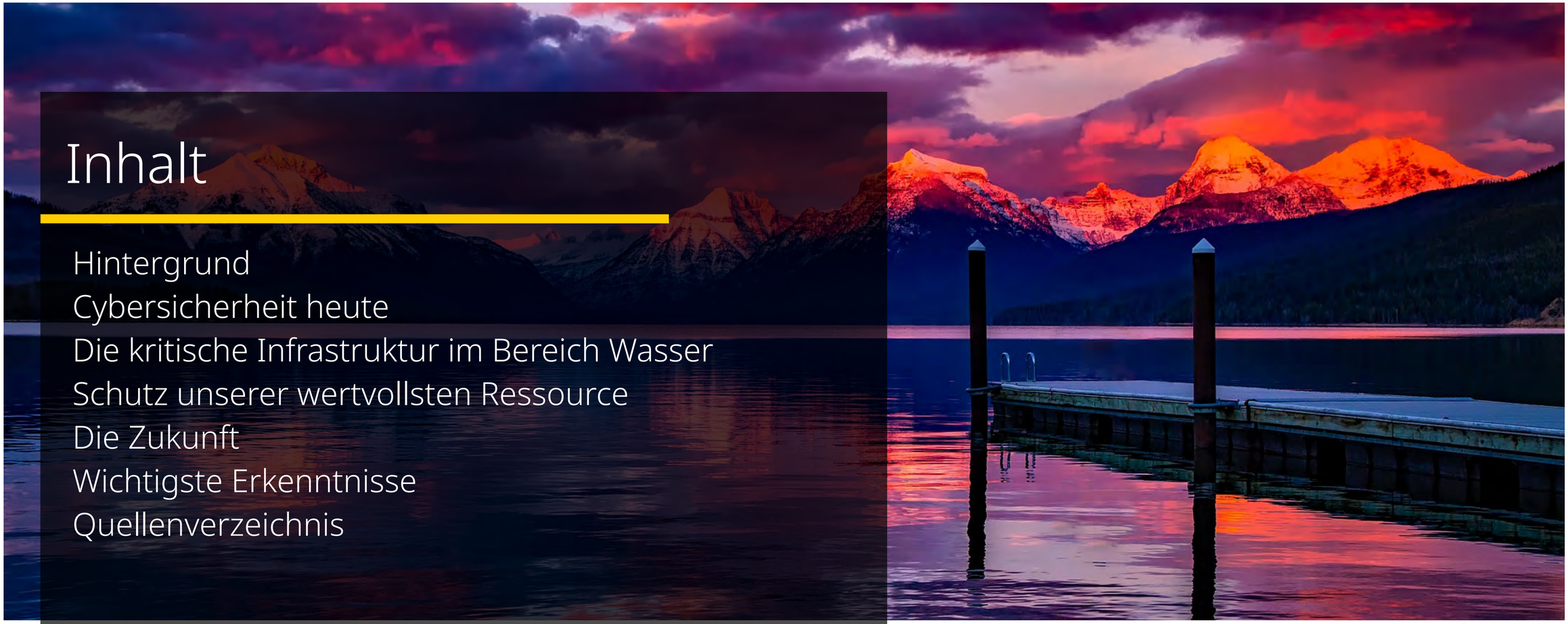
CYBERSECURITY IM WASSERSEKTOR

WHITEPAPER

OTT HydroMet

Für Unternehmen aller Branchen und auf der ganzen Welt hat das Thema Cybersicherheit absolut höchste Priorität. Der rasante technische Fortschritt macht uns immer anfälliger für Angriffe aus dem Netz. Die Folgen eines Cyberangriffs reichen von Kosten in Millionenhöhe über Schaden für den guten Ruf eines Unternehmens und im Falle von Wasserressourcen sogar bis zum Verlust von Menschenleben. Mit diesem Leitfaden möchten wir das Thema Cybersicherheit in den Fokus der Fachleute im Wassersektor rücken, über Maßnahmen zum Schutz unserer wertvollsten Ressource informieren und zeigen, dass viele Bedrohungen vermeidbar sind.



Inhalt

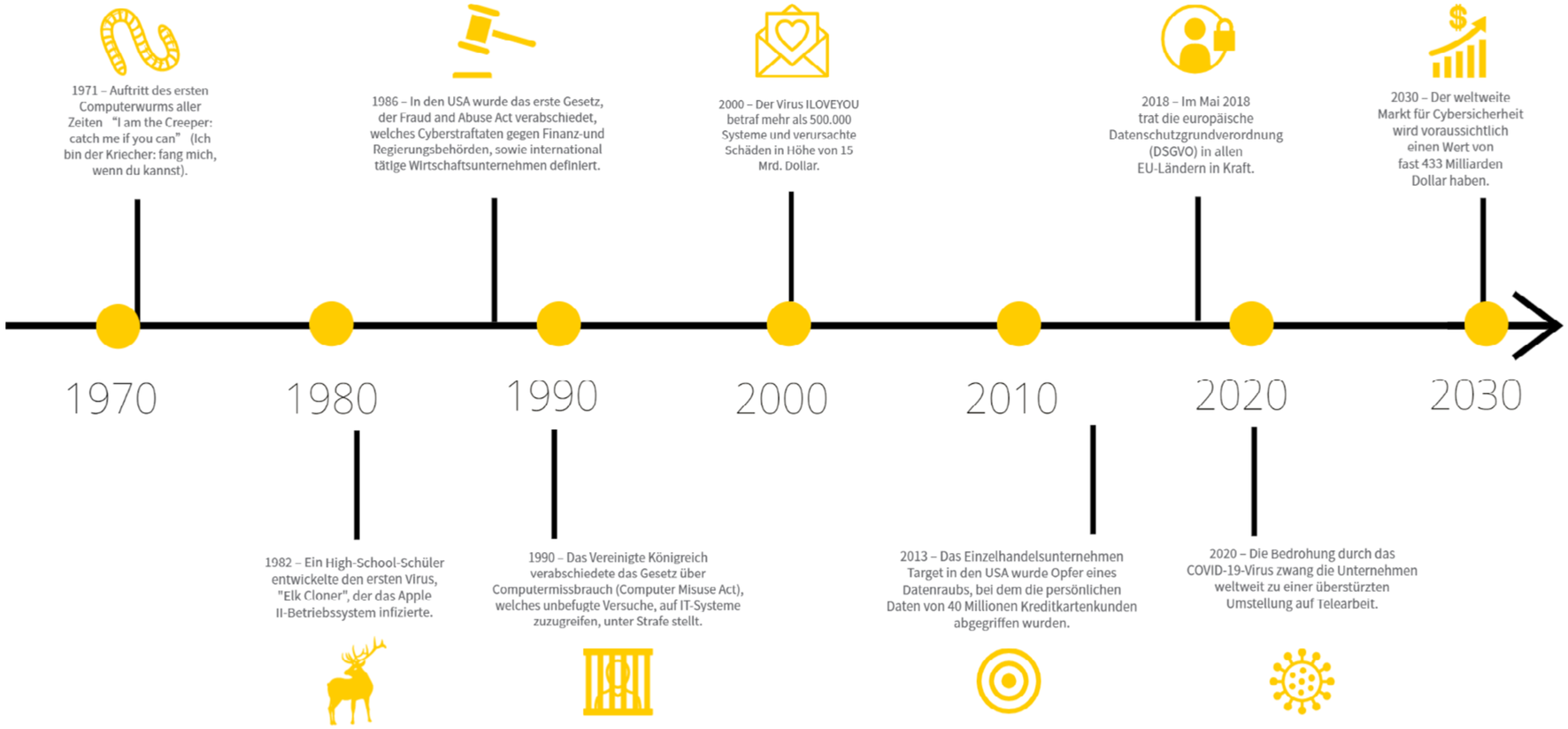
Hintergrund

Die digitale Revolution begann vor 50 Jahren, Heimcomputer und Internet hielten Einzug in unsere Gesellschaft. Seit Aufkommen der IT sehen wir uns zeitgleich mit der schnellen Digitalisierung auch mit Cyberangriffen konfrontiert. Seit 1971 der erste Computerwurm auftrat, erleben wir im 21. Jahrhundert ständig kostspielige Datenschutzverletzungen und dieses Problem wird unser ständiger Begleiter bleiben.

Weltweit ist Cybersicherheit zum großen Geschäft geworden. Laut dem “Cost of a Data Breach Report”- Bericht von IBM, wird der weltweite Markt für Cybersicherheit bis 2030 fast 433 Milliarden Dollar wert sein. Da die wirtschaftliche Entwicklung zunehmend von Daten abhängig ist, wächst auch der finanzielle Schaden, der einem Unternehmen durch einen Angriff auf seine Daten entstehen kann. Dem Bericht von IBM zufolge sind die durchschnittlichen Kosten, die eine Datenschutzverletzung verursachen kann, von 3,68 Millionen Dollar im Jahr 2020 auf 4,35 Millionen Dollar im Jahr 2022 um sage und schreibe 12,7% gestiegen.

In Europa, den USA und anderen Ländern auf der ganzen Welt wurden gesetzliche Maßnahmen zur Bekämpfung von Cyberangriffen und zum Schutz von Daten in einem digitalisierten Umfeld ergriffen, um mit dieser rasanten Entwicklung Schritt zu halten Nach 50 Jahren technologischer Innovation brauchen wir jetzt gemeinsame Anstrengungen von Regierungsvertretern, Branchenführern und Einzelpersonen, um die unbeständige Cybersicherheitslandschaft sicher zu navigieren.

Eine kurze Geschichte der Cybersecurity



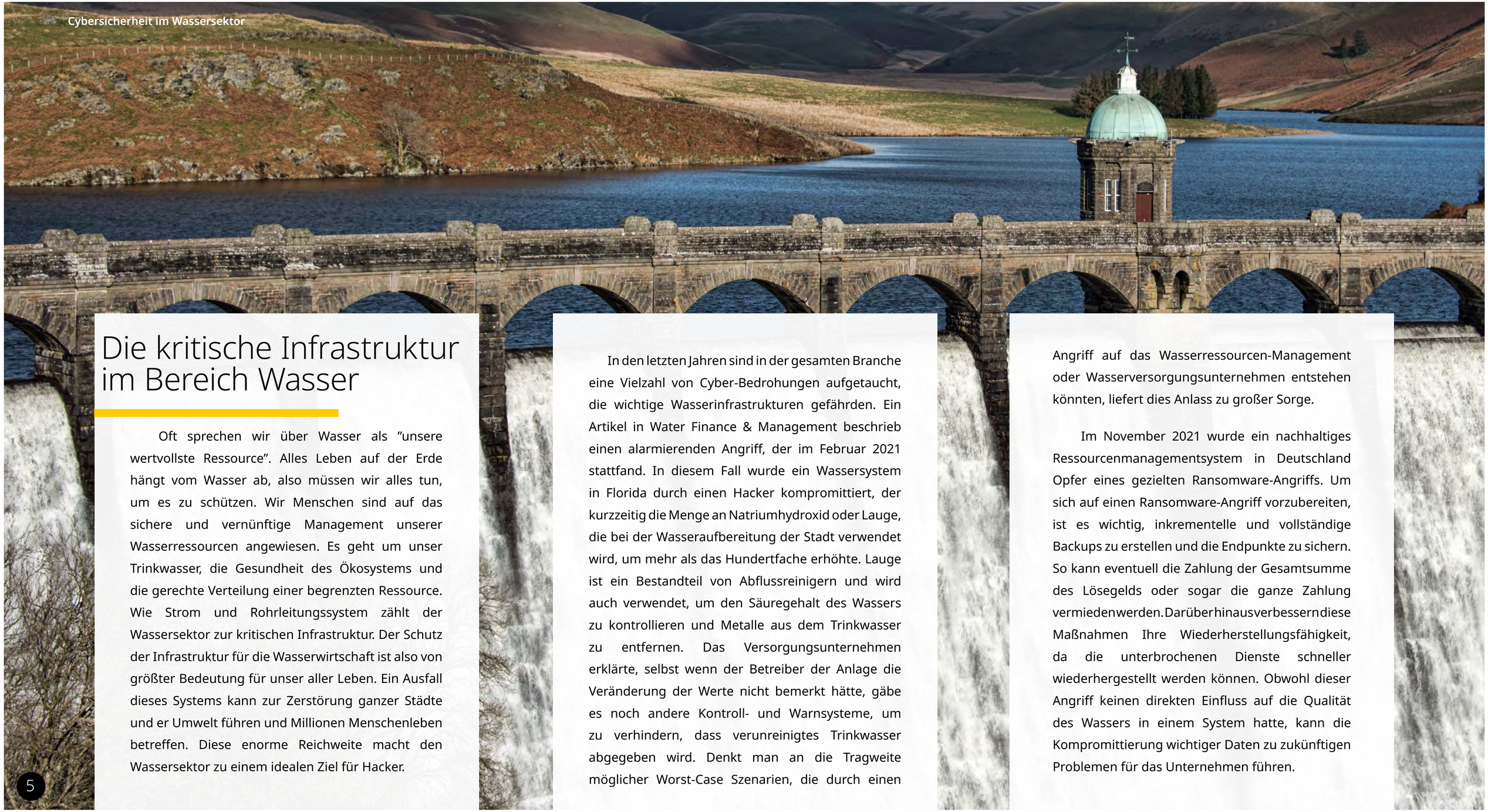
Cybersicherheit heute

Die Sicherheit unserer Daten hat in den letzten 10 Jahren enorm an Bedeutung gewonnen und auch die Art und Weise, wie wir unsere Systeme und Anlagen schützen hat sich verändert. Früher bestanden die Sicherheitsmaßnahmen darin, unsere Netzwerke mit einer einfachen Firewall und einem Virenschutz zu versehen. Doch heute denken wir weiter, wir versuchen intelligenter zu handeln als Cyberkriminelle, wir arbeiten mit Verhaltensanalysen und können Unregelmäßigkeiten in unseren Systemen frühzeitig erkennen. Allerdings finden auch die Angreifer immer raffiniertere Wege, in IT-Systeme einzudringen. Deshalb sind Prozesse und Regeln für die Sicherheit sowohl privater als auch öffentlicher Systeme eine wichtige Orientierungshilfe.

In der Europäischen Union trat im Mai 2018 die Allgemeine Datenschutzverordnung (DSGVO) in Kraft. Mit dieser Regelung wollte man Einzelpersonen eine bessere Kontrolle über ihre persönlichen Daten ermöglichen und ein für jedermann gültiges Sicherheitsniveau in der datengesteuerten digitalen Geschäftsumgebung etablieren. Die DSGVO verlangt von Unternehmen, ihre Internet-Protokolle zu verbessern, da sie im Falle einer Datenschutzverletzung Geldstrafen von bis zu 20 Millionen US-Dollar oder 4 % des weltweiten Jahresumsatzes des Unternehmens im vorangegangenen Geschäftsjahr riskieren, je nachdem, welcher Betrag höher ist. Darüber hinaus werden Unternehmen verpflichtet, bei der Entwicklung neuer Produkte und Dienstleistungen, für die personenbezogene Daten verarbeitet werden, durch Risikobewertungen und Folgenabschätzungen alle eventuell auftretenden Datenschutzprobleme zu ermitteln, zu verstehen und zu beseitigen.

In den letzten Jahren haben sowohl die Corona-Pandemie als auch das politische Klima in Russland die Besorgnis über Cyber-Bedrohungen auf der ganzen Welt in den Fokus gerückt. Im Frühjahr 2020 zwang COVID-19 den größten Teil der Welt, die Geschäftsprozesse vom Büro in eine Online-Umgebung zu verlagern. Dieser beispiellose Übergang zwang Unternehmen dazu, ihren Mitarbeitern in kürzester Zeit zu ermöglichen, ihre Arbeit zu Hause zu erledigen. Leider bedeutet diese Umstellung, dass Mitarbeiter, die im Home-Office arbeiten einem höheren Risiko von Cyberangriffen ausgesetzt sind. Nach Angaben des Abrüstungsbeauftragten der Vereinten Nationen führt die COVID-19-Pandemie dazu, dass sich die Welt auf mehr technologische Innovation und Online-Zusammenarbeit einstellt. Gleichzeitig nimmt jedoch die Cyberkriminalität zu. Die Zahl der schädlichen E-Mails stieg während der aktuellen Krise um 600 %. Der Übergang zu Telearbeit erfordert dringend ein höheres Sicherheitsbewusstsein und strengere Gesetze, um unsere wertvollen Daten zu schützen.

Im März 2022 veröffentlichte die Biden-Harris-Regierung ein "Fact Sheet: Act Now to Protect Against Potential Cyberattacks" (Jetzt handeln, um sich vor potenziellen Cyberangriffen zu schützen). Damit reagierte sie auf neue Hinweise, dass Russland gefährliche Cyberaktivitäten gegen die Vereinigten Staaten durchführen könnte. Diese Erklärung und die Executive Order on Improving the Nation's Cybersecurity (Durchführungsverordnung zur Verbesserung der Cybersicherheit der Nation) skizzieren öffentlich-private Aktionspläne zur Verbesserung der Cybersicherheit kritischer Infrastrukturen im Strom-, Pipeline- und Wassersektor. Die Gesetzgebung gibt Fachleuten aus der Wasserwirtschaft einen Leitfaden an die Hand, ihre eigenen Systeme und die ihrer Lieferanten zu analysieren und festzustellen, wie gut ihre Produkte und Dienstleistungen gegen Cyberkriminalität gesichert sind. Die weltweiten Konflikte haben großen Einfluss auf unsere Cybersicherheit und werden auch für den Wassersektor weiterhin eine wichtige Rolle spielen.



Die kritische Infrastruktur im Bereich Wasser

Oft sprechen wir über Wasser als ”unsere wertvollste Ressource”. Alles Leben auf der Erde hängt vom Wasser ab, also müssen wir alles tun, um es zu schützen. Wir Menschen sind auf das sichere und vernünftige Management unserer Wasserressourcen angewiesen. Es geht um unser Trinkwasser, die Gesundheit des Ökosystems und die gerechte Verteilung einer begrenzten Ressource. Wie Strom und Rohrleitungssystem zählt der Wassersektor zur kritischen Infrastruktur. Der Schutz der Infrastruktur für die Wasserwirtschaft ist also von größter Bedeutung für unser aller Leben. Ein Ausfall dieses Systems kann zur Zerstörung ganzer Städte und er Umwelt führen und Millionen Menschenleben betreffen. Diese enorme Reichweite macht den Wassersektor zu einem idealen Ziel für Hacker.

In den letzten Jahren sind in der gesamten Branche eine Vielzahl von Cyber-Bedrohungen aufgetaucht, die wichtige Wasserinfrastrukturen gefährden. Ein Artikel in Water Finance & Management beschrieb einen alarmierenden Angriff, der im Februar 2021 stattfand. In diesem Fall wurde ein Wassersystem in Florida durch einen Hacker kompromittiert, der kurzzeitig die Menge an Natriumhydroxid oder Lauge, die bei der Wasseraufbereitung der Stadt verwendet wird, um mehr als das Hundertfache erhöhte. Lauge ist ein Bestandteil von Abflussreinigern und wird auch verwendet, um den Säuregehalt des Wassers zu kontrollieren und Metalle aus dem Trinkwasser zu entfernen. Das Versorgungsunternehmen erklärte, selbst wenn der Betreiber der Anlage die Veränderung der Werte nicht bemerkt hätte, gäbe es noch andere Kontroll- und Warnsysteme, um zu verhindern, dass verunreinigtes Trinkwasser abgegeben wird. Denkt man an die Tragweite möglicher Worst-Case Szenarien, die durch einen Angriff auf das Wasserressourcen-Management oder Wasserversorgungsunternehmen entstehen könnten, liefert dies Anlass zu großer Sorge.

Im November 2021 wurde ein nachhaltiges Ressourcenmanagementsystem in Deutschland Opfer eines gezielten Ransomware-Angriffs. Um sich auf einen Ransomware-Angriff vorzubereiten, ist es wichtig, inkrementelle und vollständige Backups zu erstellen und die Endpunkte zu sichern. So kann eventuell die Zahlung der Gesamtsumme des Lösegelds oder sogar die ganze Zahlung vermiedenwerden.Darüberhinausverbesserndiese Maßnahmen Ihre Wiederherstellungsfähigkeit, da die unterbrochenen Dienste schneller wiederhergestellt werden können. Obwohl dieser Angriff keinen direkten Einfluss auf die Qualität des Wassers in einem System hatte, kann die Kompromittierung wichtiger Daten zu zukünftigen Problemen für das Unternehmen führen.

Schutz unserer wertvollsten Ressource

Maßnahmen, die jeder Einzelne treffen kann

Aufklärung und Sensibilisierung von Mitarbeitern sind ein wesentlicher Bestandteil des Cyberschutzes, da jeder Einzelne in einer Organisation für eine gute Cyberhygiene verantwortlich ist. In der Tat ist der Faktor Mensch das schwächste Glied bei der Abwehr von Cyberangriffen. Nach Angaben der Cybersecurity & Infrastructure Security Agency (CISA) beginnen mehr als 90 % der erfolgreichen Cyberangriffe mit einer Phishing-E-Mail. Angreifer geben sich oft als zugehörige Personen innerhalb eines Unternehmens aus, um Mitarbeiter dazu zu verleiten, ihnen Informationen zu geben. Da sich die Bedrohungen ständig weiterentwickeln, empfiehlt die CISA vier einfache Maßnahmen, die jeder Einzelne ergreifen kann, um die Cyberabwehr in seinem Unternehmen und im Wassersektor zu stärken.

1. Implementieren Sie eine Multi-Faktor Authentifizierung für Ihre Nutzerkonten. (Durch die Multi-Faktor-Authentifizierung ist die Wahrscheinlichkeit, dass Sie gehackt werden, um 99 % geringer.)
2. Aktualisieren Sie regelmäßig Ihre Software. Nutzen Sie automatische Updates.
3. Vertrauen Sie Ihrer Intuition – erst nachdenken, dann klicken.
4. Verwenden Sie starke Passwörter und im Idealfall einen Passwortmanager, um eindeutige Passwörter zu generieren und zu speichern. Senden Sie niemals Zugangsdaten auf eine Email-Anfrage hin.

Maßnahmen von Unternehmensseite

Eine Priorisierung von oben nach unten befähigt ein Team, eine Kultur des verantwortungsvollen Verhaltens im Netz zu etablieren. Die Synchronisierung von Standardprozessen innerhalb einer Gruppe fördert den Schutz und das Bewusstsein über kritische Situationen. Es gibt fünf Schritte, die vom National Institute of Standards and Technology (NIST) empfohlen werden und die Unternehmen sofort umsetzen können, um sich selbst, ihre Vermögenswerte und ihren Ruf zu schützen.

1. Risiko identifizieren: Verschaffen Sie sich ein Grundverständnis Ihrer digitalen Umgebung um das Risiko für einen Cyberangriff auf Ihre Systeme, Vermögenswerte, Daten und Ihre Arbeitsfähigkeit zu erkennen.
2. Werte schützen: Entwickeln und implementieren Sie geeignete Schutzmaßnahmen, um die Auswirkungen eines potenziellen Cybersicherheitsvorfalls zu begrenzen. Dazu gehört die Kontrolle des Zugangs zu digitalen und physischen Vermögenswerten, aber auch die Verantwortung für die Ausbildung und Schulung aller Mitarbeiter.
3. Angriffe erkennen: Nutzen Sie Systeme, die kontinuierlich überwachen, ob ungewöhnliche Aktivitäten oder sonstige Bedrohungen für Ihre operative Leistung auftreten.
4. Reagieren: Wenn es zu einem Cyberangriff kommt, müssen Sie einen Reaktionsplan bereit haben, um die Auswirkungen unter Kontrolle zu bringen. Sobald Sie den Vorfall geklärt haben, passen Sie Ihren Reaktionsplan mit den gewonnenen Erkenntnissen an.
5. Wiederherstellung: Erstellen Sie ein Konzept, wie Funktionen oder Dienste, die durch einen Cyberangriff beschädigt wurden, wieder hergestellt werden.

Phishing: Eine gängige Taktik von Angreifern, um sich Zugang zu verschaffen, besteht darin, Internetnutzer mit irreführenden E-Mail-Nachrichten oder Websites dazu zu bringen, persönliche oder vertrauliche Informationen preiszugeben, die dann unrechtmäßig verwendet werden können.

Die Zukunft

Da Unternehmen sich auf dem Weg der digitalen Transformation befinden, ist zu erwarten, dass dem Schutz des Wassersektors vor Cyberangriffen hohe Priorität eingeräumt wird und damit sowohl neue Beschäftigungsmöglichkeiten als auch die Bereitstellung finanzieller Mittel einhergehen. Sowohl in den USA als auch in der EU werden Regierungsrichtlinien weiterhin verlangen, dass Sicherheitsaspekte in die Produktgestaltung einfließen. Zu Beginn der Entwicklung eines neuen Produkts oder Softwareprogramms müssen sich Produktdesigner daher fragen: "Ich möchte, dass mein Produkt dieses oder jenes leistet... Wie mache ich das sicher?". Bisher lief das Thema Cybersicherheit in den meisten Unternehmen einfach nebenher. In Zukunft erwarten Experten, dass Cybersicherheit zu einem Kernbereich wird, gleichbedeutend mit dem Finanz-oder Marketingbereich.

Aktuell wird im Wassersektor eine Methode namens Air-Gapping als Schutzstrategie eingesetzt. Beim Air-Gapping wird ein Computer, ein Netzwerk oder ein Gerät physisch vom Internet oder LAN isoliert. Richtig angewandt, ist diese Technik eine kostengünstige und wirksame Methode, um Ihre Daten zu schützen. In dem Maße, in dem sich die Welt auf Cloud-basierte Systeme verlagert, wird Air-Gapping jedoch zu einem veralteten Ansatz. Eine nachhaltigere Strategie ist die Implementierung einer seriösen Cloud-basierten Software, die kontinuierlich Schwachstellen scannt und überwacht.

Sicherheit vor Ort und in der Cloud

Auf dem Weg in eine vernetzte Zukunft fragen sich Wasserexperten, wie sie ihre wertvollen Daten und Systeme am besten schützen können. Bei der Implementierung einer Vor-Ort- oder einer Cloud-basierten Lösung gibt es Vor- und Nachteile zu berücksichtigen. Der Vorteil der Vor-Ort-Lösung liegt darin, dass sich Server und Daten physisch in Ihrem Büro befinden. Daten im eigenen Haus zu verwalten kann zwar zweckmäßig sein, aber auch gefährlich, wenn eine Einrichtung gefährdet ist. Die Vor-Ort-Lösung bietet den Vorteil, dass die Verwaltung des Netzwerks in der Verantwortung des Unternehmens liegt, wenn Anpassungen vorgenommen werden müssen. Allerdings kann auch für eine kleine IT-Abteilung der Wartungsaufwand, der für den erfolgreichen Betrieb einer On-Premise-Lösung erforderlich ist, zu groß sein, da ständige Schulung und Überwachung der Sicherheit erforderlich sind.

Cloud-basierte Systeme hingegen speichern die Daten dezentralisiert. Das bedeutet, dass Ihre Daten überall auf der Welt in Rechenzentren gespeichert sind. Damit wird die Kontrolle darüber aufgegeben, wo genau sich Ihre wertvollsten Daten physisch befinden. Allerdings bietet die Dezentralisierung Ihrer Daten eine Erleichterung gegenüber der Datenvernichtung in einer lokalen Umgebung und minimiert daher die Anforderungen an eine qualifizierte IT-Abteilung. Viele Wasserwirtschaftsunternehmen wechseln zu einem Cloud-basierten Datenverwaltungssystem, da es eine IT-Abteilung praktisch ersetzen kann. Seriöse Online-Softwareplattformen führen kontinuierlich Scans und Überwachungen durch, um sicherzustellen, dass alles auf dem neuesten Stand ist und Schwachstellen behoben werden. Die neue Gesetzgebung verlangt von den Dienstleistern, dass sie ihre Enddienste und Datenschutzrichtlinien transparent machen, und bietet dem Wassersektor einen Kommunikationsrahmen, der cloudbasierte Systeme zu einer bevorzugten Option für ihre Datensicherheit macht.

Wichtigste Erkenntnisse

Was kostet es mich, meine Cybersicherheit zu verbessern?

Die grundlegenden Cybersicherheitspraktiken in den zuvor aufgeführten Aktionsschritten sind nicht alle kostenintensiv. Um die Kosten für Ihre Cybersicherheit angemessen bewerten zu können, führen Sie eine Risikobewertung für den Fall eines Hackerangriffs durch und vergleichen Sie den Schaden, der dadurch entstehen könnte mit Ihren Investitionen in die Cybersicherheit. Bereiten Sie sich auf das Worst-Case-Szenario vor und erstellen Sie einen Plan, wie Sie darauf reagieren können. Für besseren Schutz ist es wichtig, vorausschauend in die Zukunft zu denken und proaktiv zu handeln.

Ransomware kann ein Unternehmen viel Geld kosten und sich sehr schnell verbreiten, wenn sie einmal in ein System eingedrungen ist. Gute inkrementelle und vollständige Backups sind also wichtig, damit Sie Ihre Daten wiederherstellen können und somit nicht erpressbar sind. Testen Sie Ihre Backups, damit Sie sich darauf verlassen können, dass sie bei Bedarf funktionieren. Auch gutes Endpunkt-Management ist unerlässlich, um Unregelmäßigkeiten zu erkennen und Angriffe zu verhindern. Mit der Umstellung der Welt auf eine Cloud-basierte Umgebung verfügt Software heute glücklicherweise über innovative Funktionen, die verdächtiges Verhalten scannen, erkennen und blockieren können.

Was kann jeder Einzelne für die Datensicherheit tun?

Der Schutz unseres Wassers und der damit verbundenen Daten, die Teil einer kritischen Infrastruktur sind, verlangt die aktive Beteiligung jedes Einzelnen in dieser Branche. Wir haben mit Experten für Cybersicherheit gesprochen:

“Machen Sie sich bewusst, dass Cybersicherheit ein kontinuierlicher Prozess ist. Gewöhnen Sie sich aktive Überwachung und kontinierliche Wachsamkeit an.”

Eric Dorgelo
Chief Technology Officer
Aquatic Informatics

“Machen Sie Sicherheitsbewusstsein und Schulung zur Priorität im ganzen Unternehmen. Cybersicherheit ist nicht Aufgabe einer einzelnen Abteilung.”

Vickitt Lau
Director of Product Security and Cloud Operations
Aquatic Informatics

“Machen Sie es sich zur täglichen Aufgabe die Cybersicherheit zu verbessern. Lernen Sie jeden Tag dazu.”

Diane Kelly
Chief Information Security Officer
Danaher Water Platform

Nützliche Informationen zur Cybersicherheit für Hydrologen:

Webinar - Cybersicherheit im Wassersektor

Basismaßnahmen der CyberSicherheit

5 Gründe das Wasserdaten-Management zu modernisieren

Water Security Plan - Implementierungshandbuch für Trinkwassersysteme

Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen

Bundesamt für Sicherheit in der Informationstechnik

Cybersicherheitsstrategie für Deutschland

DCSO Deutsche Cyber-Sicherheitsorganisation

Cyber-Sicherheitsrat Deutschland e.V.

Quellenverzeichnis

ABC News, ABC News Network, https://abcnews.go.com/Health/wireStory/latest-india-reports-largest-single-day-virus-spike-70826542.

“Cost of a Data Breach Report 2022.” IBM, https://www.ibm.com/security/data-breach.

“Cybersecurity Framework.” NIST, 18 Apr. 2022, https://www.nist.gov/industry-impacts/cybersecurity-framework.

“Cybersecurity Risk Management Tool.” Home Page, https://cybersecurity.awwa.org/.

EPA, Environmental Protection Agency, https://www.epa.gov/waterriskassessment/epa-cybersecurity-best-practices-water-sector.

“Fact Sheet: Act Now to Protect against Potential Cyberattacks.” The White House, The United States Government, 22 Mar. 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/.

Farr, Andrew. “High Tech, High Stakes: How Vulnerable to Cyberattacks Is U.S. Water Infrastructure?” Water Finance & Management, 11 May 2022, https://waterfm.com/how-vulnerable-to-cyberattacks-water-infrastructure/.

O’Donovan, Brian. “Cyber Security Expert Warns Firms over Online Threats.” RTE.ie, RTÉ, 27 June 2022, https://www.rte.ie/news/2022/0627/1306985-cyber-security-conference/.

“The Path to Cyber Security 2030.” Business Insider, 4 Aug. 2022, https://www.businessinsider.in/tech/enterprise/news/the-path-to-cyber-security-2030/articleshow/93337901.cms.

Research, GlobalData Thematic, and GlobalData Thematic Research. “Cybersecurity: Timeline.” Verdict, 7 July 2020, https://www.verdict.co.uk/cybersecurity-timeline/.

“Shields Up.” Cybersecurity and Infrastructure Security Agency CISA, https://www.cisa.gov/shields-up.

**Verweise auf Informationen aus Drittquellen, einschließlich, aber nicht beschränkt auf Websites, Berichte und Veröffentlichungen, wurden nicht auf ihre Richtigkeit überprüft.*

Insights for Experts

Mehr Informationen gibt es hier:

OTT HydroMet
sales@otthydromet.com
euinfo@otthydromet.com
www.otthydromet.com

OTT HydroMet

HY-AQ-SW-wp-Cyber_Security-DE-220919