Newsletter des VfEW
Verband für Energie- und
Wasserwirtschaft
Baden-Württemberg e. V.
November 2020

vfew synergie

Liebe Leserinnen und Leser,

auch der Alltag der Energie- und Wasserversorger war in diesem Jahr von der Coronapandemie bestimmt. Doch der Umbruch der Branche schreitet unaufhaltsam fort. Die Herausforderungen bleiben groß. Ein wichtiger Baustein in der Transformation der Branche ist die Digitalisierung der Prozesse. Daraus ergibt sich ein Thema, das uns im Verband für unsere Mitgliedsunternehmen in letzter Zeit zunehmend beschäftigt hat: Die Sicherheit in der digitalen Umgebung. Denn die Digitalisierung birgt immense Chancen, aber sie bringt auch neue Sicherheitsrisiken mit sich. Mit der Uniklinik Düsseldorf sowie dem Robert-Koch-Institut sind in letzter Zeit gleich zwei prominente Einrichtungen Hackerangriffen zum Opfer gefallen. Die Folgen waren gravierend. Auch unsere Branche muss sich vorsehen: Die kriminellen Täter sind schnell und schlau, sind international organisiert und kommen in der Regel ungestraft davon. Wie wir uns schützen können, wie wichtig aber auch die Unterstützung der Politik dabei ist, möchten wir in dieser Ausgabe darstellen. Zum Schutz von uns allen, muss die Politik Regeln definieren und Wege finden, diese in der digitalen Welt auch durchzusetzen.

Bleiben Sie weiterhin gesund!

Ihr

Klaus Saiger,
Präsident des VfEW

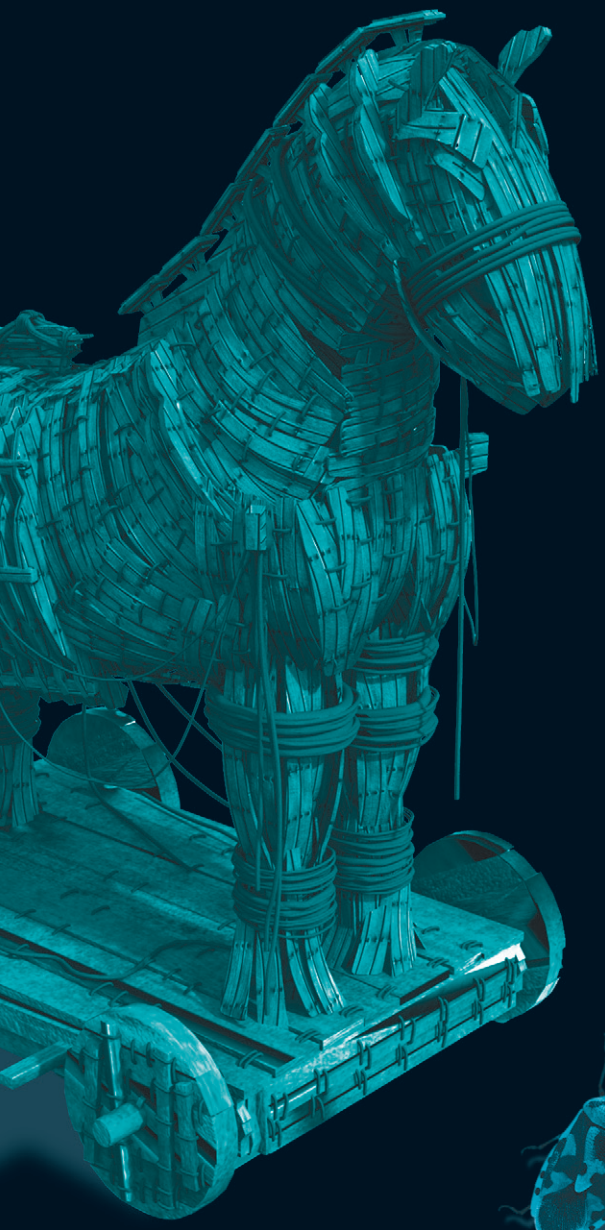
Im Visier der Cyberpiraten

IT-Sicherheit: eine Herausforderung für alle Unternehmen der Energie- und Wasserversorgung

Foto: Gorodenkoff, www.shutterstock.com

»Für einen Hacker ist Deutschland leider ein Eldorado«

Die Stadtwerke Ettlingen haben 2013 den Hacker Felix »FX« Lindner aufs eigene System angesetzt, um Schwachstellen ans Licht zu bringen. Niemand im Unternehmen war darauf vorbereitet. Eberhard Oehler, Geschäftsführer der Stadtwerke Ettlingen, hat dafür viel Aufmerksamkeit bekommen. Bis heute wird er als Redner angefragt, auch international. Götz Schartner, Geschäftsführer der CEO 8com GmbH & Co. KG, stärkt die Cyber Security von Unternehmen und schützt sie vor Cyberangriffen. Er stellt fest, dass Unternehmen bis heute wenig auf Hackerangriffe vorbereitet sind, obwohl diese zunehmen werden.



Nehmen wir an, ein Hacker würde die Stadtwerke Ettlingen angreifen – was würde der tun und mit welchen Folgen?

Schartner: »Der Hacker dringt in das System ein. Er verschlüsselt dann die Daten und zerstört die Backups. Abrechnungsdaten, Kundendaten und Konfigurationsdaten wären weg.«

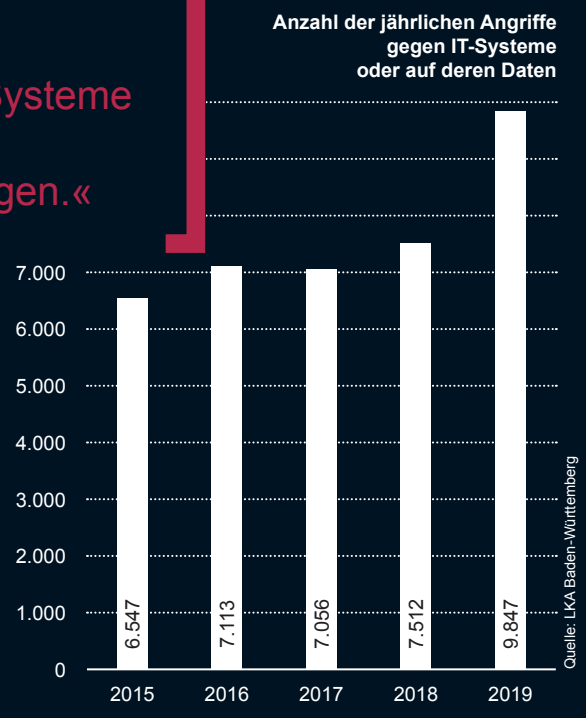
Oehler: »Es wäre eine Katastrophe für uns. Unmittelbar nach dem Angriff würde die Lösegeldforderung folgen. Diese Organisationen arbeiten hochprofessionell.«

Schartner: »Wir hatten schon den skurrilen Fall in Baden-Württemberg, dass die Wiederherstellung der Daten durch den Hacker nicht geklappt hat. Der Hacker hat sogar das Lösegeld zurückbezahlt. Das ist deren Geschäftsmodell.«

»Wenn Sie Pech haben und IT-Umgebung vollständig verseucht ist, können Sie das System nicht mehr bereinigen.«

Götz Schartner,
Geschäftsführer
CEO 8com GmbH & Co. KG

»Seit 2015 ist die Zahl der Angriffe gegen IT-Systeme oder auf deren Daten um 150 Prozent gestiegen.«



Welchen Schaden könnte ein Hackerangriff den Stadtwerken zufügen?

Oehler: »Wäre die Leitstelle vom Hackerangriff betroffen, hätten wir unmittelbar den wirtschaftlichen Schaden, wenn es dadurch bei unseren Kunden zu einem Produktionsausfall kommen würde. Der Verlust könnte sehr schnell im sechsstelligen Bereich liegen. Wenn man uns dann Fahrlässigkeit nachweisen könnte, weil wir in Sachen IT-Sicherheit zu wenig getan haben, dann wären wir für diese Schäden haftbar.«

Schartner: »Wenn Sie Pech haben und die IT-Umgebung vollständig verseucht ist, können Sie das System nicht mehr bereinigen. In einem Windowssystem haben Sie bis zu 100.000 Steuerdateien, die sie einzeln auf versteckte Vektoren überprüfen müssen. Das schaffen sie gar nicht. Sie müssen die IT austauschen und neue Hardware kaufen. Da wären Sie schnell bei 12 – 15 Millionen Euro internen Kosten, ganz grob.«

Oehler: »Beim Verlust der Kundendaten kommen in der Regel noch die Datenschutzbeauftragten der Landesbehörden, die alles überprüfen. Zu allem kommt der Reputationsschaden. Der ist kaum zu berechnen.«

Warum werden die Täter so selten aufgespürt und belangt?

Schartner: »Für die Hacker ist Deutschland ein Eldorado. Die Täter kommen meist aus Ländern, in denen die Strafverfolgung nicht funktioniert. In der Theorie könnten Sie die Täter schon finden, aber uns sind die Hände gebunden. Es gab ja mal die gesellschaftliche Diskussion über das ›Hack-Back‹, also das Zurückholen der Daten durch einen Gegenangriff aus Notwehr. Das ist bei uns nicht erlaubt, der Hacker hat also nichts zu befürchten und verdient ein enormes Geld. In anderen Ländern wie den USA oder Israel ist das besser geregelt. Unser Rechtsstaat muss doch auch wehrhaft bleiben.«

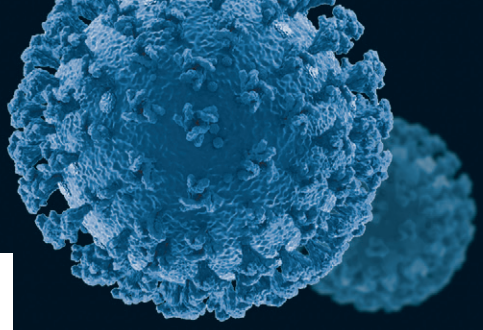
Oehler: »Wir müssen leider auch davon ausgehen, dass die Dunkelziffer der tatsächlichen Angriffe viel höher ist, als wir wissen. Die wenigsten Unternehmen machen einen solchen Vorfall öffentlich. Zum Glück ist es noch nie zu einem größeren Blackout gekommen.«

Was war der Anlass dafür, dass Sie die Stadtwerke Ettlingen absichtlich hacken ließen?

Oehler: »Ein Auslöser war die Anfrage eines Journalisten. Wir hatten auch nur eine diffuse Vorstellung davon, was durch einen Hackerangriff passieren könnte. Wir wollten lernen, wo wir angreifbar und verletzlich sind. Der Hackerangriff hat uns sehr deutlich unsere Schwachstellen aufgezeigt. Das hat eine große Welle ausgelöst, intern und extern. Bis heute werde ich von Kollegen angerufen oder als Redner dazu angefragt. Die Entscheidung war damals absolut richtig.«

Keiner in Ihrem Haus war darauf vorbereitet. Was hat es bei den Mitarbeitern ausgelöst?

Oehler: »Ich habe weder die Mitarbeiter noch die Software-Lieferanten im Vorfeld informiert. Das hat auch zu Vorwürfen geführt. Aber



ich wollte im Originalzustand wissen: Sind wir sicher oder sind wir weniger sicher?«

Schartner: »Wenn ein Hacker – bei solch einer Simulation legal und mit ethischen Vorsätzen – komplett ›durchmarschieren‹ kann, hat das eine extreme Aussagekraft und Sensibilisierungseffekte. Wenn die IT mit im Boot ist, können Sie schneller eine höhere Anzahl an Sicherheitslücken finden. Das machen wir auch. Der Ansatz, den Ettlingen gemacht hat, ist aus unserer Sicht der richtige: Da gibt es keine Unterstützung und das Ergebnis ist nicht mehr anzuzweifeln. Wir hatten mal einen Bankenvorstand als Kunden. Er wollte nicht glauben, dass man seine Bank auch hacken kann. Wir haben dann eine Videoaufnahme von ihm während der Arbeit gemacht. Der war ziemlich entsetzt.«

Oehler: »Das Thema IT-Sicherheit ist eine Daueraufgabe. Im Durchschnitt registrieren wir um die 40 neue Sicherheitslücken am Tag. Die Verletzbarkeit wird mit der weiteren Automatisierung und Digitalisierung größer. Kein Monteur schreibt mehr einen Stundenzettel, sondern gibt die Daten per Handy direkt ins System ein. 70 Prozent der Hackerangriffe werden durch Fehler der Anwender, also menschliche Schwächen, erst möglich. Wir führen deshalb immer wieder Schulungen durch, um die Mitarbeiter für neue Gefahren zu sensibilisieren. Das Wichtigste ist, die Aufmerksamkeit der Mitarbeiter für das Thema dauernd aufrechtzuerhalten.«

Was können kleinere Stadtwerke mit weniger personeller und finanzieller Ausstattung tun?

Oehler: »Oft sind wir auf die Zulieferer für die Software angewiesen. Da lohnt es sich, genau hinzuschauen, wie die mit dem Thema umgehen. Viele Programmierer sind beim Thema ›sichere Programmierung‹ nicht gut genug ausgebildet. Auch über einen fusionierten IT-Betrieb mit anderen Stadtwerken kann man nachdenken.«

Schartner: »Grundsätzlich ist jeder zur Risikovorsorge in seinem Unternehmen verpflichtet. Zu sagen, ›Das ist zu teuer, ich lass das‹, ist keine Option. IT-Sicherheit ist hoffentlich nie profitabel.«

Was erwartet uns noch?

Schartner: »Ein Hacker ist ja kein Hexenmeister, er ist ein technikbegabter Mensch, der aufgrund von Konfigurationen, Sicherheitslücken oder menschlichen Schwächen in Computersysteme eindringt. Die Wege sind heute im Wesentlichen alle bekannt. Selbst die schwerwiegenden Vorfälle der vergangenen Jahre wären mit relativ einfachen, präventiven Maßnahmen zu verhindern gewesen. Bis vor fünf Jahren gab es noch recht wenig Manipulationen oder Angriffe auf Versorger. Die sind heute täglich und es gibt hohe finanzielle Schäden. Bis das noch schlimmer wird, ist eine Frage der Zeit. Leider sind die Unternehmen aus meiner Wahrnehmung nicht besser vorbereitet, trotz aller Kenntnis.«

Oehler: »Wir haben eine sehr hohe Versorgungssicherheit, die Ausfallzeiten sind im Vergleich zu anderen europäischen Ländern weitaus besser. Wir haben daher eine gewisse ›Katastrophenarmut‹ und dadurch zu wenig Aufmerksamkeit für das Thema. Im Bereich der IT-Sicherheit findet der Austausch in der Branche leider kaum statt. Wir brauchen unbedingt die Kommunikation untereinander. Nur dadurch werden wir alle besser.« *//*

> »70 Prozent der Hackerangriffe werden durch Fehler der Anwender, also menschliche Schwächen, erst möglich.«
>
> Eberhard Oehler,
> Geschäftsführer
> der Stadtwerke Ettlingen

Erfolgsfaktor Effizienz

Der Ordnungsrahmen zur Gewährleistung der Cybersicherheit von kritischen Infrastrukturen in Deutschland und der EU wird gerade umfassend überarbeitet. Die Aktualisierungen bieten die Chance, langfristige Verbesserungen der Cybersicherheit zu erreichen. Voraussetzung für den Erfolg ist jedoch eine ökonomisch effiziente Umsetzung.

Foto: EVF

Wo steht die deutsche Cybersicherheitspolitik aktuell?

Mit dem IT-Sicherheitsgesetz (IT-SiG) wurde 2015 erstmals ein einheitlicher deutscher Ordnungsrahmen für den Umgang mit Cyberbedrohungen und zur Regulierung von Betreibern kritischer Infrastrukturen geschaffen. Durch die fortschreitende Digitalisierung und Austragung internationaler Konflikte im digitalen Raum hat sich die Gefährdungslage im Bereich der IT- und Cybersicherheit in den vergangenen Jahren jedoch zugespitzt.

Bereits im Koalitionsvertrag wurde deshalb vereinbart, den gesetzlichen Rahmen zu diesem Thema zu überarbeiten. So hat das Bundesinnenministerium (BMI) im Jahr 2019 begonnen, das IT-SiG zu novellieren. Ziel ist eine ganzheitliche Verbesserung der IT-Sicherheit von Wirtschaft, Gesellschaft und Staat sowie eine ständige Anpassung und Weiterentwicklung von Schutzmechanismen und Abwehrstrategien gegen Bedrohungen aus dem digitalen Raum. Die bisher veröffentlichten Referentenentwürfe zeigen bereits, wohin es seitens des Gesetzgebers gehen soll: Vorgesehen ist eine Ausweitung des IT-SiG auf weitere Teile der Wirtschaft, die im besonderen öffentlichen Interesse agieren, wie z. B. Unternehmen der Rüstungs- oder Chemieindustrie und auch Unternehmen mit volkswirtschaftlicher Bedeutung. Außerdem sieht der aktuelle Entwurf die Weiterentwicklung der Rechte und Pflichten von KRITIS-Betreibern vor und würde eine Ausweitung der Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) bewirken. Der Gesetzgeber beabsichtigt, das Gesetzgebungsverfahren bis Ende 2020 verabschieden zu können. Angesichts teilweise fundamentaler Meinungsverschiedenheiten zwischen den beteiligten Ministerien ist allerdings fraglich, ob dies noch in der aktuellen Legislaturperiode gelingen kann.

Welche Entwicklungen sind auf EU-Ebene zu erwarten?

Die EU-Kommission hat mit der Aktualisierung der sogenannten NIS-Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit begonnen. Mit der Einführung der NIS-Richtlinie wurde 2016 ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cybersicherheit, die Cyberabwehrfähigkeit sowie Mindestsicherheitsanforderungen und Meldepflichten für Betreiber kritischer Infrastrukturen geschaffen. Der Großteil der Anforderungen wurde im Jahr zuvor bereits durch das IT-SiG in Deutschland eingeführt. Wichtige Ziele der Novellierung sind die verstärkte zwischenstaatliche Zusammenarbeit und die Einführung erweiterter Meldepflichten, die die Meldung erheblicher Sicherheitsvorfälle, auch über Landesgrenzen hinaus, vorsieht. Entscheidend für den Erfolg der Neuerung ist zudem eine stärkere Verpflichtung von Herstellern und Lösungsanbietern, einen Beitrag zum Schutz kritischer Infrastrukturen zu leisten. Bis Anfang 2021 soll ein erster Gesetzesvorschlag vorliegen.

Wie sieht die Cybersicherheitspolitik der Zukunft aus?

Aus Sicht des BDEW hat sich der aktuelle Ansatz zum Schutz kritischer Infrastrukturen bisher bewährt, da hierdurch ein einheitliches Mindestmaß an IT- und Cybersicherheit in der EU gewährleistet werden konnte. Die Bedrohungen aus dem digitalen Raum haben in den letzten Jahren nachweislich zugenommen. Daher ist eine Überarbeitung der bestehenden Gesetzgebung sinnvoll und geboten. Der Erfolg der Überarbeitung des Ordnungsrahmens wird entscheidend davon abhängen, ob die Erfahrungen aus der bisherigen Umsetzung angemessen berücksichtigt und eingearbeitet werden. Die Betreiber der Energiewirtschaft möchten zu diesem Zweck oftmals noch intensiver mit den Behörden zusammenarbeiten. Allerdings ist der administrative Aufwand, der für Betreiber mit der Erfüllung der gesetzlichen Anforderungen verbunden ist, derzeit zum Teil sehr hoch. Um die Cybersicherheit langfristig zu stärken, muss daher das Ziel sein, den legitimen Anspruch eines sicheren Betriebs kritischer Infrastrukturen auch ökonomisch effizient umsetzen zu können. //

Autoren:

Yassin Bendjebbour, Fachgebietsleiter IT-Sicherheit, Kritische Infrastrukturen, Bundesverband der Energie- und Wasserwirtschaft (BDEW) e. V.

Sarah Bremm, Abteilung Steuern, Betriebswirtschaft, Digitalisierung, Bundesverband der Energie- und Wasserwirtschaft (BDEW) e. V.

Sichere Rechenzentren als Service

Das digitale Zeitalter in der Energiewirtschaft ist schon längst angebrochen. Leistungsstarke und vor allem sichere IT-Infrastruktur ist in der heutigen Zeit für Wirtschaftsunternehmen, Gewerbetreibende und Dienstleister unverzichtbar. Immer mehr Stadtwerke suchen nach Housing-Lösungen mit direktem Zugriff auf die eigenen Serversysteme. Was macht das Auslagern der IT-Infrastruktur in Rechenzentren so attraktiv? Bei stetig wachsenden Anforderungen an die Stadtwerke/Energieversorger wächst auch die IT-Infrastruktur. Viele Unternehmen stoßen dabei raum- und datensicherheitstechnisch sowie betriebswirtschaftlich an ihre Kapazitätsgrenzen.

Einen besonderen Service bietet die Energieversorgung Filstal (EVF) in ihrem neuen nach ISO/IEC 27001 zertifizierten Datacenter: schnelle Anbindung an sichere IT-Racks. Das EVF-Datacenter im Stauferpark Göppingen mit Platz für knapp 150 IT-Racks ist eines der größten und modernsten Colocation-Rechenzentren in Baden-Württemberg. Ausgestattet mit modernster Technologie, einem zertifizierten Sicherheitskonzept und individuellen Anbindungslösungen bietet es die perfekte Infrastruktur für IT- und Serversysteme.

Die Internetanbindung erfolgt über die redundanten Glasfaserleitungen des lokalen Carriers imos. In der näheren Umgebung können sogar Dark-Fiber-Anbindungen direkt zum Kunden realisiert werden. Diese individuellen Lösungen garantieren höchste Sicherheit und maximale Performance.

Zum Sicherheitskonzept des EVF-Datacenters gehören eine mehrstufige, biometriegestützte Sicherheitskontrolle mit Videoüberwachung. Die Stromversorgung und alle relevanten Systeme sind redundant verbaut und über ein USV-System und eine Netzersatzanlage abgesichert. Ein ausfallsicheres Kühlsystem mit zusätzlicher indirekter Freiluftkühlung sorgt energieeffizient für die ideale Umgebungstemperatur.

Die Vorteile für Stadtwerke und kommunale Energieversorger liegen auf der Hand: Kleine dezentrale Rechenzentren gewährleisten kürzere »Latenzzeiten« (Reaktionszeiten) und Fixkosten für Betrieb und Abschreibungen der IT-Infrastruktur können in variable und damit flexible Kosten umgewandelt werden. Last, but not least: die kontinuierliche Suche und Realisierung von Optimierungspotenzial. Die beste Geschäftsidee ist obsolet, wenn das Businessfundament auf einer veralteten und fehleranfälligen Technologie ruht.

Für individuelle Beratung und weiter Informationen stehen Ihnen die EVF-Experten zur Verfügung unter E-Mail info@evf-datacenter.de. //

Blick aus dem Büro von …

… Gregor Rohbogner, Geschäftsführer Oxygen Technologies

Wenn ich aus meinem Fenster schaue, dann sieht man im Hintergrund die Windräder auf dem Roßkopf, einem der »Hausberge« Freiburgs. Sie stehen symbolisch für die Vision unserer Firma: eine klimaneutrale Energieversorgung. Diese wird aber nur möglich sein, wenn kleine, dezentrale Energieanlagen attraktiv bleiben, indem ein wirtschaftliches Betreiben möglich ist – sowohl für den Verbraucher als auch für den Energiedienstleister. Dazu muss die Politik dauerhaft die passenden Rahmenbedingungen schaffen. Die für die Systemstabilität notwendigen digitalen und technischen Voraussetzungen liefern bereits heute innovative Unternehmen wie wir. Nur gemeinsam mit allen Akteuren aus Politik und Energiewirtschaft lässt sich der Klimawandel noch stoppen. Ich bin mir bewusst, dass das von allen Beteiligten einen gewissen Mut erfordert, altbewährte Pfade zu verlassen und neue Wege zu gehen. Aber diese Wege werden sich lohnen.

Herausgeber: Verband für Energie- und Wasserwirtschaft (VfEW) e. V., Schützenstraße 6, 70182 Stuttgart
Redaktion: Torsten Höck (V. i. S. d. P.), Isabell Bilger, Mandy Saur
Gestaltung: Jürgen Gerhardt, XX Design Partner, Stuttgart
Druck: logo Print GmbH, Metzingen