, etc.)
- SCHRAML: Organisatorische Maßnahmen, Techn. Maßnahmen/Produkte
- AQASYS
  - Struktur, Design/Architektur, sichere Datenbankzugriffe/Sicherheitsrichtlinien
  - System Methoden, Vermeidung XSS, SQL Injection, Brute Force, DDNS
  - Loginverfahren, Fehlversuche/Brute Force, SHA, 2-Faktor TOTP, Domain/Active Directory, SSL/TLS Verschlüsselung/Authentifizierung mit Zertifikaten, VPN Einsatz
  - Benutzer-/Rechtemanagement
  - Dokumentation im Leitvorgangsarchiv
  - Backup, SQL
  - Aktuelle Server-/PC Betriebssysteme
  - Zentrale: VPN mit fester IP, Webserver mit fester IP, Portfreigabe; Firewall Management; Monitoring
- AQASYS Web/App
  - SSL/TLS.
- Alarmierung?
  - Umfangreiche Alarmierung, Identifikation Quittierung
  - Redundanz der Alarmierung
- MIP
  - Robuste Linux Systeme, Härtung, Netzwerksegmentierung
  - Notbediensystem mit HMI, Redundanz/Ausfallsicherheit, Verfügbarkeit, Anlagen-/Betriebssicherheit
- Fernwirktechnik
  - Sicheres Fernwirken über Security Gateways
  - VPN, VPN Router, Stationen als VPN Clients (OpenVPN, Ipsec, WireGuard)
  - Erhöhte IT-Sicherheit

# Agenda

- Motivation: Gesetzgeber/NIS2, BSI/LSI, KRITIS & Verbände (DWA, DVGW)
- ZIELE und MASSNAHMEN
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität (z.B. Netzwerkkommunikation, Netzwerksicherheit), u. weitere
  - → siehe auch Anforderungen DWA-Tool (z.B. Brandschutz, Ersatzregelungen, Notfallpläne, etc.)
- SCHRAML: Organisatorische Maßnahmen, Techn. Maßnahmen/Produkte
- AQASYS
  - Struktur, Design/Architektur, sichere Datenbankzugriffe/Sicherheitsrichtlinien
  - System Methoden, Vermeidung XSS, SQL Injection, Brute Force, DDNS
  - Loginverfahren, Fehlversuche/Brute Force, SHA, 2-Faktor TOTP, Domain/Active Directory, SSL/TLS Verschlüsselung/Authentifizierung mit Zertifikaten, VPN Einsatz
  - Benutzer-/Rechtemanagement
  - Dokumentation im Leitvorgangsarchiv
  - Backup, SQL
  - Aktuelle Server-/PC Betriebssysteme
  - Zentrale: VPN mit fester IP, Webserver mit fester IP, Portfreigabe; Firewall Management; Monitoring
- AQASYS Web/App
  - SSL/TLS.
- Alarmierung?
  - Umfangreiche Alarmierung, Identifikation Quittierung
  - Redundanz der Alarmierung
- MIP
  - Robuste Linux Systeme, Härtung, Netzwerksegmentierung
  - Notbediensystem mit HMI, Redundanz/Ausfallsicherheit, Verfügbarkeit, Anlagen-/Betriebssicherheit
- Fernwirktechnik
  - Sicheres Fernwirken über Security Gateways
  - VPN, VPN Router, Stationen als VPN Clients (OpenVPN, Ipsec, WireGuard)
  - Erhöhte IT-Sicherheit

# Agenda

- Motivation: Gesetzgeber/NIS2, BSI/LSI, KRITIS & Verbände (DWA, DVGW)
- ZIELE und MASSNAHMEN
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität (z.B. Netzwerkkommunikation, Netzwerksicherheit), u. weitere
  - → siehe auch Anforderungen DWA-Tool (z.B. Brandschutz, Ersatzregelungen, Notfallpläne, etc.)
- SCHRAML: Organisatorische Maßnahmen, Techn. Maßnahmen/Produkte
- AQASYS
  - Struktur, Design/Architektur, sichere Datenbankzugriffe/Sicherheitsrichtlinien
  - System Methoden, Vermeidung XSS, SQL Injection, Brute Force, DDNS
  - Loginverfahren, Fehlversuche/Brute Force, SHA, 2-Faktor TOTP, Domain/Active Directory, SSL/TLS Verschlüsselung/Authentifizierung mit Zertifikaten, VPN Einsatz
  - Benutzer-/Rechtemanagement
  - Dokumentation im Leitvorgangsarchiv
  - Backup, SQL
  - Aktuelle Server-/PC Betriebssysteme
  - Zentrale: VPN mit fester IP, Webserver mit fester IP, Portfreigabe; Firewall Management; Monitoring
- AQASYS Web/App
  - SSL/TLS.
- Alarmierung?
  - Umfangreiche Alarmierung, Identifikation Quittierung
  - Redundanz der Alarmierung
- MIP
  - Robuste Linux Systeme, Härtung, Netzwerksegmentierung
  - Notbediensystem mit HMI, Redundanz/Ausfallsicherheit, Verfügbarkeit, Anlagen-/Betriebssicherheit
- Fernwirktechnik
  - Sicheres Fernwirken über Security Gateways
  - VPN, VPN Router, Stationen als VPN Clients (OpenVPN, Ipsec, WireGuard)
  - Erhöhte IT-Sicherheit

# Agenda

- Motivation: Gesetzgeber/NIS2, BSI/LSI, KRITIS & Verbände (DWA, DVGW)
- ZIELE und MASSNAHMEN
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität (z.B. Netzwerkkommunikation, Netzwerksicherheit), u. weitere
  - → siehe auch Anforderungen DWA-Tool (z.B. Brandschutz, Ersatzregelungen, Notfallpläne, etc.)
- SCHRAML: Organisatorische Maßnahmen, Techn. Maßnahmen/Produkte
- AQASYS
  - Struktur, Design/Architektur, sichere Datenbankzugriffe/Sicherheitsrichtlinien
  - System Methoden, Vermeidung XSS, SQL Injection, Brute Force, DDNS
  - Loginverfahren, Fehlversuche/Brute Force, SHA, 2-Faktor TOTP, Domain/Active Directory, SSL/TLS Verschlüsselung/Authentifizierung mit Zertifikaten, VPN Einsatz
  - Benutzer-/Rechtemanagement
  - Dokumentation im Leitvorgangsarchiv
  - Aktuelle Server-/PC Betriebssysteme
  - Zentrale: VPN mit fester IP, Webserver mit fester IP, Portfreigabe; Firewall Management; Monitoring
- AQASYS Web/App
  - SSL/TLS.
- Alarmierung?
  - Umfangreiche Alarmierung, Identifikation Quittierung
  - Redundanz der Alarmierung
- MIP
  - Robuste Linux Systeme, Härtung, Netzwerksegmentierung
  - Notbediensystem mit HMI, Redundanz/Ausfallsicherheit, Verfügbarkeit, Anlagen-/Betriebssicherheit
- Fernwirktechnik
  - Sicheres Fernwirken über Security Gateways
  - VPN, VPN Router, Stationen als VPN Clients (OpenVPN, Ipsec, WireGuard)
  - Erhöhte IT-Sicherheit

# Agenda

- Motivation: Gesetzgeber/NIS2, BSI/LSI, KRITIS & Verbände (DWA, DVGW)
- ZIELE und MASSNAHMEN
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität (z.B. Netzwerkkommunikation, Netzwerksicherheit), u. weitere
  - → siehe auch Anforderungen DWA-Tool (z.B. Brandschutz, Ersatzregelungen, Notfallpläne, etc.)
- SCHRAML: Organisatorische Maßnahmen, Techn. Maßnahmen/Produkte
- AQASYS
  - Struktur, Design/Architektur, sichere Datenbankzugriffe/Sicherheitsrichtlinien
  - System Methoden, Vermeidung XSS, SQL Injection, Brute Force, DDNS
  - Loginverfahren, Fehlversuche/Brute Force, SHA, 2-Faktor TOTP, Domain/Active Directory, SSL/TLS Verschlüsselung/Authentifizierung mit Zertifikaten, VPN Einsatz
  - Benutzer-/Rechtemanagement
  - Dokumentation im Leitvorgangsarchiv
  - Aktuelle Server-/PC Betriebssysteme
  - Zentrale: VPN mit fester IP, Webserver mit fester IP, Portfreigabe; Firewall Management; Monitoring
- AQASYS Web/App
  - SSL/TLS.
- Alarmierung?
  - Umfangreiche Alarmierung, Identifikation Quittierung
  - Redundanz der Alarmierung
- MIP
  - Robuste Linux Systeme, Härtung, Netzwerksegmentierung
  - Notbediensystem mit HMI, Redundanz/Ausfallsicherheit, Verfügbarkeit, Anlagen-/Betriebssicherheit
- Fernwirktechnik
  - Sicheres Fernwirken über Security Gateways
  - VPN, VPN Router, Stationen als VPN Clients (OpenVPN, Ipsec, WireGuard)
  - Erhöhte IT-Sicherheit

# Agenda

- Motivation: Gesetzgeber/NIS2, BSI/LSI, KRITIS & Verbände (DWA, DVGW)
- ZIELE und MASSNAHMEN
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität (z.B. Netzwerkkommunikation, Netzwerksicherheit), u. weitere
  - → siehe auch Anforderungen DWA-Tool (z.B. Brandschutz, Ersatzregelungen, Notfallpläne, etc.)
- SCHRAML: Organisatorische Maßnahmen, Techn. Maßnahmen/Produkte
- AQASYS
  - Struktur, Design/Architektur, sichere Datenbankzugriffe/Sicherheitsrichtlinien
  - System Methoden, Vermeidung XSS, SQL Injection, Brute Force, DDNS
  - Loginverfahren, Fehlversuche/Brute Force, SHA, 2-Faktor TOTP, Domain/Active Directory, SSL/TLS Verschlüsselung/Authentifizierung mit Zertifikaten, VPN Einsatz
  - Benutzer-/Rechtemanagement
  - Dokumentation im Leitvorgangsarchiv
  - Aktuelle Server-/PC Betriebssysteme
  - Zentrale: VPN mit fester IP, Webserver mit fester IP, Portfreigabe; Firewall Management; Monitoring
- AQASYS Web/App
  - SSL/TLS.
- Alarmierung?
  - Umfangreiche Alarmierung, Identifikation Quittierung
  - Redundanz der Alarmierung
- MIP
  - Robuste Linux Systeme, Härtung, Netzwerksegmentierung
  - Notbediensystem mit HMI, Redundanz/Ausfallsicherheit, Verfügbarkeit, Anlagen-/Betriebssicherheit
- Fernwirktechnik
  - Sicheres Fernwirken über Security Gateways
  - VPN, VPN Router, Stationen als VPN Clients (OpenVPN, Ipsec, WireGuard)
  - Erhöhte IT-Sicherheit

# Agenda

- Motivation: Gesetzgeber/NIS2, BSI/LSI, KRITIS & Verbände (DWA, DVGW)
- ZIELE und MASSNAHMEN
  - Vertraulichkeit
  - Integrität
  - Verfügbarkeit
  - Authentizität (z.B. Netzwerkkommunikation, Netzwerksicherheit), u. weitere
  - → siehe auch Anforderungen DWA-Tool (z.B. Brandschutz, Ersatzregelungen, Notfallpläne, etc.)
- SCHRAML: Organisatorische Maßnahmen, Techn. Maßnahmen/Produkte
- AQASYS
  - Struktur, Design/Architektur, sichere Datenbankzugriffe/Sicherheitsrichtlinien
  - System Methoden, Vermeidung XSS, SQL Injection, Brute Force, DDNS
  - Loginverfahren, Fehlversuche/Brute Force, SHA, 2-Faktor TOTP, Domain/Active Directory, SSL/TLS Verschlüsselung/Authentifizierung mit Zertifikaten, VPN Einsatz
  - Benutzer-/Rechtemanagement
  - Dokumentation im Leitvorgangsarchiv
  - Aktuelle Server-/PC Betriebssysteme
  - Zentrale: VPN mit fester IP, Webserver mit fester IP, Portfreigabe; Firewall Management; Monitoring
- AQASYS Web/App
  - SSL/TLS.
- Alarmierung?
  - Umfangreiche Alarmierung, Identifikation Quittierung
  - Redundanz der Alarmierung
- MIP
  - Robuste Linux Systeme, Härtung, Netzwerksegmentierung
  - Notbediensystem mit HMI, Redundanz/Ausfallsicherheit, Verfügbarkeit, Anlagen-/Betriebssicherheit
- Fernwirktechnik
  - Sicheres Fernwirken über Security Gateways
  - VPN, VPN Router, Stationen als VPN Clients (OpenVPN, Ipsec, WireGuard)
  - Erhöhte IT-Sicherheit

# Anlagen- und gerätespezifische Zertifikate


- Der Kunde (die Anlage) erhält von SCHRAML einen **Sicherheits-USB-Stick**, mit dem die individuellen, anlagen- und gerätespezifische Zertifikate erzeugt und auf die Geräte übertragen werden.

- Der Sicherheits-USB-Stick ist FIPS Security 140-2 Level 3 zertifiziert und verfügt über eine AES 256-bit Hardware-Verschlüsselung, so dass der Stick nicht ausgelesen werden kann.
- Die Zertifikate werden für **keine andere** Anlage genutzt. Das heißt: Ausschließlich die Geräte mit den von diesem Dongle erstellten Zertifikaten vertrauen sich.

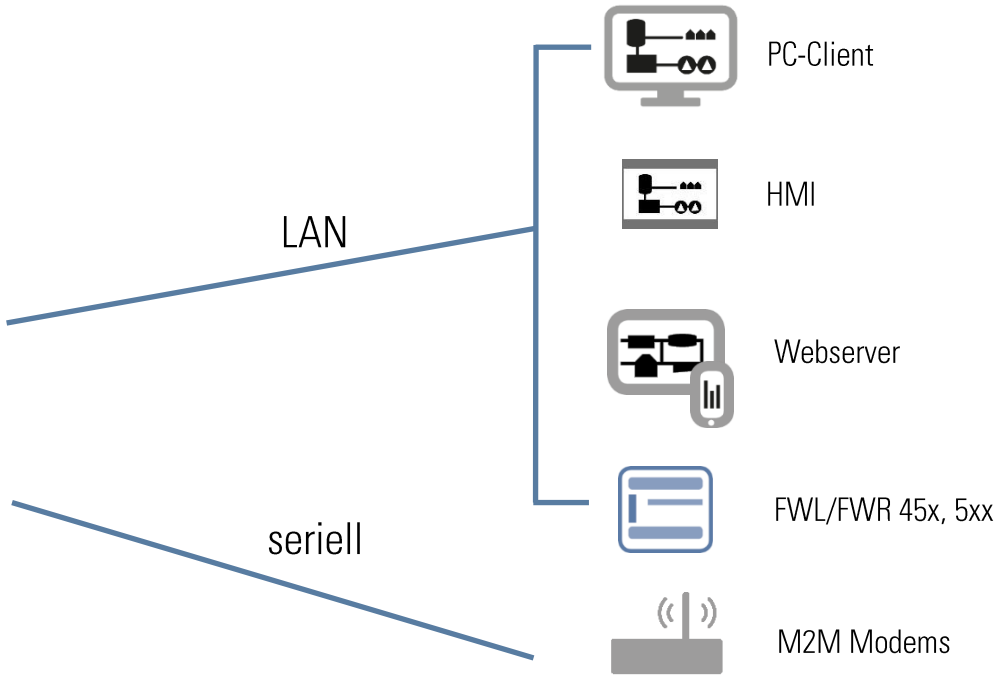
Für die verschlüsselte und sicher authentifizierte Kommunikation müssen somit alle nachstehenden Komponenten mit einem entsprechenden Zertifikat ausgestattet werden:

- alle **AQASYS Clients**
  (PC-Client, AQASYS HMI, Webserver, Report Designer)
- **AQASYS Server**
- Sicherheitsserver **MIP bzw. MIP Task**
- für Fernwirkstationen mit mobiler Datenübertragung:
  - auf **FWR 520 oder FWL 550**
  - auf alle **3G/4G M2M-Modems**
- bei Fernwirkstationen mit DSL, LAN, DSL/VPN-Datenübertragung:
  - auf **alle FWL-Stationen**

# Anwendung des Sicherheits-USB-Sticks zur Erstellung und Übertragung der Zertifikate (1)

- Der Stick geht ab Auslieferung in das Eigentum der Anlage über. Die Anlage entscheidet, wer (intern/extern) diesen Stick verwenden darf, d.h. anlagen- und gerätespezifische Zertifikate damit erstellen kann. D.h. die Anlage trägt die Verantwortung für ihre spezifischen Zertifikate und damit auch für ihre eigene IT-Sicherheit.

- <u>Inbetriebnahme</u>




  - 1. Schritt: Einstecken in USB-Anschluss des PLS-Rechners (Server)