Maßnahmen der Wasserversorgung gegen Cyberattacken Teil 1

Infotag Wasser- Oberschützen

Mario Unterwainig
BMNT, Abteilung Siedlungswasserwirtschaft
Oberschützen, 14. November 2019

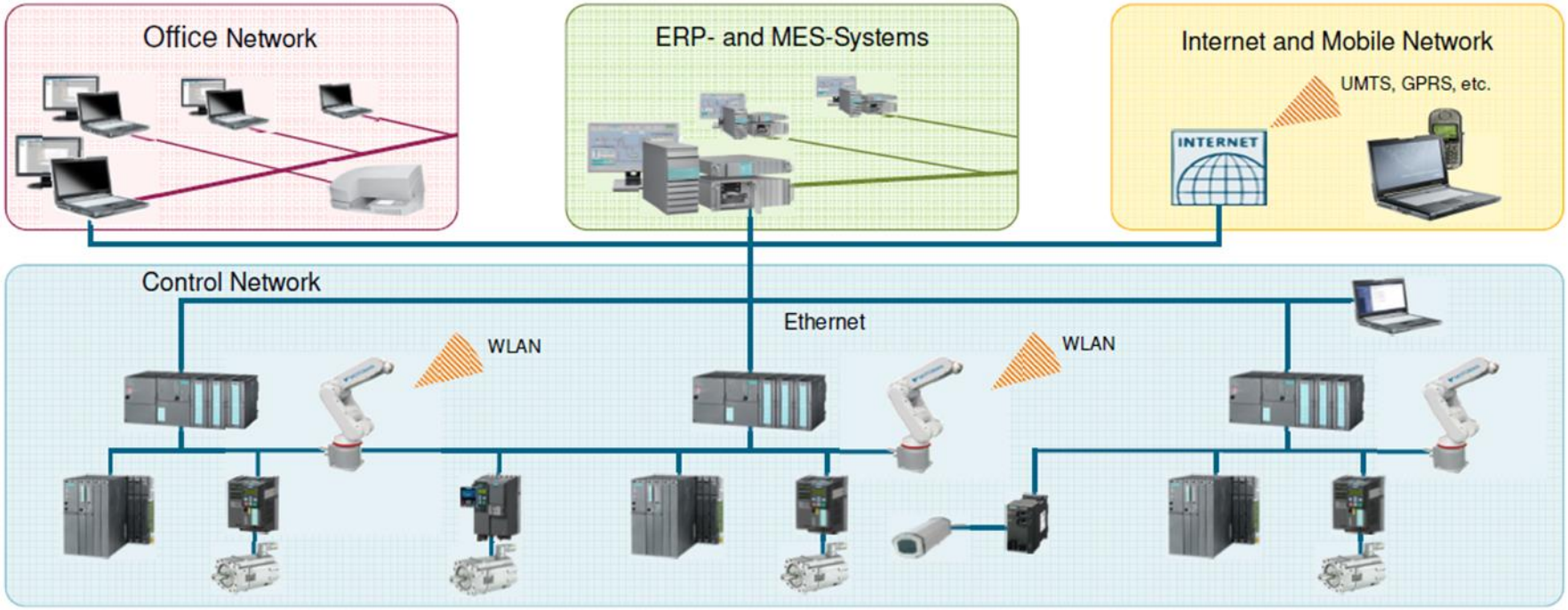
Inhalt

- Einleitung und Überblick
- Strategie und Umsetzung
- Zusammenfassung

Einleitung und Überblick

Quelle: Wikipedia; Nassim Taleb

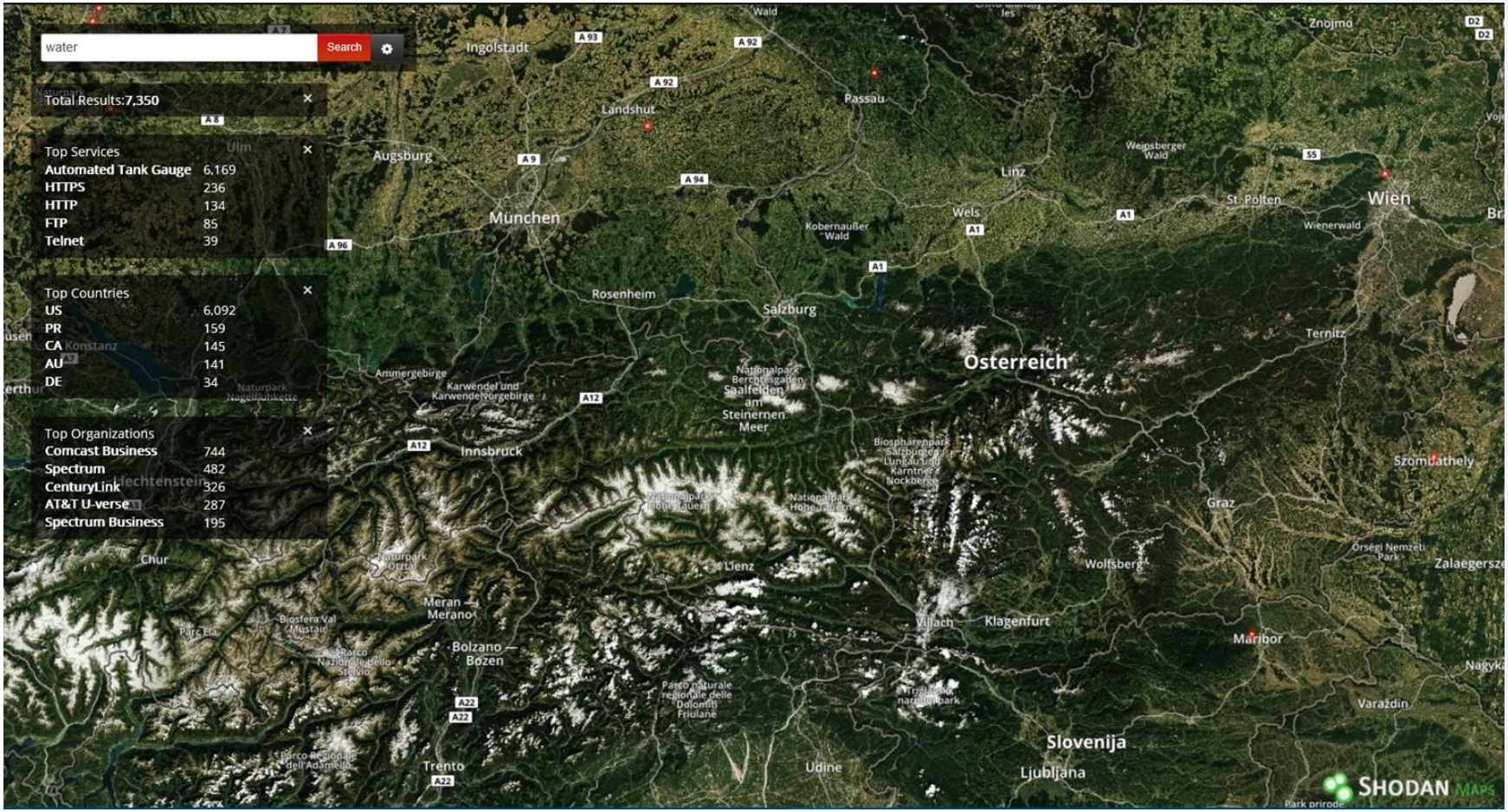
OT im Wandel



Quelle: Siemens AG

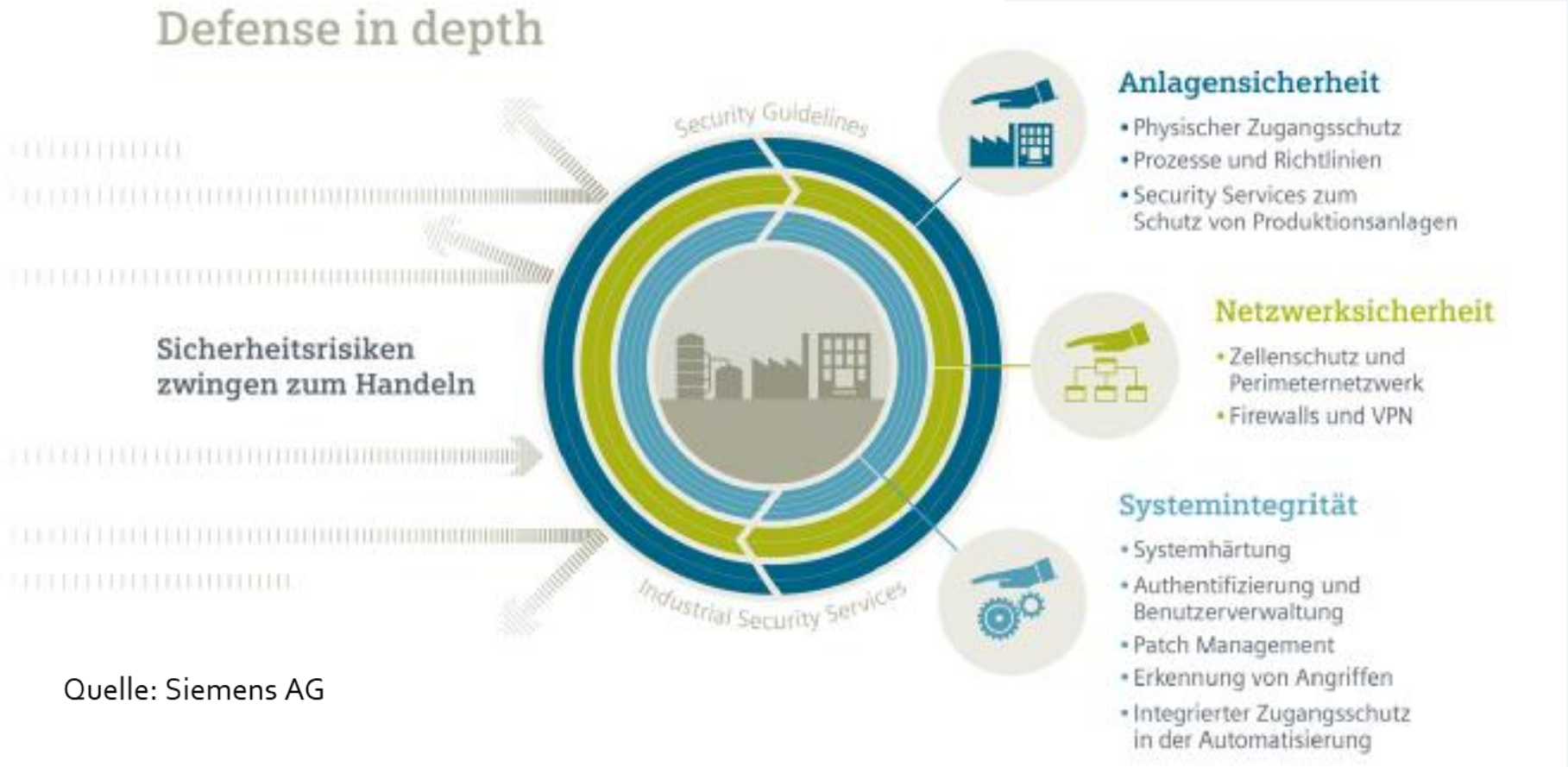
OT und IT

Quelle: Siemens AG



Quelle: Shodan

Strategie und Umsetzung

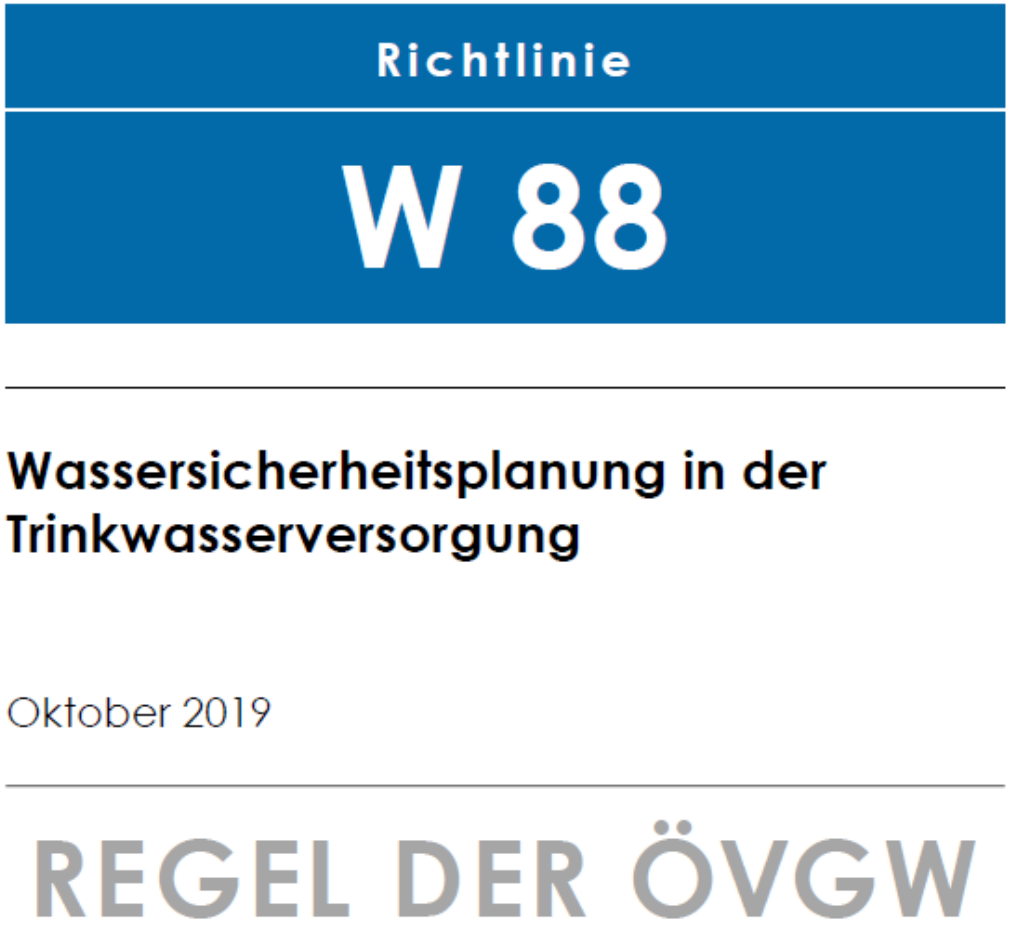


Quelle: Siemens AG

5 „Tibeter" des Multibarrierenkonzepts zur Erhöhung der Cybersicherheit

1. Identifizieren
2. Schützen
3. Erkennen
4. Reagieren
5. Wiederherstellen

Alles neu?



Quelle: ÖVGW W 88

Identifizieren I

Quelle: ÖVGW W 88

Identifizieren II

- Verständnis der **Cybersicherheitsrisiken** für Systeme, Personen, Vermögenswerte, Daten usw. zu entwickeln
- Versteht man die **aktuellen Geschäftsanforderungen** und die damit verbundenen Risiken, bzw. kann der Wasserversorger konkrete **Bedrohungen erkennen** und seine Sicherheitsmaßnahmen priorisieren
- Zu den wichtigsten Aktivitäten in diesem Schritt gehören:
  - Asset Management
  - Governance und Risikobewertung
- Hilfsmittel siehe W 88

Identifizieren III

CHECKLISTE TEIL IV: IKT-Gefährdungen					
13	**Verlust oder Offenlegung von Information**	*Zutreffend*	*Nicht Zutreffend*	*Unklar*	*ÖVGW Regel*
13.1	Offenlegung schützenswerter Informationen *Beispiele: Passwörter in Lade oder auf PC geklebt, Ausgabe an Dritte (alle Gefährdungen)*	O	O	O	**W 74** **W 71/3**
13.2	Verlust von Geräten, Datenträgern oder Dokumenten *Beispiele: USB-Stick verloren mit Information über Fernwirktechnik (alle Gefährdungen)*	O	O	O	**W 74** **W 71/3**
14	**Ausspähen von Informationen**				
14.1	Ausspähen von Informationen, Spionage *Beispiele: Trojanisches Pferd über E-Mail, um Passwörter oder andere Zugangsdaten auszuspähen; akustisch nicht gut gesicherte Arbeitsplätze – Besucher/Gäste hören mit (alle Gefährdungen)*	O	O	O	**W 74** **W 71/3**
14.2	Social Engineering *Beispiele: Manipulation von Mitarbeitern per Anruf (Administrator, der noch schnell das Passwort braucht, um etwas zu beheben); Aufbau längerer Beziehung zum Opfer; Phishing (alle Gefährdungen)*	O	O	O	**W 74** **W 71/3**
14.3	Diebstahl von Geräten, Datenträgern oder Dokumenten *Beispiele: Diebstahl von mobilen Endgeräten (Laptops, Tablets, Smartphones) und v. a. Datenträgern; Mitnahme von vertraulichen Daten bei Verlassen des Unternehmens (alle Gefährdungen)*	O	O	O	**W 74** **W 71/3**

Quelle: ÖVGW W 88

Schützen I

- Implementieren geeigneter **Sicherheitsmaßnahmen** und -**kontrollen**, um die kritische Infrastruktur vor Cyberbedrohungen zu schützen
  - physischer **Zugangsschutz** der Anlagen
  - das **Identitätsmanagement** und die **Zugangskontrolle**
  - die **Sensibilisierung** und **Schulung** von Mitarbeitern

Schützen II

- Sicherstellen, dass **Kommunikations**- und **Steuernetzwerke** geschützt sind
- Definieren von **Berechtigungsstufen** nach dem Prinzip der kleinstmöglichen Berechtigung sowie der Trennung von Funktionen
- Sicherstellen, dass Unterhaltsarbeiten an Ihren Systemen, die über **Fernzugriffe** erfolgen, **aufgezeichnet** und **dokumentiert** werden
- Sicherstellen, dass kein unautorisierter Zugriff möglich ist

Erkennen I

- Ereignisse **schnell erkennen** und die Risiken für den Betrieb darstellen
- Bestimmen Sie die **Auswirkungen** möglicher Events
- Sicherstellen, dass **Aktivitäten** von **externen Dienstleistern** überwacht werden, so dass Cybersecurity-Vorfälle entdeckt werden können

Erkennen II

- Definieren Sie **klare Rollen** und **Verantwortlichkeiten**, so dass klar ist, wer wofür zuständig ist und wer welche Kompetenzen hat
- **Kommunizieren** Sie detektierte **Vorfälle** an die zuständigen Stellen (z.B. Lieferanten, Kunden, Partner, Behörden etc.)

Reagieren

- Ergreifen von **Maßnahmen** gegen einen eingetretenen Cybersicherheitsvorfall
- Dabei können folgenden Techniken verwendet werden, um die Auswirkungen eines Vorfalls einzugrenzen:
  - Planung
  - Kommunikation und Analyse
  - Verbesserung von Reaktionen

Wiederherstellen

- Implementieren von **Aktivitäten** zum **Wiederherstellen** seiner Dienstleistung, die von einem Sicherheitsvorfall betroffen waren
- Aktivitäten die eine **rechtzeitige Wiederherstellung** des „Regelbetrieb"unterstützen, um die Auswirkungen von Vorfällen zu verringern
- Dazu gehören **Wiederherstellungsplanung**, Verbesserungen (z. B. Einführung neuer Richtlinien oder Aktualisierung bestehender Richtlinien) und Kommunikation, bzw. **Backups**
- Siehe W 74

Zusammenfassung I

Quelle: ÖVGW W 88

Zusammenfassung II

	Informations-und Kommunikationstechnologie (IKT)-Gefährdungen in der Abwasserreinigung							
	Anlagenbereiche Zonierungskonzept nach IEC-62443	Physischer Zugangsschutz		OT-Netzwerk				
	Komponente	Schaltschrank	Schachtbauwerk	Router	SPS	HMI	Sensor	Aktor
	Datum der Risikoanalyse							
	Hersteller							
	Fabrikat-Type							
	Firmwareversion							
	Seriennummer							
	Betriebsmittelkennzeichnung							
	Netzwerkanbindung							
	Gefahrenlisten Matrix (LARS ICS)							
1	Verlust oder Offenlegung von Information							
	Offenlegung schützenswerter Informationen	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend
1.1	*Beispiele: Passwörter in Lade oder auf PC geklebt, Ausgabe an Dritte (alle Gefährdungen)*			Standardpasswort geändert	Programmierschutz für SPS eingerichtet	Unterweisung der Mitarbeiter	Standardpasswort geändert	Standardpasswort geändert
	Verlust von Geräten, Datenträgern oder Dokumenten	nicht zutreffend	nicht zutreffend	umgesetzt	umgesetzt		umgesetzt	umgesetzt
1.2	*Beispiele: USB Stick verloren mit Information über Fernwirktechnik (alle Gefährdungen)*			Konfiguration gesichert	SPS Programm sicher abgelegt	Konfiguration gesichert	Konfiguration gesichert	Konfiguration gesichert
	Integritätsverlust schützenswerter Informationen	nicht zutreffend	nicht zutreffend	umgesetzt	umgesetzt		umgesetzt	umgesetzt
1.3	*Historie von Messungen gelöscht*			Protokollierung von Verbindungen	Protokollierung von Fehlermeldungen		Protokollierung von Verbindungen	Protokollierung von Verbindungen
2	Ausspähen von Informationen							

Quelle: ÖWAV AK-IKT-Sicherheit in der ARA, eigene Bearbeitung

Zusammenfassung III

- Maßnahmen Matrix

Funktion	Kategorie	ID	Aktivität	Praxisbeispiele	Ampel
	Inventar Management (Asset 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 entspricht. Mit hoher Priorität sind dabei besonders jene Anlagen und IKT-Systeme bedacht, die für den Abwasserentsorger zur Erfüllung des Betriebsziels einer geordneten Abwasserbehandlung wesentlich sind.	Id.I.1	Inventarisieren Sie all Ihre internen und externen IKT-Systme bzw. Softwareplattformen / -Lizenzen und Applikationen die für den Betrieb der Trinkwasserversorgung relevant sind. Dies umfasst mindestens: Fabrikat, Type, Herstellernummer (Baujahr), Firmware/Softwareversion		
		Id.I.2	Definieren Sie klare Rollen und Verantwortlichkeiten im Bereich der Cyber Security.		
	Subrating	**Id.I.**			
	Geschäftsumfeld (Business Environment) Die Ziele, Aufgaben und Aktivitäten des Unternehmens sind priorisiert und bewertet. Diese Informationen dienen als Grundlage für die Zuweisung der Verantwortlichkeiten hinsichtlich Cyber	Id.II.1	Erfassen Sie ihre externen Dienstleister und die eingesetzten Produkte bzw. kritische Abhängigkeiten	Internetanbieter, Mobilfunkbetreiber, Fernwartungszugriffe	
		Id.II.2	Sind kritische Abhängigkeiten vorhanden, müssen Anforderungen für kritische Dienstleistungen festgehalten sein.	Redundante Anbindungen, alternative Anbieter, Wartungsverträge, Verfügbarkeit und Wartezeiten von Dienstleistern	

Zusammenfassung IV

	Anlagenbereiche Zonierungskonzept nach IEC-62443	Physischer Zugangsschutz						
	Komponente	Gebäude	Zaun - Tor	Schaltschrank	Schachtbauwerk	Server	Workstation	N
	Datum der Risikoanalyse							
	Hersteller							T
	Fabrikat-Type							V
	Firmwareversion							V
	Seriennummer							S
	Betriebsmittelkennzeichnung							
	Netzwerkanbindung							E
	Gefahrenlisten Matrix (LARS ICS)							
	Gefahrenlisten Matrix (LARS ICS)							
1	Verlust oder Offenlegung von Information							
	Offenlegung schützenswerter Informationen	zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	nicht zutreffend	
1.1	*Beispiele: Passwörter in Lade oder auf PC geklebt, Ausgabe an Dritte (alle Gefährdungen)*	Unterweisung der Mitarbeiter (DSGVO)				Sichere Benutzer und Kennwortvergabe	Unterweisung der Mitarbeiter (DSGVO)	
	Maßnahme	umgesetzt						
	Beschreibung der Maßnahme	Si.II.1 und Si.II.2						

Quelle: ÖWAV AK-IKT-Sicherheit in der ARA, eigene Bearbeitung

Zusammenfassung V

- IKT spielt zunehmende Rolle➔ deswegen IKT-Sicherheit wichtig (Truthahn Illusion)
- BMNT Studie „*Sicherheit von Informations- und Kommunikationssystemen in der österreichischen Siedlungswasserwirtschaft*"
- Umsetzung NISG für betroffene Betreiber (auch im Trinkwasser)
- Was ist mit dem Rest? 5.5000 WVU's
- Richtlinien W 88, W 74 erste Schritte zur Erhöhung der IKT-Sicherheit
- **Ausbaufähig** und **Zusammenführung** der einzelnen Teile in ein Dokument für Betreiber

Danke für Ihre Aufmerksamkeit!

Mario Unterwainig
BMNT, Abteilung Siedlungswasserwirtschaft
mario.unterwainig@bmnt.gv.at