JOANNEUM RESEARCH DIGITAL

Aktuelle Bedrohungen aus der Cyberwelt für die kritische Infrastruktur Wasserversorgung

DI Christian Derler

Graz, 04. Juli 2022

Aktuelle Bedrohungen aus der Cyberwelt für die kritische Infrastruktur Wasserversorgung

- Digitalisierung vergrößert die Angriffsfläche für Cyberattacken
- Wasserversorgungsunternehmen bleiben davon nicht verschont
- Art der Bedrohung und Methoden ändern sich laufend und werden komplexer
- ***Agenda – Teil 1***
  - Motivation und Fallbeispiele: Cyberangriffe auf die Wasserversorgung
  - Welche Angriffsmethoden und Ziele stecken dahinter?
  - Schäden durch Cyberangriffe
  - Stand der Forschung in Sachen Cybersichere Wasserversorgung
    – Überblick Forschungsprojekte
  - Was kann die Forschung leisten und wie profitieren Sie davon?

Forschungsgruppe Cyber Security and Defence

Security-by-Design – safety and security of AI systems; AI based security testing

Security-at-runtime – incident detection based on AI

Cyber Defence – analysis and incident detection

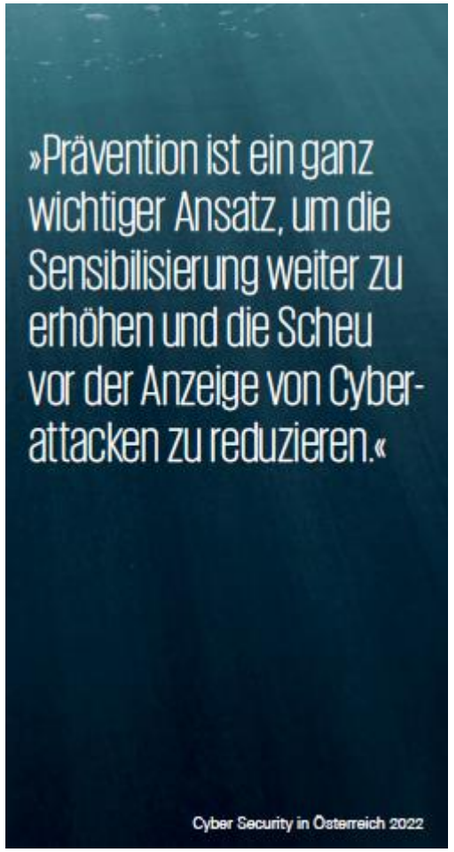
C4ISR applications

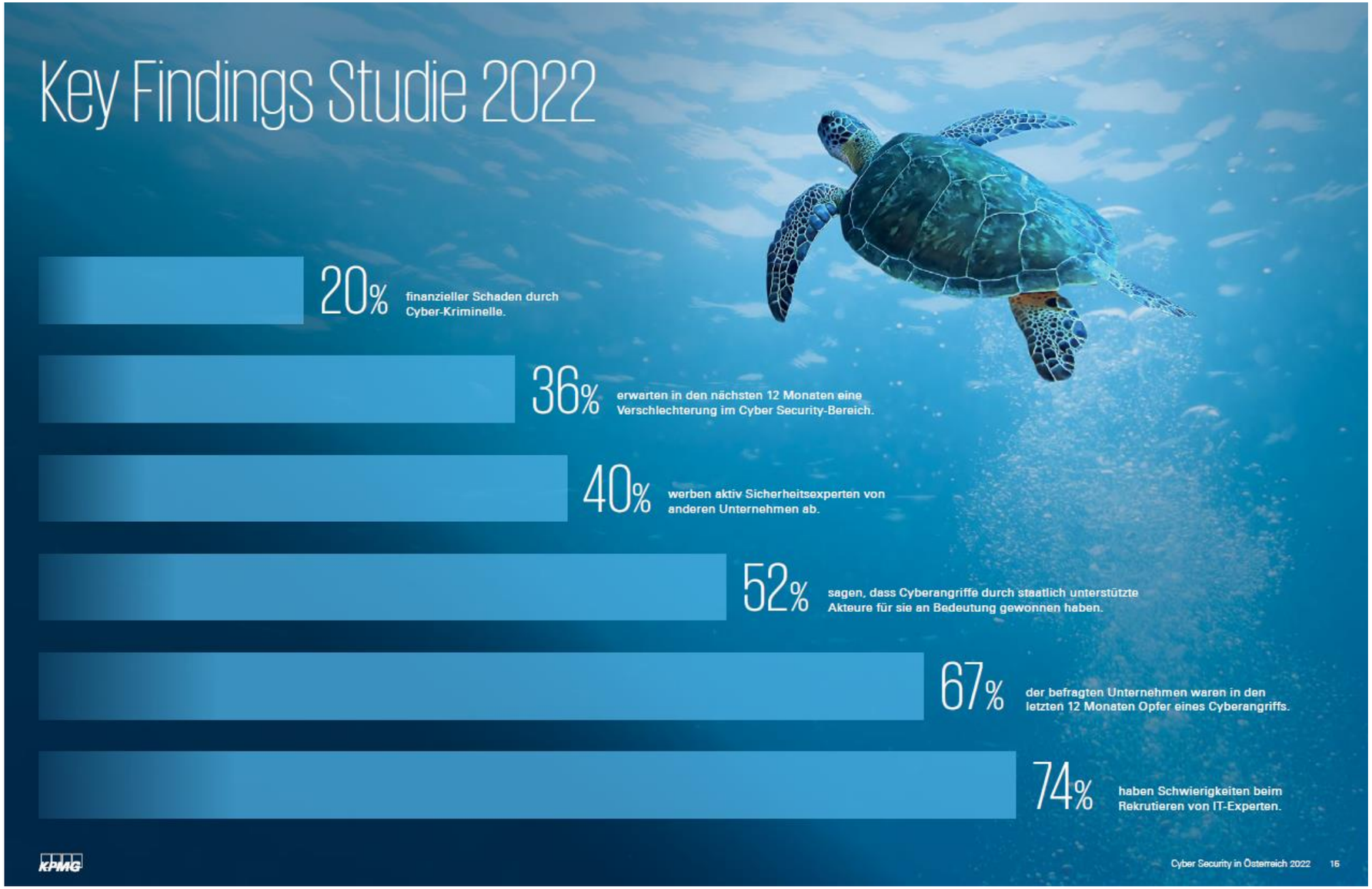
Foto: JOANNEUM RESEARCH

Federal Ministry Republic of Austria Interior

Federal Ministry Republic of Austria Defence

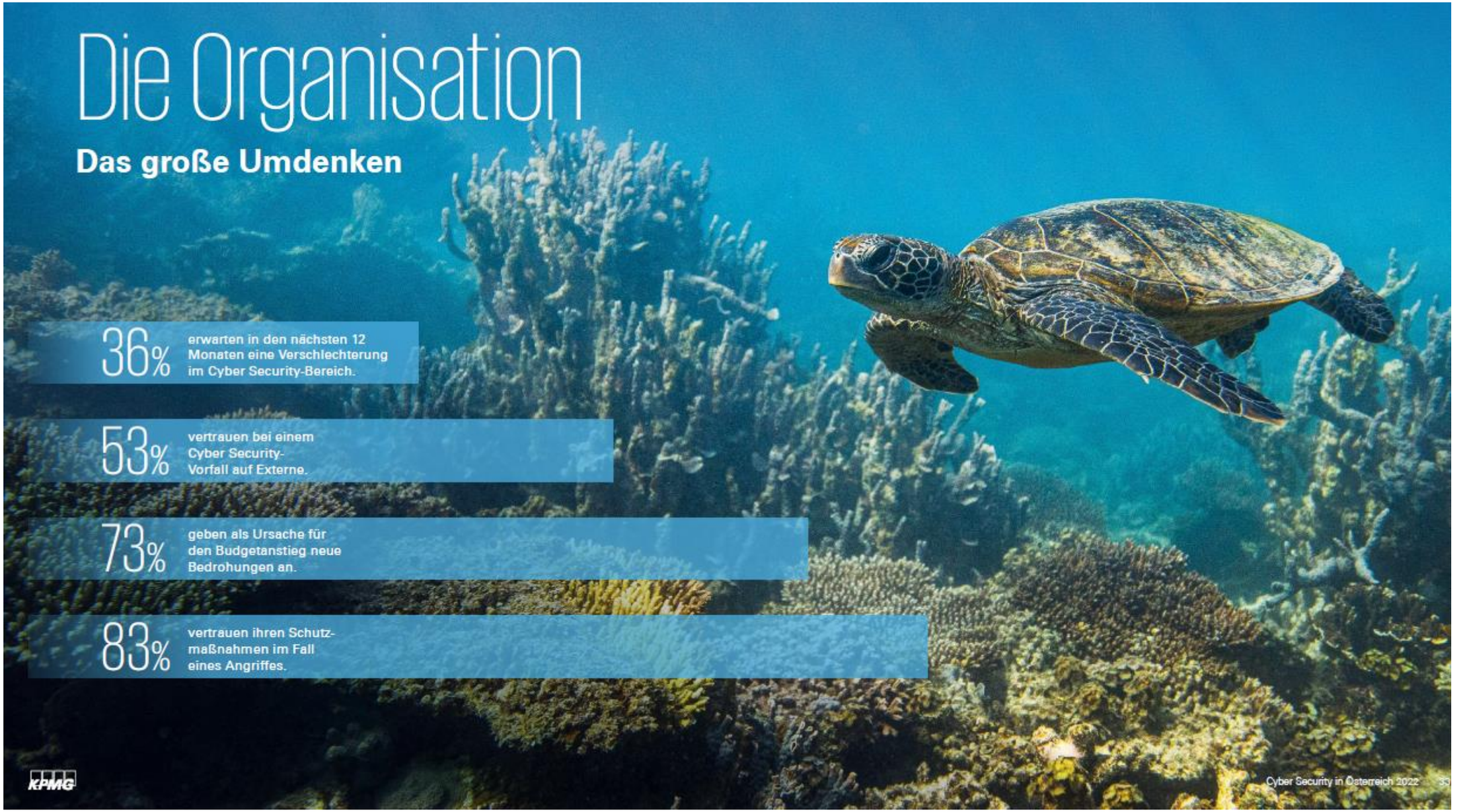
Motivation





Source: KPMG – Cyber Security in Österreich 2022; https://home.kpmg/at/de/home/insights/2022/05/cyber-security-oesterreich-2022.html

JOANNEUM RESEARCH DIGITAL



JOANNEUM RESEARCH DIGITAL

Motivation

- *Das Bedrohungspotential steigt*
  - Die Konsequenzen für Organisationen können **katastrophal** sein
  - Die offensichtlichste Folge von Cyberattacken ist **finanzieller Schaden,** entweder als Folge von Betrug, Erpressung und Lösegeldzahlung, Strafzahlungen oder Verdienstentgang und Verlust von Erlöschancen
  - Im Jahr **2021 stiegen die Kosten von Datendiebstahl von** 3,86 Millionen auf 4,24 Millionen US$

Source: https://www.ey.com/en_gl/consulting/how-to-manage-cyber-risk-with-a-security-by-design-approach

Sources:
EY How to manage cyber risk with a Security by Design approach
IBM Cost of a Data Breach Report 2021
EY Global Information Security Survey 2021

Motivation

- *Cybersecurity Markt – komplex und durch Krisen getrieben*
  - Organisationen haben damit zu **kämpfen**, eine klare, nachhaltige und effiziente Sicherheitsfunktion aufrecht zu erhalten
  - Viel zu viel Organisationen haben einen rein **reaktiven** Zugang zur Cybersecurity
  - *EY Global Information Security Survey* deckt auf, dass 65% der Unternehmen sich **mit Cybersecurity erst dann beschäftigen, wenn es bereits zu spät ist**

Source: https://www.ey.com/en_gl/consulting/how-to-manage-cyber-risk-with-a-security-by-design-approach

Sources:
EY How to manage cyber risk with a Security by Design approach
IBM Cost of a Data Breach Report 2021
EY Global Information Security Survey 2021

Motivation

43% say they have never been as concerned as they are now about their ability to manage the cyber threat.

68% of CEOs are planning a major technology investment in the next 12 months.

36% of respondents agree that it is only a matter of time before they suffer a breach that could have been avoided through investment.

More than half

55% of respondents say cybersecurity is coming under more scrutiny today than at any other point in their careers.

Source: EY Global Information Security Survey 2021

JOANNEUM RESEARCH DIGITAL

BBC Sign in News Sport

NEWS

Home Video World UK Business Tech

Technology

Hack attacks cut internet Liberia

4 November 2016

MIMIKAMA ZUERST DENKEN - DANN KLICKEN

Mimikama durchsuchen

AKTUELLES THEMEN SHOP NEWSLETTER ÜBER MIMIKAMA® PRESSE & KONTAKT

Hackerangriff auf Wiener Stephansdom

Die Glocken des Wiener Stephansdoms haben in der Nacht auf Mittwoch Bewohner und Bewohnerinnen der Innenstadt aus dem Schlaf gerissen. Die Ursache: offenbar ein Hackerangriff.

Tom Wannenmacher, 16. März 2022

DERSTANDARD

Unterstützung Abo Immosuche Jobsuche Anmelden

Web › Netzpolitik › IT-Security International Inland Wirtschaft Sport Panorama Kultur Etat Wissenschaft Lifestyle Diskurs Karriere Immobilien mehr...

82 Postings

IT-SICHERHEIT

Cyberangriff auf Innsbrucker Med-Uni: Erste Daten im Darknet aufgetaucht

Unter anderem dürften Reisepässe, Vertrags- und Finanzdaten erbeutet worden sein. Den Angriff beansprucht die Ransomware-Gruppe Vice Society für sich

Mickey Manakas, Andreas Proschofsky
27. Juni 2022, 17:02, 82 Postings

Gut eine Woche nach Bekanntwerden des Cyberangriffs auf die Medizinische Universität Innsbruck veröffentlichten die Angreifer am Wochenende eine erste Kostprobe der gestohlenen Daten. Infolgedessen übernahm die Ransomware-Gruppe Vice Society die Verantwortung für die Attacke. Zuletzt legten die Akteure die Verwaltung der italienischen Stadt Palermo lahm.

Ein Verzeichnis der erbeuteten Daten ist im Darknet zu finden. Glaubt man diesem, dürften Vertrags- und Finanzdaten, aber auch Reisepässe und Krankmeldungen von Mitarbeiterinnen und Mitarbeitern kopiert worden sein. An mehreren Stellen werden Namen genannt, die mit solchen aus dem Personal der Hochschule übereinstimmen. Unterdessen finden sich bisher jedoch keine Hinweise darauf, dass auch Patientinnen-Daten veröffentlicht wurden.

Manuela Groß, Vizerektorin für Finanzen und IT der Med-Uni Innsbruck, während einer Pressekonferenz zum Cyberangriff.

Foto: APA/EXPA/JOHANN GRODER

WERBUNG
Magenta lol Business

DERSTANDARD

Unterstützung Abo Immosuche Jobsuche Anmelden

Inland › Bundesländer › Kärnten International Wirtschaft Web Sport Panorama Kultur Etat Wissenschaft Lifestyle Diskurs Karriere Immobilien mehr...

NETZPOLITIK

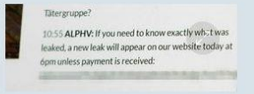
Grundversorgung weg, Politikerdaten im Netz: Wie Hacker Kärnten lahmlegten

Der Cyberangriff auf Kärnten ist exemplarisch dafür, wie Hacker seit Beginn der Pandemie vorgehen

Muzayen Al-Youssef, Walter Müller
13. Juni 2022, 06:00, 479 Postings

Als die Kärntner Landesregierung Anfang vergangener Woche per Livestream vor die Medien trat, um Fragen zum Hackerangriff auf die Kärntner Landesverwaltung zu beantworten, waren jene Hacker, die dafür verantwortlich sind, offenbar selbst anwesend. Sie drohten im Chat: Entweder zahlt Kärnten Lösegeld – fünf Millionen US-Dollar in Form von Kryptowährungen –, oder die Daten werden publiziert.

Das Land ist der Forderung nicht gefolgt. Nun tauchen häppchenweise Daten im Netz auf. An den Folgen arbeiten die IT-Experten des Landes mithilfe externer Experten nunmehr seit mehr als zwei Wochen praktisch rund um die Uhr. Mehrere zehntausend Personendaten waren bei dem Cyberangriff zumindest eingesehen worden: 80.000 Stammdatenblätter von Niederlassungs- und Aufenthaltsbewilligungen seit 1999, 4.000 Kontaktdaten des Veranstaltungsmanagements und knapp 200 Gigabyte Daten aus internem Schriftverkehr von Regierungsmitgliedern und Mitarbeitern.



Das Land hat noch immer mit den Folgen des Angriffs zu kämpfen.

Foto: APA/GERT EGGENBERGER

Kärntens Landeshauptmann Peter Kaiser (SPÖ, Zweiter von links) informierte vor rund einer Woche mit IT-Experten über den Angriff

Security News

TR Ma Sa

Decemb

TRITON as TROJ malwar industri was inv plant's op the Middle harm was question a down. How

chael Niavarani, der daraufhin auf Face-

glocken oder ich habe einen katholischen

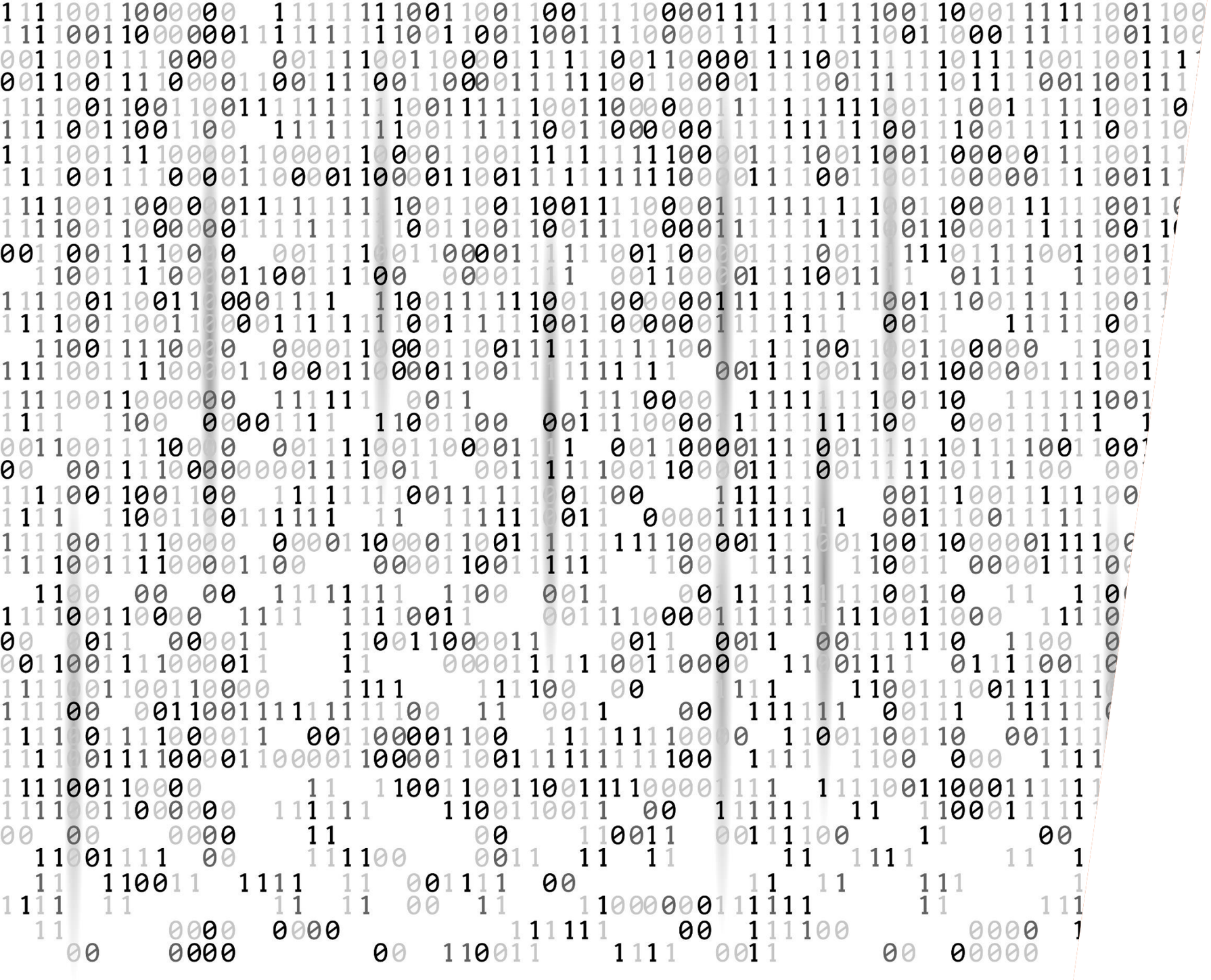
wn its ork and

Quelle: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/triton-wielding-its-trident-new-malware-tampering-with-industrial-safety-systems

JOANNEUM RESEARCH DIGITAL

Cyberattacken Fallbeispiele

- **SolarWinds**
  - Supply Chain Attacke: Angreifer fügten Malware in die Orion-Softwareupdate-Plattform des Anbieters ein. Ab März 2019 waren 18.000 Kunden bedroht und etwa 100 Unternehmen in den Vereinigten Staaten und die Netzwerke von neun Bundesbehörden kompromittiert.
- **A1 Telekom**
  - von November 2019 bis Mai 2020
- **EasyJet** (2020)
  - 9 Million Kunden betroffen, 2208 Kunden verzeichneten Kredit- oder Bankomat-kartenzugriffe.
- **REvil** verlangte $50 Millioen Lösegeld:
  - Im April 2021 traf die russische Ransomware-as-a-service gang REvil den Apple Zulieferer Quanta mit einer $50 Million Ransomware-Attacke.
- **Colonial Pipeline**
  - Im Mai 2021griff die kriminelle Gruppe DarkSide das IT System von Colonial Pipeline an. Die Folge war ein tagelanges Zusammenbrechen der Treibstoffversorgung an der US Ostküste. Colonial Pipeline bezahlte $4,4 Million Lösegeld.
- **Kaseya**
  - Kurz nachdem $11 Million vom Fleischverarbeter JBS durch eine Ransomeware-Attacke erpresst worden waren, forderte REvil $70 Million von Kaseya, was die höchste Lösegeldforderung bisher darstellt.



JOANNEUM RESEARCH DIGITAL

Cyberangriffe auf die Wasserversorgung

Cyberangriffe – Das Schlachtfeld

- **Digitalisierung**
  - Klassische **Cybersicherheitslösungen** werden zunehmend **ausgehebelt**
  - Antreiber: Beschleunigte **Digitalisierung**
- **Der Fokus verschiebt sich**
  - **IT-Netzwerk:** Intrusion detection (**war einmal…**)
  - Die Cybersecurity Front bewegt sich nun in Richtung **kritischer Infrastruktur**
  - Große Zahl von Menschen und Industrien sind betroffen: **Energiesystem, Wasserversorgung, Kommunikation, Transport, Gesundheitswesen,** usw.

Digitalisierung der Wasserversorgung

- Übergang von traditionell physischer Infrastruktur zu einem **cyber-physischen System (CPS)**
- CPS integrieren physikalische Prozesse, Computerrechenleistung und Netzwerktechnik, um den Betrieb des Systems zu überwachen und zu steuern
- **Physische Anlagen** (Leitungen, Pumpen, Ventile) werden **vernetzt** und mittels **IoT Geräte** gesteuert; sie werden Teil sog. **Industrial Control Systems (ICS)**
- Diese Entwicklung ist zwangsläufig mit der Schaffung **neuer Schwachstellen** und der **Vergrößerung der Angriffsfläche** verbunden, was die Sicherheit (Safety and Security) solcher Systeme **neuen und erst entstehenden Bedrohungen** aussetzt

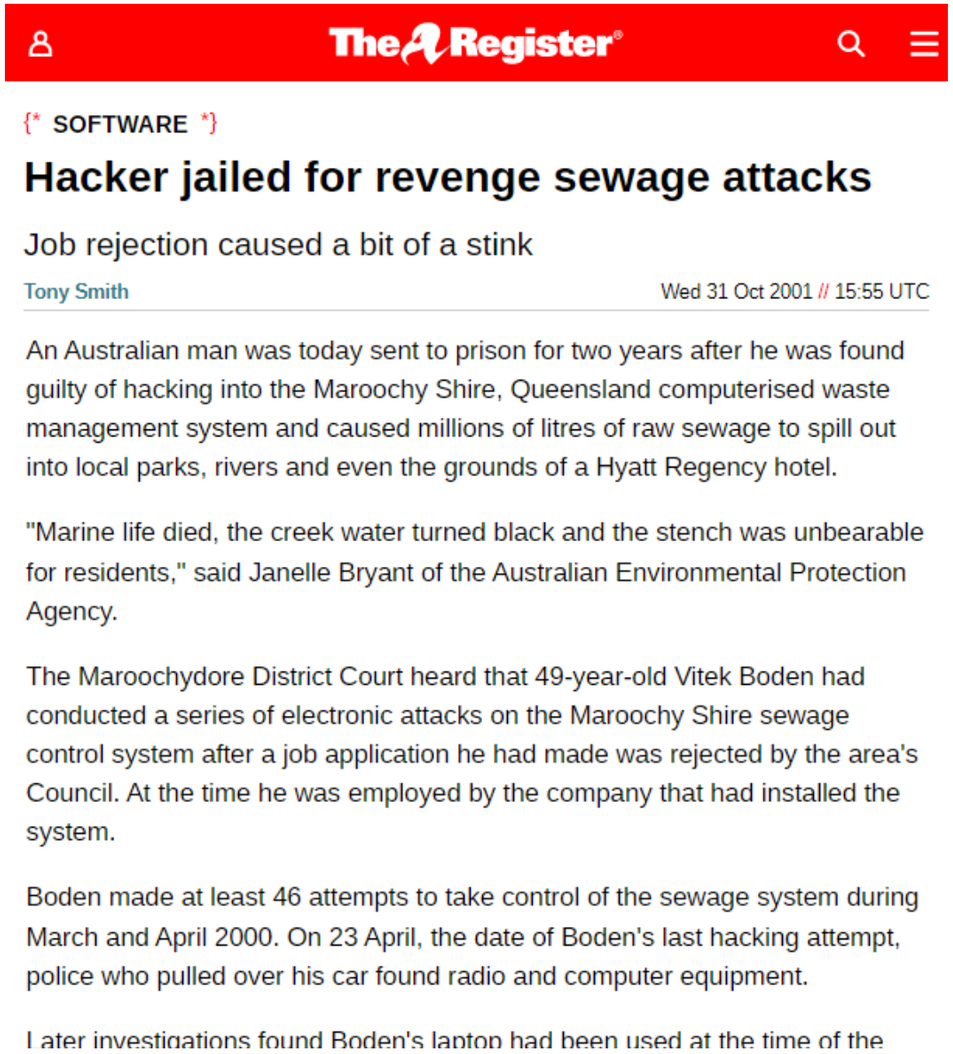
(In)Famous cyber attacks on water treatment facilities

- Cyber attacks on water → a weapon of destabilization between countries, public health...
- Evident increase in the cyber-attack attempts targeting water distribution systems
- Still concentrated on the limited number of geo locations (USA, Australia, Israel), but…
- 2021 → a reported attack on water treatment infrastructure in Norway

Source: https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water/

Attack #1 (2000): A wastewater treatment plant in the Shire of Maroochy, Australia

- **When**: March and April 2000
- **Where**: Maroochy sewage treatment plant in Australia
- **Who**: Former technical contractor
- **Why**: His application for employment was rejected



The Register®

{* SOFTWARE *}

Hacker jailed for revenge sewage attacks

Job rejection caused a bit of a stink

Tony Smith — Wed 31 Oct 2001 // 15:55 UTC

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hyatt Regency hotel.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency.

The Maroochydore District Court heard that 49-year-old Vitek Boden had conducted a series of electronic attacks on the Maroochy Shire sewage control system after a job application he had made was rejected by the area's Council. At the time he was employed by the company that had installed the system.

Boden made at least 46 attempts to take control of the sewage system during March and April 2000. On 23 April, the date of Boden's last hacking attempt, police who pulled over his car found radio and computer equipment.

Later investigations found Boden's laptop had been used at the time of the

Source: https://www.theregister.com/2001/10/31/hacker_jailed_for_revenge_sewage/

Attack #1 (2000): A wastewater treatment plant in the Shire of Maroochy, Australia

- **Objectives/Goal**: Cause damage
- **How**:
  - Attacker hijacked the activity of several pumps by sending spurious commands
  - One of the pumps stopped working, causing wastewater to be discharged into the seabed
  - Allegedly had 46 attempts to hack the factory's information systems, without ever being detected
- **Damage**: poisoning local flora and fauna, and creating foul odors in the surrounding area...

Attack #2 (2007): A canal system in California (USA)

- **When**: August 2007
- **Where**: California canal system (TCAA, Tehama Colusa Canal Authority in Willows)
- **Who**: Former employee
- **Why**: Not clear

COMPUTERWORLD UNITED STATES

NEWS

Insider charged with hacking California canal system

Ex-supervisor installed unauthorized software on SCADA system, indictment says

By Robert McMillan

IDG News Service | NOV 29, 2007 12:00 AM PST

SAN FRANCISCO -- A former employee of a small California canal system has been charged with installing unauthorized software and damaging the computer used to divert water from the Sacramento River.

Michael Keehn, 61, former electrical supervisor at the Tehama Colusa Canal Authority (TCAA) in Willows, Calif., faces 10 years in prison on charges that he "intentionally caused damage without authorization to a protected computer," according to Keehn's Nov. 15 indictment. He did this by installing unauthorized software on the TCAA's Supervisory Control and Data Acquisition (SCADA) system, the indictment states.

Source: https://www.computerworld.com/article/2540235/insider-charged-with-hacking-california-canal-system.html

Attack #2 (2007): A canal system in California (USA)

- **Objectives/Goal**: “the attacker intentionally caused damage without authorization to a protected computer"
- **How**:
  - Installing unauthorized software on a computer used to divert water from the Sacramento River for irrigation purposes
  - An installation damaged the computer, part of the SCADA system
- **Damage**: the intrusion cost the TCAA more than $5,000 in damages

Attack #3 (2013): A drinking water plant in Georgia (USA)

- **When**: April 2013
- **Where**: The drinking water facility of a small town in North Georgia
- **Who**: Not clear, but according to management former employees could still have keys or passes they did not know about...
- **Why**: Not clear

Source: https://www.stormshield.com/news/twenty-years-of-cyber-attacks-on-the-world-of-water/#undefined

Attack #3 (2013): A drinking water plant in Georgia (USA)

- **Objectives/Goal**: cause damage
- **How**:
  - No doors or windows were broken into, the attackers are thought to have got into the station over the barbed wire before gaining access to the monitoring system
  - They changed the fluorine and chlorine settings
- **Damage**: the management company had to advise the 400 residents not to use the tap water for a few days

***Attack #4 (2016)*: A public provider in Michigan (USA)**

- **When**: April 2016
- **Where**: Lansing Board of Water & Light (BWL) – Michigan utility provider
- **Who**: Not clear
- **Why**: Money extortion

Newsletters Webinars Events Magazine Papers

government technology

Special: Remote Work AI Cloud Cybersecurity Digital Education HHS Local Network

CYBERSECURITY

Ransomware Attack on Michigan Utility Provider Highlights Organizational Vulnerabilities

On April 25, an attack launched against the Lansing Board of Water and Light proved just how vulnerable organizations can be to this ballooning threat vector.

May 04, 2016 • Eyragon Eidam

If you've been anywhere near a social media newsfeed in the last couple of years, then you've likely seen the horror stories about ransomware attacks. What looks like an attachment sent by a friend infects your computer or network and sends you on a hellish misadventure to recover files taken hostage.

For the most part, these stories have circulated through the networks of pedestrian Internet users, but have exploded into the national spotlight as hospitals and other organizations fall prey to them.

Source: https://www.govtech.com/security/ransomware-attack-on-michigan-utility-provider-highlights-organizational-vulnerabilities.html

Attack #4 (2016): A public provider in Michigan (USA)

- **Objectives/Goal**: Money extortion by locking down supporting systems
- **How**:
  - An employee allegedly clicked on a malicious email attachment
  - The attack did not affect the water and electricity distribution systems, but the ransomware made some of BWL's operations unavailable, including phone lines and customer service
- **Damage**: The directors then chose to pay the ransom demanded by the cyber criminals in order to resume normal business operations

Attack #5 (2018): A distribution company in North Carolina (USA) – hacked twice

- **When**: October 2018
- **Where**: Onslow Water and Sewer Authority (ONWASA), located in Jacksonville, North Carolina
- **Who**: ONWASA said "cyber criminals" had carried out the attack, "who may be based in a foreign country."
- **Why**: Money extortion

ONWASA

MEDIA RELEASE

FOR RELEASE: Monday, October 15, 2018, 7:30am
CONTACT: Jeffrey Hudson, CEO
910-455-0722 (*CURRENTLY ONLY METHOD*)

CYBER-CRIMINALS TARGET CRITICAL UTILITY IN HURRICANE-RAVAGED AREA

In the wake of the Hurricane Florence disaster, ONWASA, a critical water utility has been specifically targeted by cyber-criminals. ONWASA's internal computer system, including servers and personal computers have been subjected to a sophisticated ransomware attack that has left the utility with limited computer capabilities. Customer information was not compromised in the attack. However, many other databases must be recreated in their entirety. The utility is coordinating with the Federal Bureau of Investigation, the Department of Homeland Security, the State of North Carolina, and a several technology security companies.

The safety of the public's water supply and the area's environment is not in danger. The crisis is technological in nature.

On October 4th ONWASA began e
malware. The virus was initially th
specialists. The specialist continue
have been a timed event, the malv
October 13th.

An ONWASA IT staff member was
resources by disconnecting ONWA
databases and files. The attack is
North Carolina. Information on
news/north-carolina-officials-refus

ONWASA had multiple layers of co
defenses of the computer systems
criminals, who may be based in a fo
and corporations. Ransom monie
Furthermore, there is no expectatio
with criminals nor bow to their de
painstaking process of rebuilding it

SUBSCRIBE CYBERSCOOP

TECHNOLOGY

Ransomware hits computer networks of North Carolina water utility

(Getty)

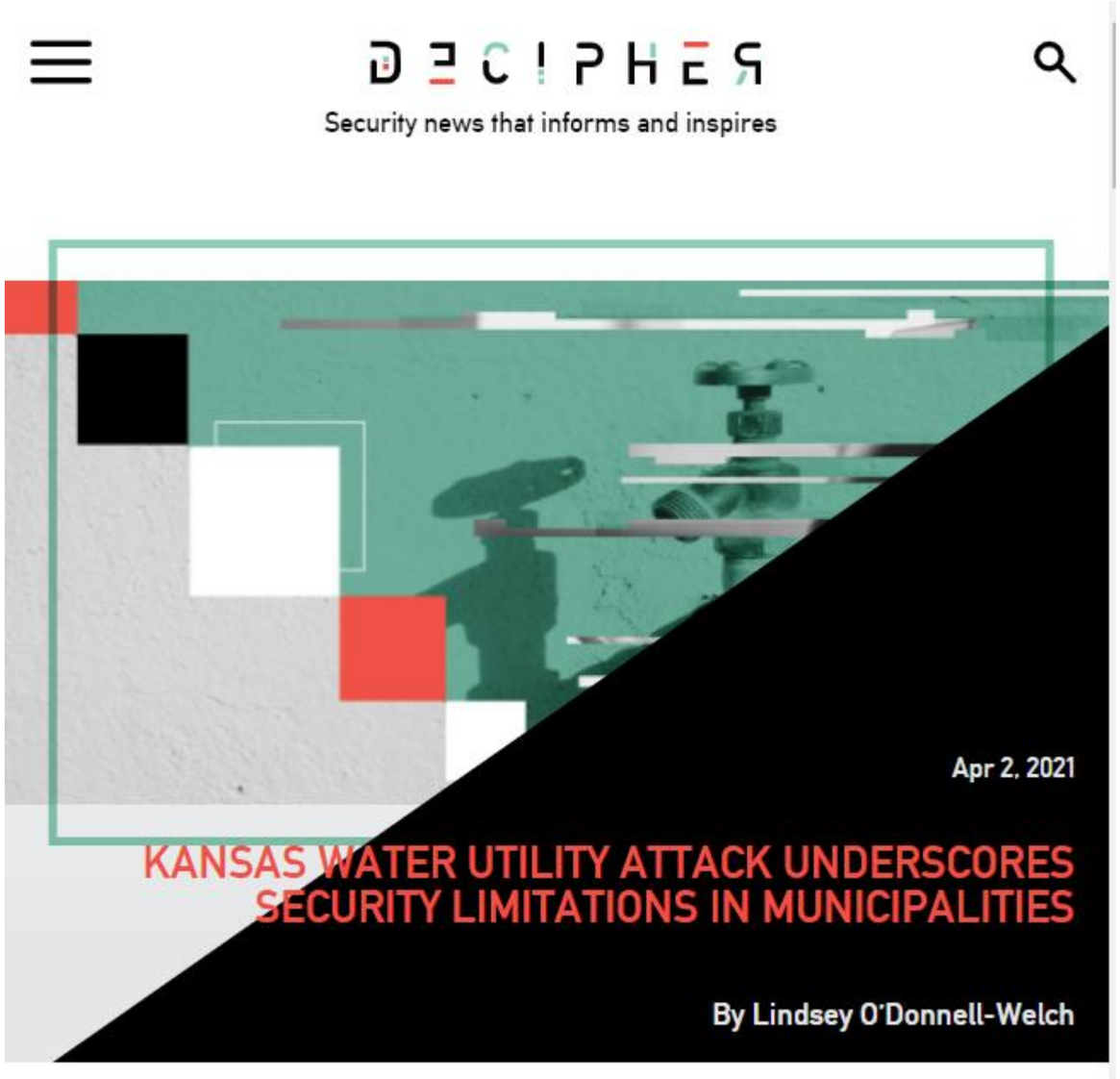
Source: https://www.onwasa.com/DocumentCenter/View/3701/Scan-from-2018-10-15-08_08_13-A
https://www.cyberscoop.com/ransomware-hits-onwasa-computer-network-north-carolina-water-utility/

Attack #5 (2018)*: A distribution company in North Carolina (USA) – *hacked twice

- **Objectives/Goal**: Money extortion by locking down supporting systems
- **How**:
  - On 3 October, the Emotet ransomware was reported to have spread through the company's information systems, followed by the Ryuk ransomware around ten days later
  - The attack has left the utility operating with limited computer capabilities, with workers setting up accounts and fulfilling service orders manually
  - Allegedly customer information wasn't compromised, and the incident did not affect the safety of the water supply
- **Damage**: ONWASA vowed not to pay any ransom and to instead "undertake the painstaking process of rebuilding its databases and computer systems from the ground up."

Attack #6 (2019): A distribution company in Kansas (USA)

- **When**: March 2019
- **Where**: Public water utility in Ellsworth County, Kansas
- **Who**: Former employee
- **Why**: Damage



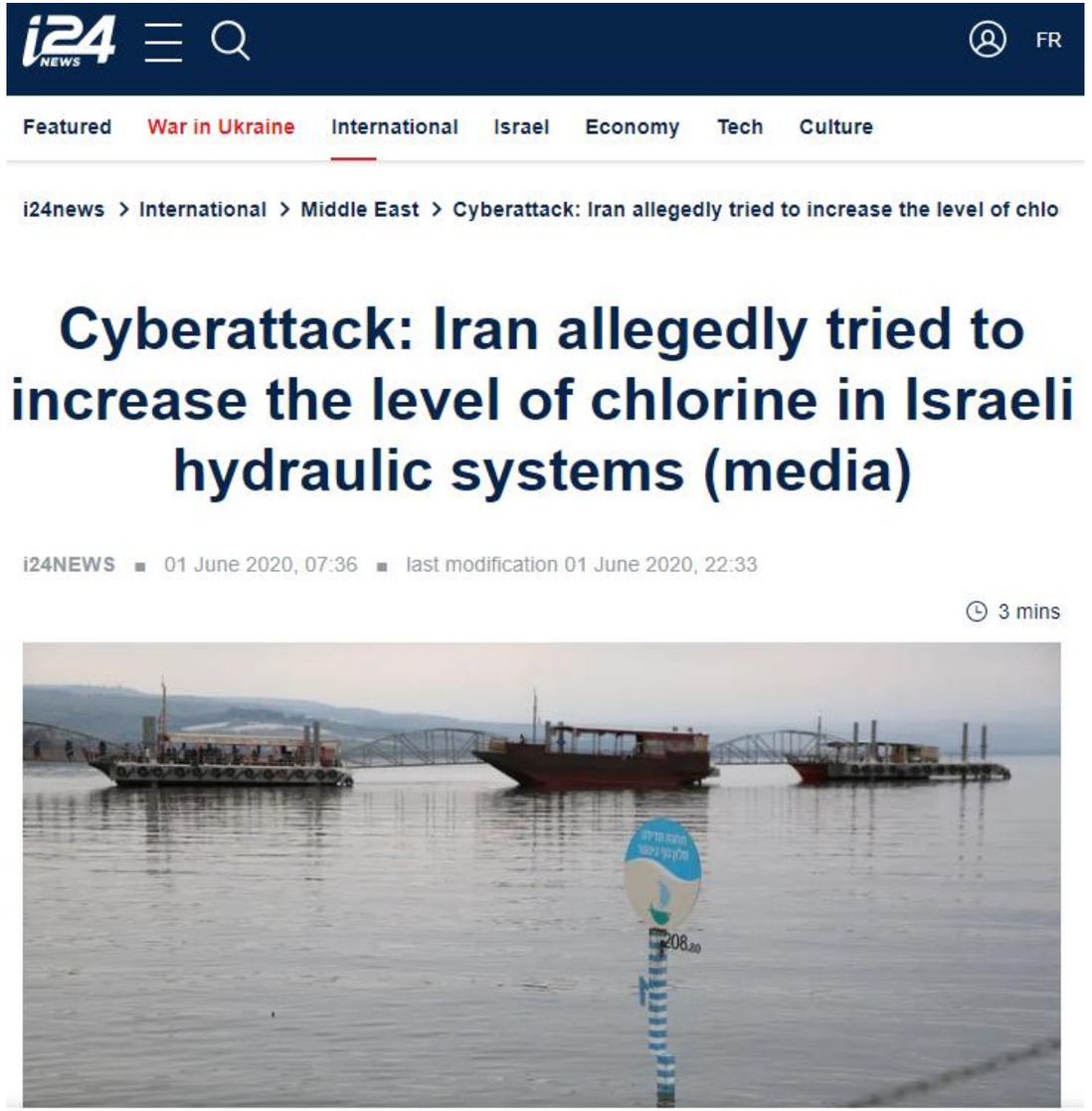
Source: https://duo.com/decipher/kansas-water-utility-attack-underscores-security-limitations-in-municipalities

Attack #6 (2019): A distribution company in Kansas (USA)

- **Objectives/Goal**: Damage by tempering with water disinfectant levels
- **How**:
  - The perpetrator allegedly took control of the company's information systems remotely to shut down the processes behind the facility's cleaning and disinfecting procedures
  - The former employee had previously worked on the factory's monitoring systems and his access had not been revoked when he left the company
- **Damage**: A representative with the Ellsworth County Rural Water District said the incident did not have an impact on customers

Attack #7 (2020): Pumping stations and treatment facilities (Israel)

- **When**: April 2020
- **Where**: Several pumping stations and wastewater treatment facilities in Israel
- **Who**: Cyber criminals suspected of being affiliated with the Iranian regime
- **Why**: Damage



Source: https://www.i24news.tv/fr/actu/international/moyen-orient/1590989473-cyberattaque-l-iran-aurait-tente-d-augmenter-le-niveau-de-chlore-dans-les-systemes-israeliens-d-approvisionnement-en-eau-media

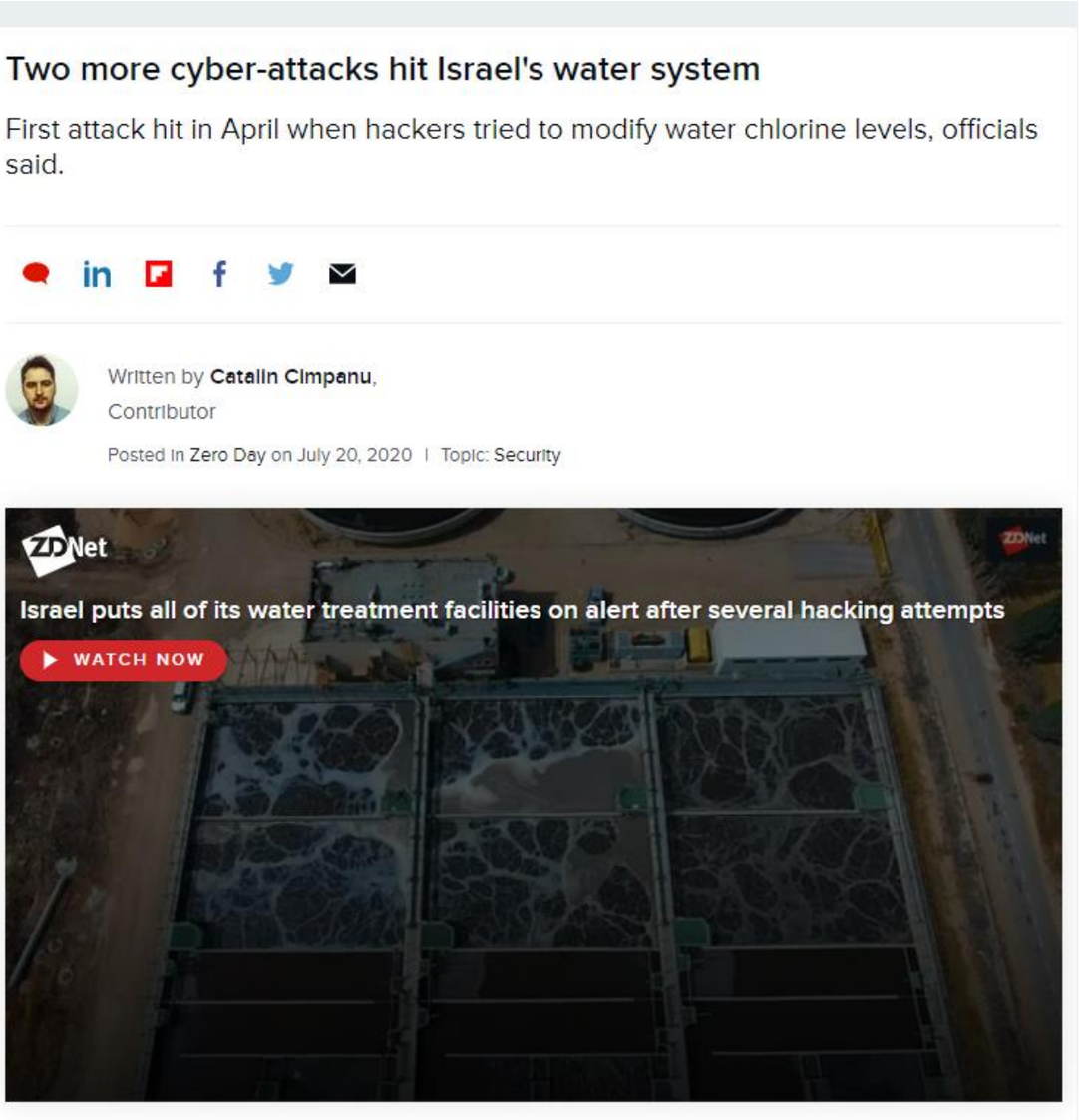
Attack #7 (2020): Pumping stations and treatment facilities (Israel)

- **Objectives/Goal**: Damage by tempering with water disinfectant levels
- **How**:
  - The attackers attempted to increase the level of chlorine in some of the water supply systems that supply part of the Israeli population
  - "This is a complex attack that was close to succeeding, and it is unclear how and why it failed," according to officials
- **Damage**: The government is reported to have quickly countered, prompting all the water and energy infrastructures in the country to change the passwords to all their SCADA systems

“In the worst-case scenario, hundreds of civilians could have fallen ill”

Attack #8 (2020)*: Water pumps (Israel) - *two attacks

- **When**: June 2020
- **Where**: Agricultural water pumps in the Galilee region and a water supply system in the province of Mateh Yehuda
- **Who**: Not clear…
- **Why**: Damage



Two more cyber-attacks hit Israel's water system

First attack hit in April when hackers tried to modify water chlorine levels, officials said.

Written by **Catalin Cimpanu**, Contributor

Posted in Zero Day on July 20, 2020 | Topic: Security

Source: https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

Attack #8 (2020): Water pumps (Israel) - two attacks

- **Objectives/Goal**: Damage by tempering with water disinfectant levels
- **How**:
  - Details of the attack were not released, but it is believed that, once again, the cyber criminals attempted to alter the quality of the water by changing the chlorine levels
- **Damage**: Officials said the attacks didn't cause any damage to the attacked organizations

“The attack on Israel's water utility seems, however, to have been an important moment between the two countries, as it also marked the start of a series of **mysterious accidents and explosions** detected across Iran's critical infrastructure -- such as **petrochemical plants, nuclear fuel enrichment centers, power plants, ports, and more**.”

Attack #9 (2020): A recycled water reservoir (Israel)

- **When**: December 2020
- **Where**: Israeli reclaimed water reservoir
- **Who**: Iranian threat-actor, named “Unidentified TEAM”
- **Why**: Damage

OTORIO

What We’ve Learned from the Dec 1st Attack on an Israeli Water Reservoir?

03 Dec 2020

What Happened?

On the night of December 1st, 2020, an Iranian threat-actor published a video of a breach in an Israeli reclaimed water reservoir HMI system.

Source: https://www.otorio.com/blog/what-we-ve-learned-from-the-december-1st-attack-on-an-israeli-water-reservoir/

Attack #9 (2020): A recycled water reservoir (Israel)

- **Objectives/Goal**: Damage
- **How**:
  - According to the cyber criminals, the HMI (Human Machine Interface) system could be accessed from the Internet without any authentication required
  - Allowing any malicious individual to take control of certain parameters such as the temperature or pressure of the water
- **Damage**: Reputation damage, further damage not known

2020 – "*Annus horribilis* in Israel"

Attack #10 (2021): Wastewater treatment plants in San Francisco (USA)

- **When**: January 2021
- **Where**: Local water treatment facility, San Francisco Bay area of California
- **Who**: Not known
- **Why**: Not known

Source: https://www.nbcnews.com/tech/security/hacker-tried-poison-calif-water-supply-was-easy-entering-password

Attack #10 (2021): Wastewater treatment plants in San Francisco (USA)

- **Objectives/Goal**: Damage
- **How**:
  - An attacker reportedly took control of a local water treatment facility and deleted computer programs involved in the treatment of drinking water
  - Initial indications are that the cyber criminal hacked into the plant's systems using the credentials of former employees, which were used to connect to the TeamViewer remote control software
  - The hack wasn't discovered until the following day, and the facility changed its passwords and reinstalled the programs
- **Damage**: "No failures were reported as a result of this incident, and no individuals in the city reported illness from water-related failures"

Attack #11 (2021): Wastewater treatment plant in Florida (USA)

- **When**: February 2021
- **Where**: Local water treatment facility, in the town of Oldsmar, Florida
- **Who**: Not known
- **Why**: Not known

BLOG

Florida Water Treatment Plant Hit With Cyber Attack

Steve Kardon February 9, 2021

On Friday, February 5, 2021, a hacker initiated an attack on an Oldsmar, Florida water treatment facility which briefly adjusted the levels of sodium hydroxide from 100 parts per million to 11,100 parts per million. This attack occurred about 15 miles from the location of, and two days before the Super Bowl. If successful, the attack would have increased the amount of sodium hydroxide to an incredibly

Source: https://www.industrialdefender.com/florida-water-treatment-plant-cyber-attack/

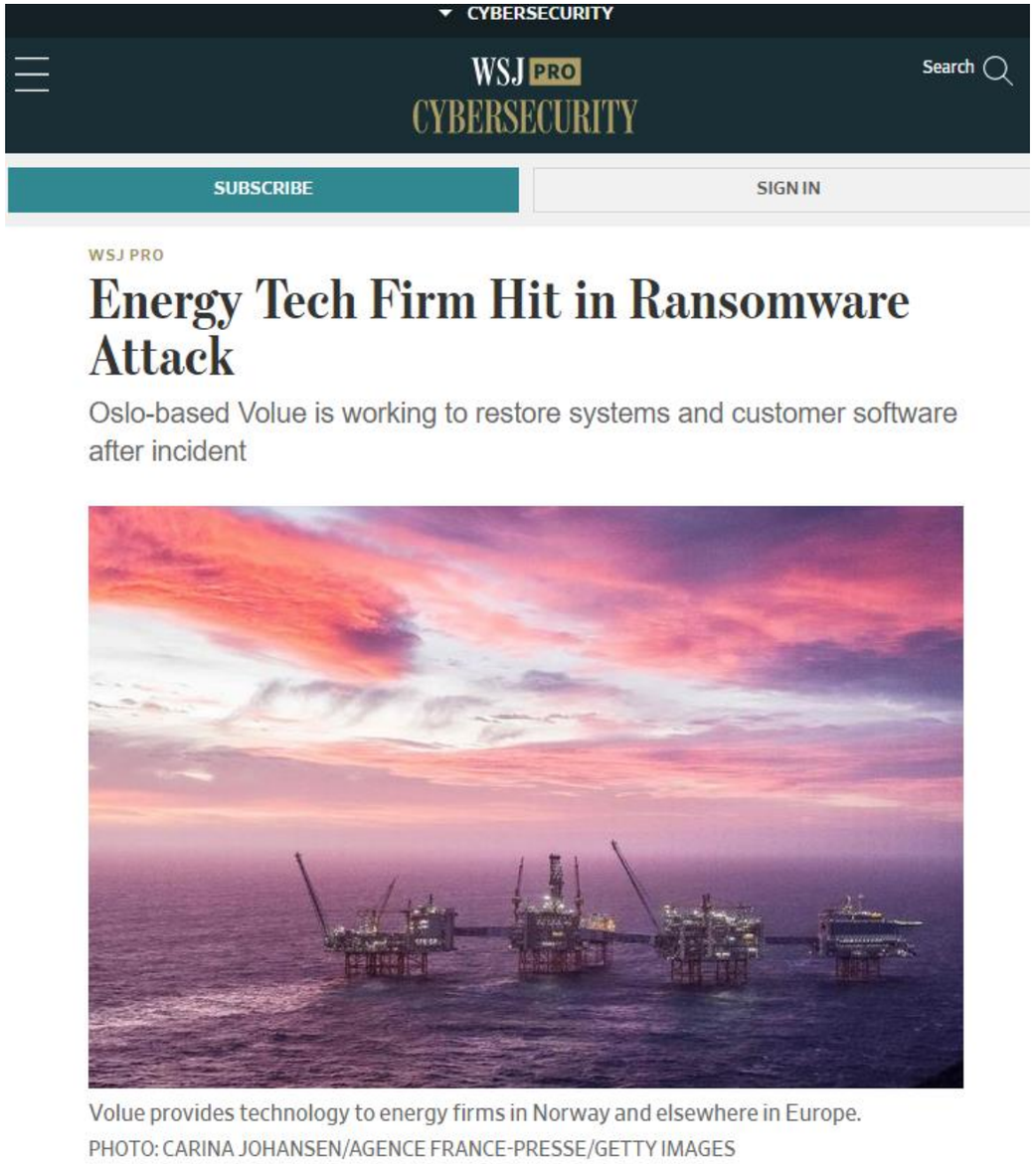
Attack #11 (2021): Wastewater treatment plant in Florida (USA)

- **Objectives/Goal**: Damage
- **How**:
  - The attackers reportedly collected TeamViewer login credentials shared by several employees, and then exploited flaws present within a Windows 7 operating system
  - This intrusion would have allowed the cyber criminals to significantly increase the level of sodium hydroxide making the drinking water **extremely toxic**
- **Damage**: Luckily, facility staff were able to quickly get the situation under control and save some 15,000 Oldsmar residents from being poisoned

There's an old saying in the American West: ***"Whiskey is for drinking; water is for fighting."***

Attack #12 (2021): Water treatment infrastructure (Norway)

- **When**: May 2021
- **Where**: Norwegian company that equips several water treatment facilities with applications and software
- **Who**: Not known
- **Why**: Not known



CYBERSECURITY

WSJ PRO CYBERSECURITY

Search

SUBSCRIBE SIGN IN

WSJ PRO

Energy Tech Firm Hit in Ransomware Attack

Oslo-based Volue is working to restore systems and customer software after incident

Volue provides technology to energy firms in Norway and elsewhere in Europe.

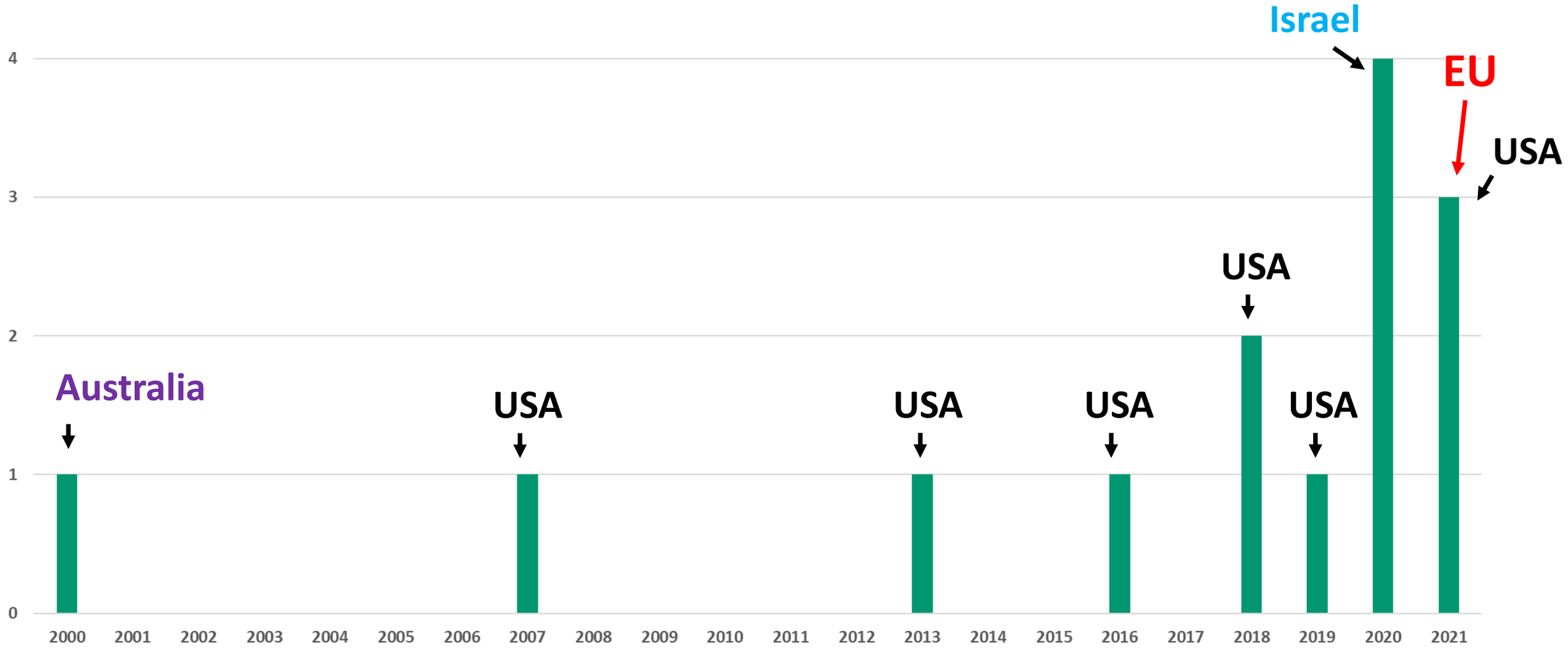
PHOTO: CARINA JOHANSEN/AGENCE FRANCE-PRESSE/GETTY IMAGES

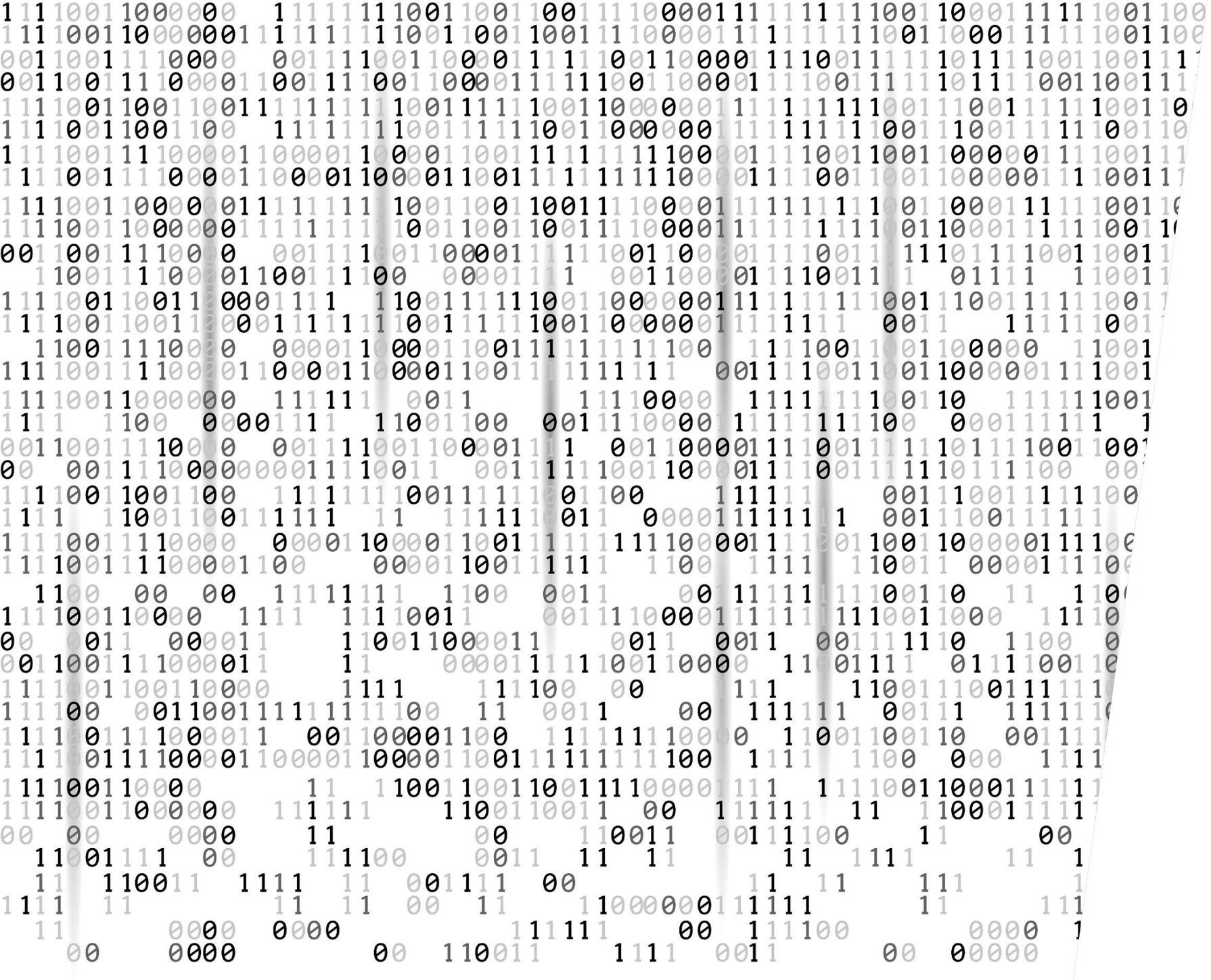
Source: https://www.wsj.com/articles/energy-tech-firm-hit-in-ransomware-attack-11620764034

Attack #12 (2021): Water treatment infrastructure (Norway)

- **Objectives/Goal**: Money extortion
- **How**:
  - Have fallen victim to the Ryuk ransomware
  - The ransomware spread to the information systems of **200 public water suppliers** in the country, Volue's customers.
  - Several customer front-end platforms were reportedly impacted and the company quickly put in place means to isolate and then restore the infected systems, thereby limiting the impact on its customers
- **Damage**: Not known

Timeline of attacks





JOANNEUM RESEARCH DIGITAL

Wissenschaftliche Projekte im Bereich Wasserversorgung

Forschungsthemen

- Leckagekennung
- Smart metering
- Digitalisierung
- Nachhaltigkeit / Kreislaufwirtschaft
- Cybersecurity

Leckage Vorbeugung / Erkennung

- SWAMP – Smart Water Management Platform, H2020 (2017-2020)
  - IoT based methods and approaches for smart water management in precision irrigation domain
  - Pilots - **Italy**, **Spain**, and **Brazil**
  - Automation, drones, IoT, Big Data,Cloud/Fog, …
- SMARTWATER4EUROPE, FP7 (2014-2017)
  - Demonstration of integrated smart water supply solutions at 4 sites across Europe
  - Demo sites - Vitens, Acciona,Thames Water and Lille University
  - Leak detection, water quality management, energy optimization, customers interaction

Smart metering

- SMART.MET, H2020 (2017-2022)
  - Drive the development of new technologies to deal with the collection and management of smart metering data, through a joint Pre-Commercial Procurement (PCP)
  - Led by a group of 7 water utilities: Viveraqua (Verona, IT), Promedio (Badaroz SP), Eau de Paris (Paris FR), SDEA (Bas-Rhin FR), CILE (Liege BE), Vizmuvek (Budapest HU), Hydrobru (Brussels Vivaqua BE)

Digitalisierung

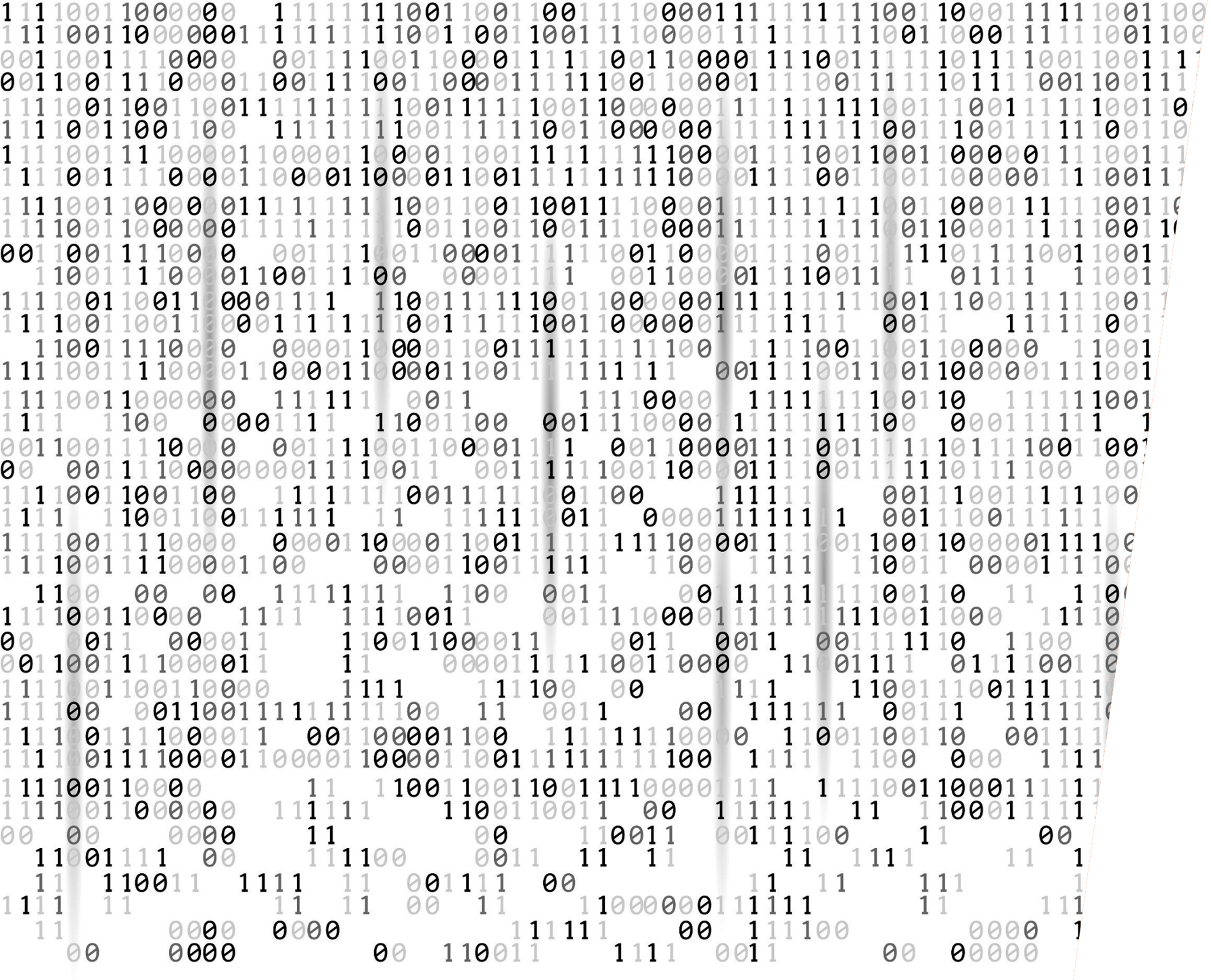
- NAIADES, H2020 (2019-2022)
  - Smart Water Management for the Sustainable Development Goals
  - Supports the modernization and digitization of the water sector by providing a holistic solution for the control and management of water ecosystems
  - Takes into consideration issues pertaining to **cost**, **safety**, **complexity**, **vulnerability**, **societal acceptance**, **user behaviour** and **ethics**
  - Pilots: Ville de Carouge (**Switzerland**), Alicante (**Spain**), Brăila (**Romania**)
- AQUA3S, H2020 (2019-2022)
  - Create strategies and methods enabling water facilities to easily integrate solutions regarding water safety and security
  - Detect and tackle water-related crises
  - Sensor networks supported by UAVs, satellite images, social media observations
  - Pilots: **Italy**, **France**, **Belgium**, **Cyprus**, **Greece**, **Bulgaria**

Nachhaltigkeit / Kreislaufwirtschaft

- WATER-MINING, H2020 (2020-2024)
  - Next generation water-smart management systems: large scale demonstrations for a circular economy and society
  - Mining water & resources from desalination brines, urban & industrial wastewater streams
- B-WaterSmart, H2020 (2020-2024)
  - Accelerating Water Smartness in Coastal Europe
  - Demo sites – Alicante (**Spain**), Bodo (**Norway**), East Frisia (**Germany**), Flanders (**Belgium**), Lisbon (**Portugal**), Venice (**Italy**)
- Project-O, H2020 (2018-2022)
  - Developing practical tools for a circular water economy
  - Pilots: **Italy**, **Israel**, **Spain**, **Croatia**

Cybersecurity

- STOP-IT, H2020 (2017-2021)
  - Strategic, Tactical, Operational Protection of water Infrastructure against cyber-physical Threats
  - Pilots: Aigües de Barcelona (ES), Berliner Wasserbetriebe (DE), MEKOROT (IL) and Oslo VAV (NO)
  - **mature technologies** improved via their combination and embedment (incl. public warning systems, smart locks) and
  - **novel technologies** whose TRL will be increased (incl. cyber threat incident services, secure wireless sensor communications modules, context-aware anomaly detection technologies; fault-tolerant control strategies for SCADA integrated sensors, high-volume real-time sensor data protection via blockchain schemes; authorization engines; irregular human detection using new computer vision methods and WiFi and efficient water contamination detection algorithms)
  - creation of a **European Water ISAC** (Information Sharing and Analysis Centre)



JOANNEUM RESEARCH DIGITAL

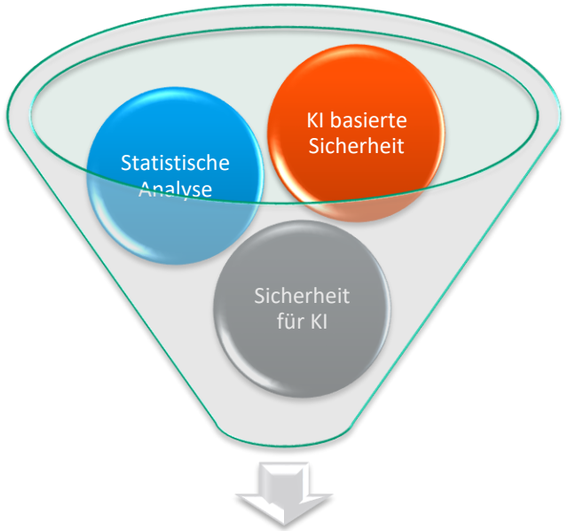
Cybersicherheit in der Wasserversorgung @JR-CSD

Cybersicherheit in der Wasserversorgung @JR-CSD

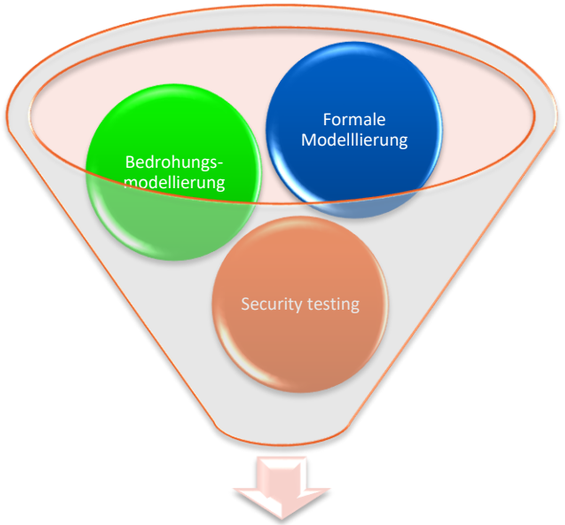
- EU Projekte
- National geförderte Projekte

SPARTA

CRITICAL CHAINS



AI@JR-CSD



SbD@JR-CSD

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

JOANNEUM RESEARCH DIGITAL

KI basierte Sicherheit

- Anwendungsgebiete:
  - Finanzbetrugserkennung
  - Erkennung von APT Attacken
  - Erkennung von gezielten Angriffen auf smarte Wasserversorgungs-systeme
  - Statistische Analyse

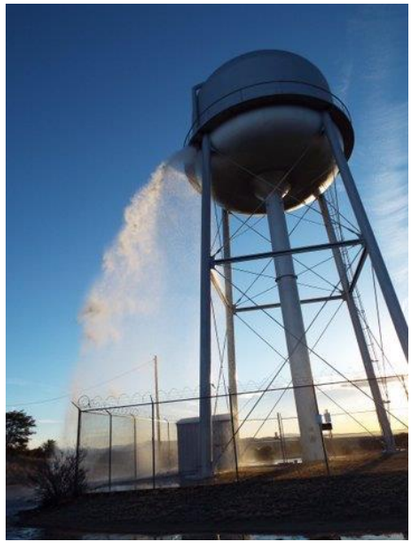
CRITICAL CHAINS

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

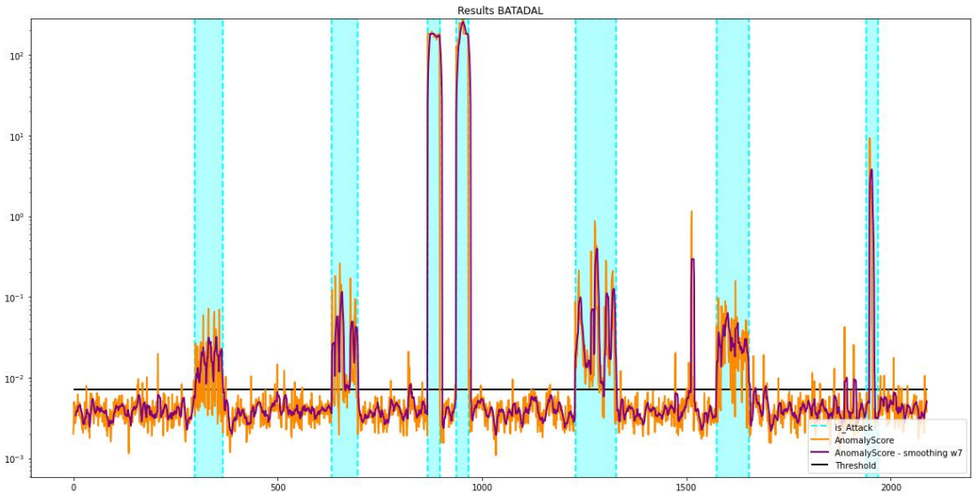
JOANNEUM RESEARCH DIGITAL

Smart water distribution system attack detection

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie



- **Cyber-Physical System**
- BATADAL (data from challenge)
  - Based on a real-world medium-sized network
  - SCADA reading (e.g. water level, pump status…)
- Data preparation
  - Time values are encoded as cyclic processes
    “Robust-Scaling” of the feature values
- Different anomaly detection methods tested
  - The normal AE produces by far the best results
  - We proposed and additional step – anomaly scores smoothing



JOANNEUM RESEARCH DIGITAL

Smart water distribution system attack detection

- Top performance for BATADAL dataset in comparison with other algorithms

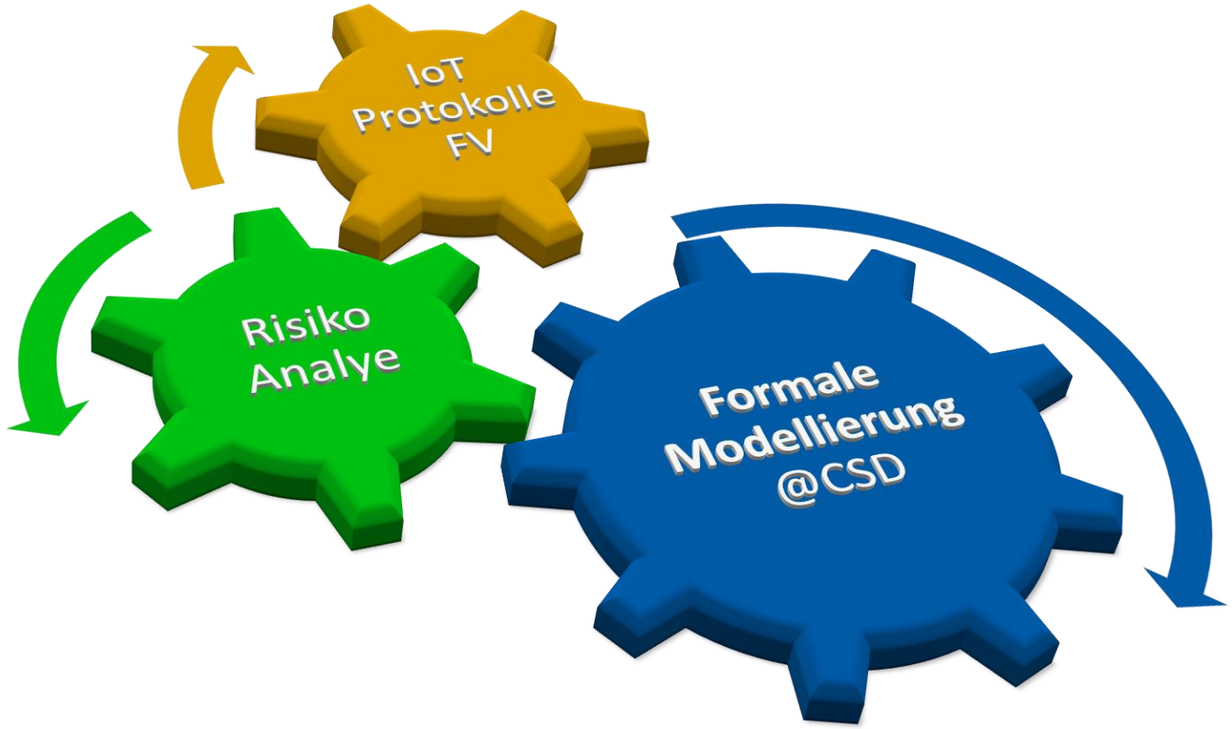
Table 1 A comparison of the algorithms on BATADAL dataset

Rank	Name	No. attacks	S	S_{TTD}	S_{CLF}	F_1	TPR	TNR	PPV	TP	FP	TN	FN
1	B1	7	0.9701	0.9650	0.9752	0.9700	0.9533	0.9970	0.9873	388	5	1677	19
2	QDA	7	0.9495	0.9584	0.9406	0.8981	0.9091	0.9721	0.8873	370	47	1635	37
3	B2	7	0.9491	0.9580	0.9402	0.8813	0.9214	0.9590	0.8446	375	69	1613	32
4	B3	7	0.9267	0.9360	0.9174	0.9057	0.8378	0.9970	0.9855	341	5	1677	66
5	MD	7	0.9165	0.9069	0.9260	0.8920	0.8722	0.9798	0.9126	355	34	1648	52
6	Ensemble	7	0.9142	0.8998	0.9286	0.8856	0.8845	0.9727	0.8867	360	46	1636	47
7	B4	6	0.8942	0.8570	0.9313	0.8894	0.8894	0.9732	0.8894	362	45	1637	45
8	LOF	7	0.8773	0.8567	0.8978	0.8560	0.8182	0.9774	0.8976	333	38	1644	74
9	SOD	7	0.8617	0.8350	0.8884	0.8120	0.8280	0.9489	0.7967	337	86	1596	70
10	B5	7	0.8015	0.8350	0.7679	0.5382	0.8575	0.6784	0.3921	349	541	1141	58
11	B6	7	0.7727	0.8850	0.6605	0.4829	0.3292	0.9917	0.9054	134	14	1668	273
12	Naive	7	0.7500	1.0000	0.5000	0.3261	1.0000	0.0000	0.1948	407	1682	0	0
13	OSVM	7	0.7143	0.6967	0.7319	0.6332	0.4644	0.9994	0.9947	189	1	1681	218
14	LDA	5	0.6787	0.6575	0.6999	0.5709	0.4005	0.9994	0.9939	163	1	1681	244
15	B7	3	0.5344	0.4290	0.6398	0.4220	0.3956	0.8841	0.4522	161	195	1487	246

AE + smoothing (JR)

Formale Modellierung

- Anwendungsgebiete:
  - **Formale Verifikation** von Smart Home IoT Protokollen
  - **Risiko / Resilienz Analyse** basierend auf probabilistische Modellprüfung
    - **Smart water** Angriffe – Wasser Kontamination und Wassertank-Überlauf
    - **Smart Grid** Blackout Attacke
    - **Smart Home** Attacke – HLK Attacke and Smartmeter Attacke
    - **FinTech** adversarial AI Attacken



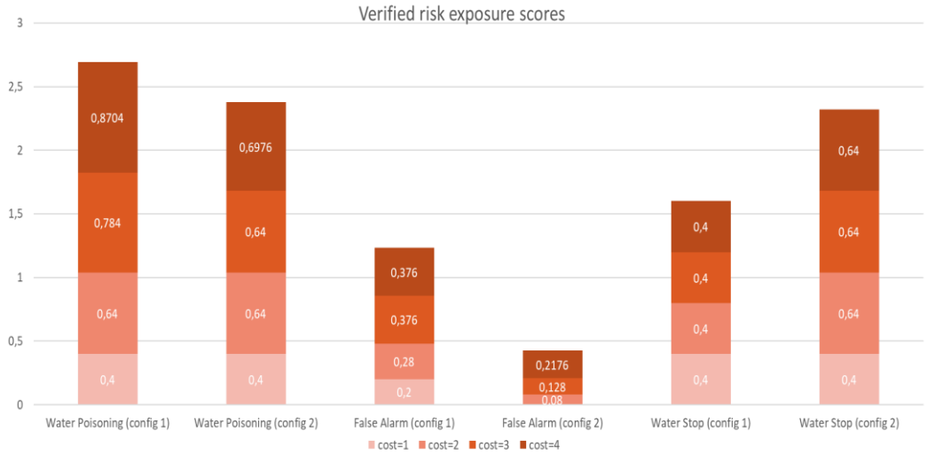
CRITICAL CHAINS

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

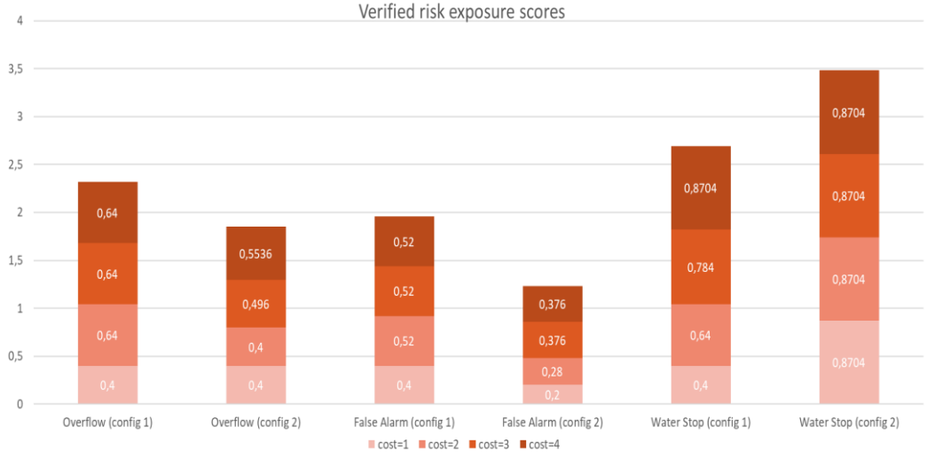
JOANNEUM RESEARCH DIGITAL

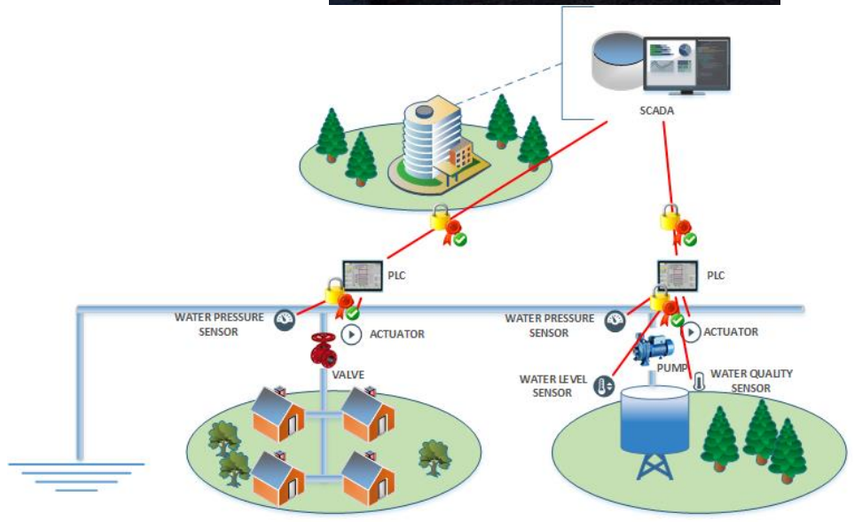
Risikoanalyse in der Smart Water IoT Umgebung

Wasser-Kontaminations-Szenario



Wasertank-Überlauf-Szenario





JOANNEUM RESEARCH DIGITAL

JOANNEUM RESEARCH DIGITAL

Lanzeitperspektive

Organisations

- EU Information Sharing Analysis Centers – ISACs
  - EU Water ISAC – under preparation in the project STOP-IT
  - USA Water ISAC

- Water Europe Technology and Innovation group
  - Almost 250 members
    - 8 multi national corporations, 101 RTOs, 21 Utilities, 86 Suppliers and SMEs, 5 Large Water Users, 6 Public Authorities, 19 Civil Society Organisations
  - Water Europe Vision 2030 - Multiple Waters for Multiple Purposes and Users

    "A future-proof European model for a water-smart society"

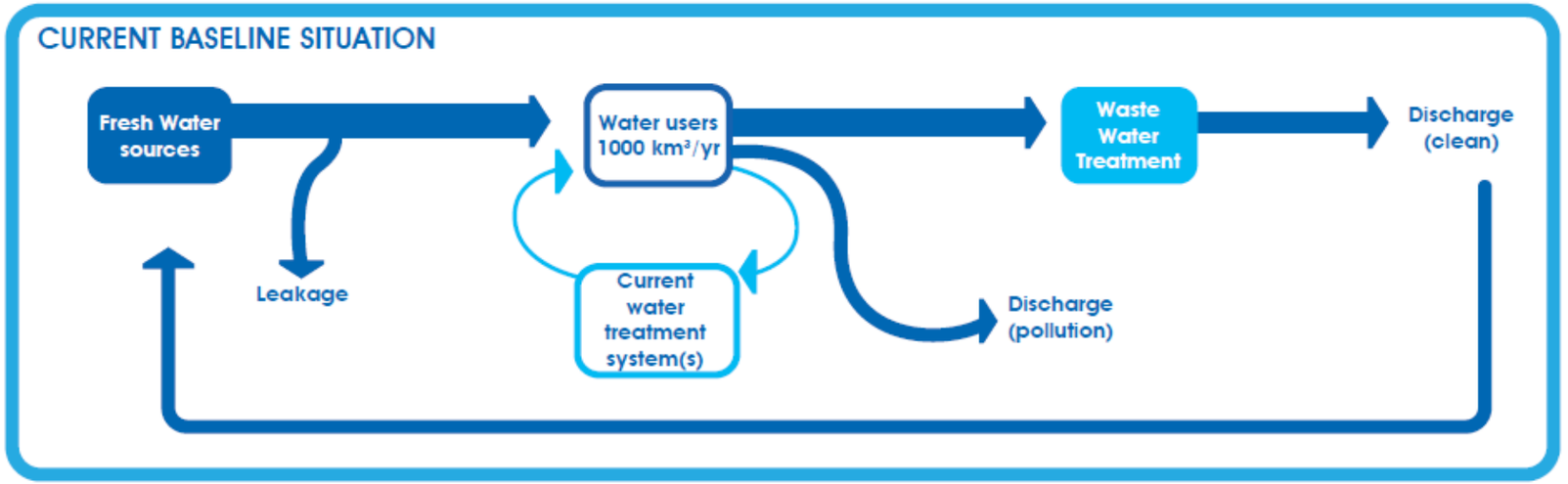
    "A paradigm shift towards a sustainable and circular water-smart society"

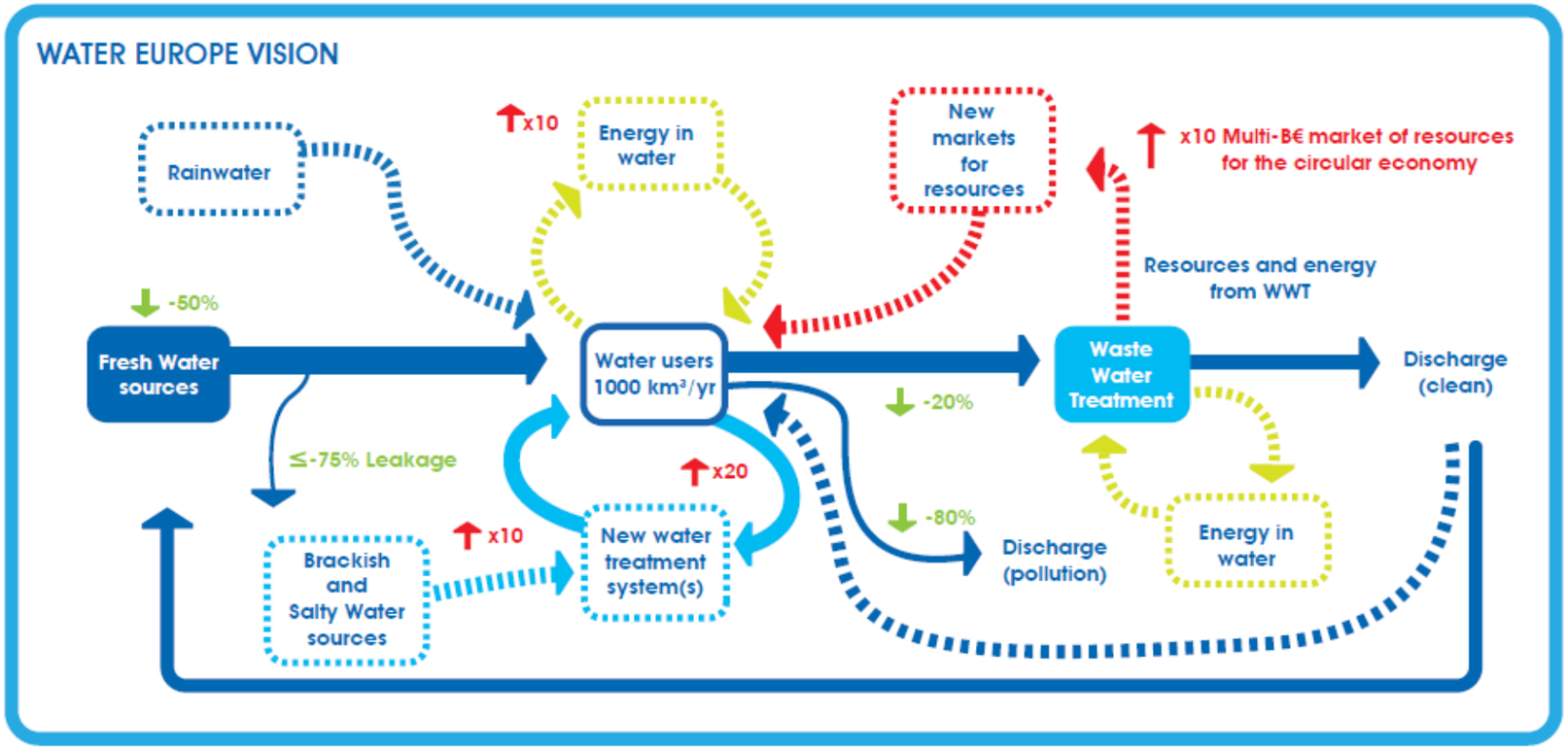
Water Europe
Technology & Innovation

JOANNEUM RESEARCH DIGITAL

Vision

- ***An opportunity for Europe: Increasing water resource efficiency and circularity***
- The key impact on resource efficiency and circularity in the water sector





Source: Water Europe

Teilnahme am Forschungsprozess - Fördermöglichkeiten

Unterstützung durch Sie

- Wissen über eingesetzte Technologien und Prozesse
- Reale Anwendungsfälle
- Reale Anforderungen
- Daten für Forschungszwecke
  - Privacy preserving
  - Zum Teil Daten aus Simulation

Nutzen für Sie

- Informationsgewinn über den Stand der Forschung
  - Threat intelligence sharing
  - Neue Angriffsmethoden und Abwehrmechanismen
  - Cyber-Risikoanalyse
- Enger Austausch zwischen Forschung und Betreiber bis zum Produkt
- Förderung

JOANNEUM RESEARCH DIGITAL

DI Christian Derler
JOANNEUM RESEARCH
Forschungsgesellschaft mbH

DIGITAL– Institut für Informations- und Kommunikationstechnologien

Steyrergasse 17, 8010 Graz
Tel. +43 664 602 876 1196
christian.derler@joanneum.at

www.joanneum.at/digital