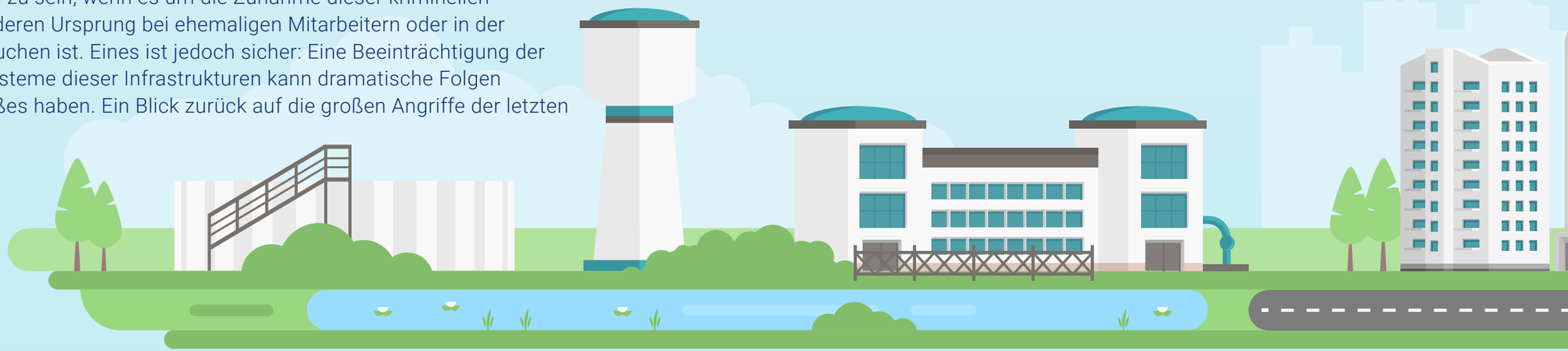
Die Cyberangriffe auf die Wasserwirtschaft in den letzten zwanzig Jahren

Als ebenso kritischer wie unverzichtbarer Sektor sah sich die Wasserwirtschaft in den letzten zwanzig Jahren mit zahlreichen Cyberbedrohungen konfrontiert. Eine Waffe zur Destabilisierung von Ländern, der öffentlichen Gesundheit ... Cyber-Kriminelle haben tausend Gründe für einen Angriff auf den Wassersektor. Und nicht alle Länder scheinen gleich zu sein, wenn es um die Zunahme dieser kriminellen Tendenz geht, deren Ursprung bei ehemaligen Mitarbeitern oder in der Geopolitik zu suchen ist. Eines ist jedoch sicher: Eine Beeinträchtigung der Informationssysteme dieser Infrastrukturen kann dramatische Folgen großen Ausmaßes haben. Ein Blick zurück auf die großen Angriffe der letzten Jahre.



2000
AUSTRALIEN

—Im März und April 2000 hat ein ehemaliger technischer Dienstleister der Kläranlage Maroochy in Australien die Kontrolle über die Systeme der Anlage in böswilliger Absicht übernommen. Nachdem seine Bewerbung um eine Anstellung abgelehnt worden war, soll er sich in das System gehackt und sich Zugriff auf mehrere Pumpen verschafft haben. Dann wäre eine der Pumpen ausgefallen, wodurch Abwasser zum Meeresgrund geleitet, die lokale Fauna und Flora vergiftet wurde und üble Gerüche sich in der Umgebung ausgebreitet haben ... Für diesen „Erfolg“ hätte es nicht weniger als 46 Versuche gebraucht, sich Zugriff auf die Informationssysteme der Anlage zu verschaffen, und dies, ohne jemals entdeckt worden zu sein. Ein Angriff, der die Anfälligkeit der Wasserwirtschaft angesichts von Cyberbedrohungen deutlich macht.

STORMSHIELD

2007
USA

— Im Sommer 2007 wurde ein ehemaliger Mitarbeiter einer kleinen kalifornischen Wasserbehörde (Tehama Colusa Canal Authority in Willows) wegen der Installation von nicht autorisierter Software auf einem Computer, der für die Umleitung von Wasser aus dem Sacramento River für Bewässerungszwecke eingesetzt wird, angeklagt. Durch diese Installation wurde der Computer, der Teil des SCADA-Systems zur Prozessüberwachung und -steuerung war, beschädigt. Dieser ehemalige Mitarbeiter, der seinerzeit als leitender Elektriker für die IT-Systeme des Unternehmens verantwortlich war, besaß noch immer die Zugangsrechte zum Standort.

2013
USA

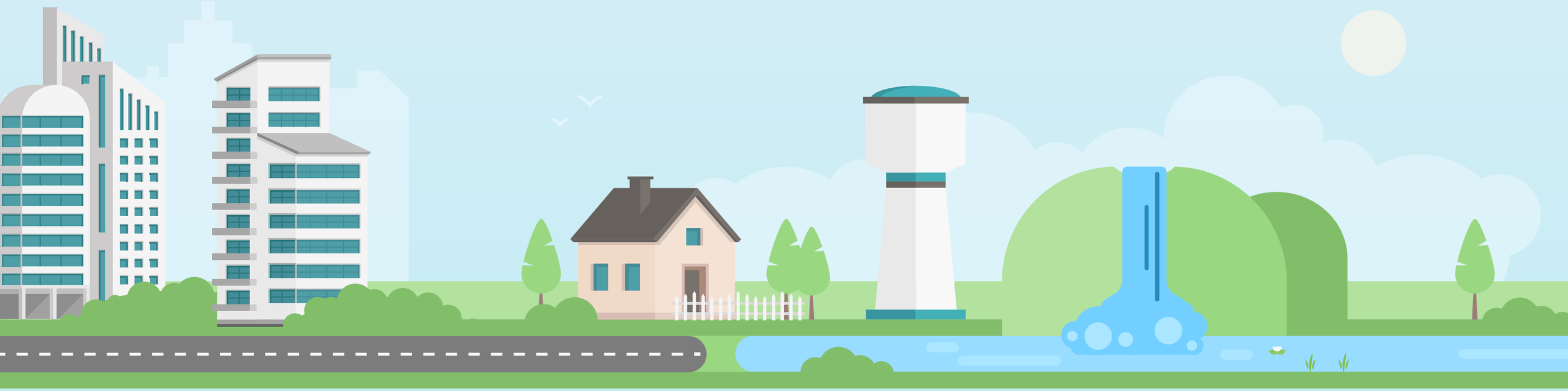
— Im April 2013 wurde ein Anschlag auf eine Trinkwasseranlage in einer kleinen Stadt in Nord-Georgia verübt. Es wurden keine Türen oder Fenster aufgebrochen, die Angreifer sollen über den Stacheldrahtzaun in die Anlage eingedrungen sein und sich dann Zugang zum Überwachungssystem verschafft haben. Daraufhin nahmen sie Änderungen an den Fluorid- und Chloreinstellungen vor, wodurch sich die Betreibergesellschaft veranlasst sah, den 400 Einwohnern zu raten, einige Tage lang kein Leitungswasser zu trinken bzw. zu verwenden.

Auf die Frage nach den möglichen Tätern antwortete der Geschäftsführer der Anlage, dass die Fahrzeuge der Mitarbeiter geortet wurden und dass sich keiner von ihnen zum Zeitpunkt des Angriffs in der Nähe der Anlage befand. Dann musste er allerdings hinzufügen, dass ehemalige Mitarbeiter noch Schlüssel oder Zugangsmöglichkeiten haben könnten, von denen sie nichts wussten …

2016
USA

— Im Bundesstaat Michigan wurde der öffentliche Wasser- und Stromversorger The Lansing Board of Water & Light (BWL) Opfer eines Ransomware-Angriffs. Ein Mitarbeiter soll auf einen bösartigen Anhang in einer E-Mail geklickt haben. Der Angriff hatte mutmaßlich keine Auswirkungen auf die Wasser- und Stromsysteme, aber die Ransomware sorgte dafür, dass einige Bereiche von BWL, einschließlich Telefonleitungen und Kundendienst, nicht verfügbar waren.

Die Führungsebene entschied daraufhin, das von den Cyber-Kriminellen geforderte Lösegeld in Höhe von 25.000 US-Dollar zu zahlen, um den normalen Geschäftsbetrieb wieder aufnehmen zu können. Ein solcher Fall darf sich bei Ihnen nicht wiederholen.



STORMSHIELD

2018
USA

—Anfang Oktober 2018 hat die Onslow Water and Sewer Authority (ONWASA) mit Sitz in Jacksonville, Colo, zweimal einen illegalen Zugriff auf ihre Computer festgestellt. Am 3. Oktober hätte sich die Ransomware Emotet über die Informationssysteme des Unternehmens verbreitet, und dann anschließend, etwa zehn Tage später, die Ryuk-Ransomware. Das Unternehmen, das nicht weniger als 150.000 Haushalte mit Wasser versorgt, war gezwungen, einen Teil seiner IT-Infrastruktur abzuschalten, um die Verbreitung der Malware einzudämmen. Dieser doppelte Angriff soll den Betrieb der Wasser- und Abwassersysteme nicht gestört haben, aber zahlreiche Datenbanken und Schlüsselelemente von ONWASA wurden vermeintlich verschlüsselt.

Das Unternehmen war daher gezwungen, seine Tätigkeit für mehrere Wochen zurückzufahren und einen Teil seiner Informationssysteme zu erneuern bzw. neu einzurichten.

2019
USA

— Im März 2019 war das öffentliche Wasserversorgungsunternehmen in Ellsworth County, Kansas, seinerseits Ziel einer bösartigen Aktion eines ehemaligen Mitarbeiters. Der Täter hat sich vermeintlich Fernzugriff auf die Informationssysteme des Unternehmens verschafft, um Änderungen an der Aufbereitung des für die Bevölkerung vorgesehenen Trinkwassers vorzunehmen.

Der ehemalige Mitarbeiter arbeitete ausgerechnet an den Überwachungssystemen der Anlage und als er das Unternehmen verließ, wurden seine Zugriffsrechte nicht widerrufen.

2019
ISRAEL

— Diese Liste legt einen kurzen Stopp im Nahen Osten ein, genauer gesagt in Israel. Im April 2020 hätten Cyber-Kriminelle, die mutmaßlich mit dem iranischen Regime in Verbindung stehen, mehrere Pump- und Aufbereitungsanlagen für Abwasser angegriffen und versucht, den Chlorgehalt in einigen Wasserversorgungssystemen, die einen Teil der israelischen Bevölkerung versorgen, zu erhöhen. Die Regierung hätte schnell reagiert und alle Wasser- und Energieinfrastrukturen des Landes aufgefordert, die Passwörter für alle SCADA-Systeme zu ändern, um sich vor weiteren illegalen Zugriffen zu schützen.

2020
ISRAEL

— Im Juni desselben Jahres meldeten die israelischen Behörden, dass auch Wasserpumpen zur Versorgung der Landwirtschaft in der Region Galiläa angegriffen wurden, ebenso wie ein Wasserversorgungssystem in der Provinz Mateh Yehuda. Details des Angriffs wurden nicht veröffentlicht, aber es wird vermutet, dass die Cyber-Kriminellen auch hier versuchten, die Qualität des Wassers durch Veränderung des Chlorgehalts zu beeinträchtigen.

STORMSHIELD

2020
ISRAEL

— Annus horribilis in Israel, da eine Gruppe iranischer Hacker Anfang Dezember 2020 einen Fehler im Steuerungssystem eines Vorratsbehälters mit aufbereitetem Wasser aufdeckte. Den Cyber-Kriminellen zufolge war das HMI-System (Human Machine Interface [Mensch-Maschine-Schnittstelle]) ohne Authentifizierung über das Internet zugänglich, so dass jeder, der Böses im Schilde führte, auf bestimmte Parameter wie die Temperatur oder den Druck des Wassers zugreifen und ihre Kontrolle übernehmen konnte.

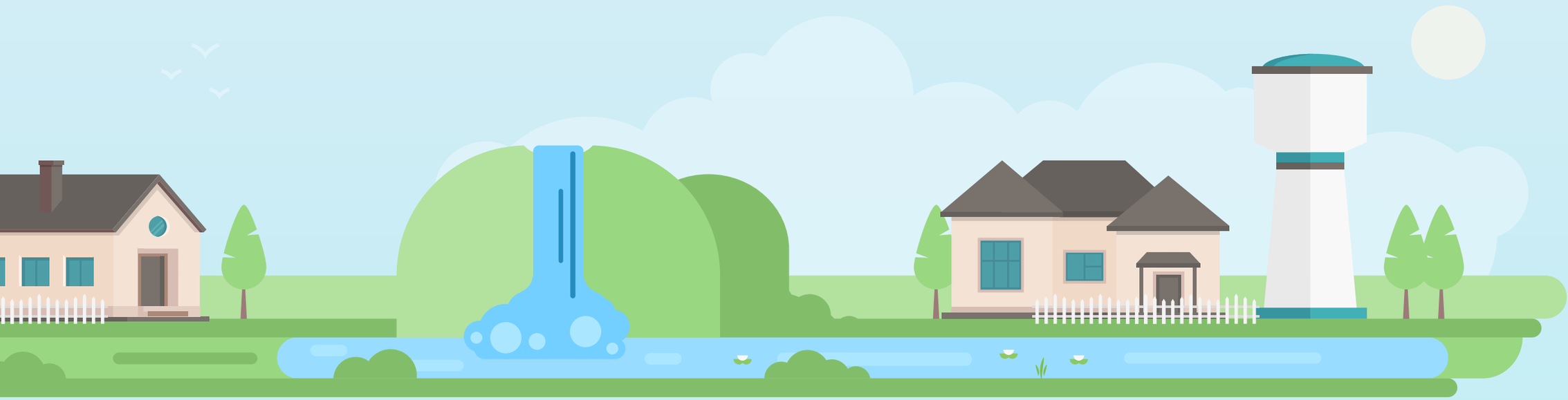
2021
USA

— Wir sind wieder zurück in den Vereinigten Staaten, in der San Francisco Bay in Kalifornien. Im Januar 2021 hätte ein Hacker die Kontrolle über eine lokale Wasseraufbereitungsanlage übernommen und die Computerprogramme für die Trinkwasseraufbereitung gelöscht. Der Angriff wird derzeit noch von den US-Behörden analysiert. Erste Hinweise deuten darauf hin, dass sich der Cyber-Kriminelle Zugriff auf die Systeme des Klärwerks verschafft hat, indem er die Zugangsdaten ehemaliger Mitarbeiter für die Verbindung mit dem TeamViewer, einer Software für den Fernzugriff und die Fernsteuerung, genutzt hat.

Einen Monat später, im Februar 2021, stand die Stadt Oldsmar, Florida, kurz vor einer Gesundheitskatastrophe. Cyber-Kriminelle hätten die Kontrolle über die Kläranlage der Stadt übernommen, deren Computersysteme nur unzureichend geschützt waren. Tatsächlich hätten nach den ersten Erkenntnissen der Untersuchung zwei Einstiegspunkte den Angriff ermöglicht: Zum einen hätten die Angreifer TeamViewer-Anmeldedaten gesammelt, die von mehreren Mitarbeitern gemeinsam genutzt wurden, und zum anderen hätten sie Schwachstellen im Windows 7-Betriebssystem ausgenutzt. Dieser Angriff hätte es den Cyber-Kriminellen ermöglicht, die Natriumhydroxid-Konzentration deutlich zu erhöhen und somit das Trinkwasser zu vergiften. Glücklicherweise konnten die Mitarbeiter der Anlage die Situation schnell unter Kontrolle bringen und rund 15.000 Einwohner der Stadt Oldsmar vor einer Vergiftung bewahren.

2021
NORWEGEN

— Volue, ein norwegisches Unternehmen, das mehrere Wasseraufbereitungsinfrastrukturen mit Anwendungen und Software ausstattet, soll der Ryuk-Ransomware zum Opfer gefallen sein. Dieser Angriff hätte sich Anfang Mai 2021 ereignet und die Informationssysteme von 200 öffentlichen Wasserversorgern im Land, alles Kunden von Volue, wären von der Ransomware infiziert gewesen. Mehrere Front-End-Plattformen von Kunden wären betroffen gewesen. Das Unternehmen hat schnell Maßnahmen zur Isolierung und anschließenden Wiederherstellung der infizierten Systeme ergriffen, um die Auswirkungen auf seine Kunden zu begrenzen. Volue zufolge wären beim jetzigen Stand der Dinge 70 % der Kunden nicht von dem Angriff betroffen oder unerreichbar gewesen. Die vollständigen Details dieses Cyberangriffs sind jedoch noch nicht bekannt und die Ermittlungen dauern an.



STORMSHIELD