Interview mit **Prof. Dr. Ines Zenke**, Partnerin, Becker Büttner Held

# »Stadtwerke brauchen grundsätzlich eine Cyber-Security-Awareness.«

Auch kleinere Stadtwerke geraten zunehmend ins Visier von kriminellen Hackern. Im Gespräch mit e|m|w-Redakteur Philip Akoto erklärt die Rechtsanwältin Ines Zenke von der Wirtschaftskanzlei Becker Büttner Held, warum Kommunalversorgern, die zu sorglos agieren, neben dem eigentlichen Schadensfall auch rechtliche Konsequenzen drohen können und wie sich die Risiken effektiv minimieren lassen.

Foto: © BBH

**e|m|w:**
**Frau Zenke, Ihre Kanzlei Becker Büttner Held legt ihren Schwerpunkt auf die Energie- und Infrastrukturwirtschaft. Inwiefern beschäftigen Sie sich in diesem Zusammenhang mit Cybercrime beziehungsweise Cybersicherheit?**

**Zenke:**
Die Frage zu stellen, heißt eigentlich, sie zu beantworten. Unsere modernen Infrastrukturen sind nicht nur (über)lebenswichtig für uns alle, sie sind auch immer mehr digitalisiert. Das macht sie zu einem „hochwertigen" Ziel für Cyberangriffe. Der Gesetzgeber spricht hier von „kritischer Infrastruktur" und hat für sie eigene speziellere Regeln vorgegeben, die dann auch noch sektorspezifisch konkretisiert werden. Es ist für uns daher ganz natürlich, dass wir auch diese Aspekte im Rahmen unserer ganzheitlichen Beratung abdecken – von der rechtlichen Einordnung bis zur praktischen Umsetzung durch zertifizierte Sicherheitsexperten und -expertinnen.

**e|m|w:**
**Das Bundesamt für Informationssicherheit – kurz BSI – warnt seit knapp zwei Jahren, dass die Zahl der Hackerangrif-**

**fe auf die Energiewirtschaft steigt. Wie nehmen Sie diese Entwicklung wahr?**

**Zenke:**
Die Aussagen des BSI decken sich mit unseren Wahrnehmungen. Aus unseren Gesprächen mit der Branche und unseren Mandanten ergibt sich ein sehr eindeutiges Bild: Cyberangriffe werden häufiger und Unternehmen der Daseinsvorsorge, insbesondere auch Energieversorger, werden zunehmend als Ziel von Hackerangriffen ausgesucht. Und zwar sehr bewusst, weil ihr Ausfall für das Gemeinwesen empfindliche Folgen hätte. Dabei scheint die Unternehmensgröße kaum eine Rolle zu spielen. Eine Aussage wie „Warum sollte man ausgerechnet unser Stadtwerk angreifen? Wir sind doch viel zu klein" entspricht deshalb nicht unbedingt der Logik, die hinter Cyberangriffen steckt. Dafür genügt ein Blick auf die Fälle, die öffentlich bekannt geworden sind. Grundsätzlich ist kein Unternehmen „zu klein", um nicht ein potenzielles Ziel von Hackern zu werden. Wir brauchen deshalb eine grundsätzliche Cyber-Security-Awareness.

» Jede Lücke, sei sie noch so klein, kann am Ende als Einstieg genutzt werden.«

**e|m|w:**
**Welchen Schluss sollten Stadtwerke daraus für sich ziehen?**

**Zenke:**
Cybersicherheit ist eine Leitungsaufgabe. Das ist nicht das Hobby der einen Person in der IT – es ist eine zentrale Verantwortung der Geschäftsleitung. Als solche muss sie über das Compliance-System adressiert werden. Denn am Ende wird die Geschäftsleitung – sowohl in zivilrechtlicher als auch in strafrechtlicher Hinsicht – beweisen müssen, dass im Vorfeld alles getan wurde, um entsprechende Angriffe effektiv abzuwehren und das Unternehmen zu schützen. Dazu gehören nicht nur der Einsatz von irgendeiner Firewall, sondern die Organisation von Verantwortungsketten, die Implementierung von Regeln mit regelmäßigen Tests auf Wirksamkeit und die Schulung der Mitarbeitenden.

**e|m|w:**
**Was ist am Ende das Einfallstor für Hackerangriffe – die Technik oder der Mensch?**

**Zenke:**
Die zunehmende Digitalisierung der Wirtschaft und der Gesellschaft, vor allem aber auch der hohe Vernetzungsgrad bei Energieinfrastrukturen, bringt es mit sich, dass die Ansatzpunkte für Cyberangriffe vielfältiger werden. Das hat sich durch die Corona-Pandemie sicherlich noch verstärkt: Home-Office, Home-Schooling, E-Learning erfordern digitale Plattformen und Angebote. Dadurch haben sich für Hacker neue Möglichkeiten ergeben. Ein Hackerangriff kann aber auch über

die Lieferkette eines Unternehmens oder die IT-Infrastruktur eines Stadtwerke-Dienstleisters erfolgen, sogenannte Supply Chain Attacks.

Am Ende ist es oft beides: Technik, das heißt Software-Schwachstellen in Firewalls, Betriebssystemen, Browser und der Mensch. Schauen wir uns die Methode Phishing an. Es ist zum einen die Technik, die die E-Mail nicht als potenziell schadensverursachend einstuft. Und es ist zum anderen der Mensch, der die E-Mail öffnet, den Anhang anklickt und damit ein Schadprogramm ins System lässt, das sensible Daten abgreift. 100-prozentige Sicherheit gibt es weder für die Technik noch für den Menschen. Und: Jede Lücke, sei sie noch so klein, kann am Ende als Einstieg genutzt werden. Das kann bitter werden. Eine Mandantin hat eine solche Phishing-Email zum Beispiel mal knapp 90.000 Emissionszertifikate gekostet. Beim heutigen Preis von zum Beispiel 80 Euro pro Stück ist das alles andere als lustig. Aber wenn Sie mit Leuten aus der Sicherheitsbranche sprechen, ist deren Einschätzung – es ist der Mensch. Was mich wieder zur Compliance bringt. Und der Notwendigkeit von Verantwortungsketten, Schulungen, Regeln.

**e|m|w:**
**Worauf zielen solche Angriffe?**

**Zenke:**
Das Ziel ist bei allen Angriffen gleich, nämlich Zugriff auf die Netzwerke zu erlangen, um dort weitere Schwachstellen zu analysieren und schließlich einen Zugriff auf die Server zu bekommen. Die Methoden sind unterschiedlich: Je nach Angriff werden gezielt IT-Teilsysteme sabotiert oder Daten gelöscht beziehungsweise erbeutet. Ein worst case für die Energieversorgung wäre natürlich die Korrumpierung der Netzsteuerung und damit die Gefahr, dass ein Blackout herbeigeführt wird. Damit dies nicht passiert, stellt das BSI-Gesetz an kritische Infrastrukturen besonders hohe Ansprüche bei der Cybersicherheit. Grundsätzlich gilt: Je besser Unternehmen bei der Cybersicherheit aufgestellt sind, desto souveräner werden sie mit einem Angriffsversuch umgehen können.

**e|m|w:**
**Gibt es den typischen Ablauf einer Cyberattacke, vielleicht abhängig von der Angriffsmethode?**

**Zenke:**
„Den" typischen Verlauf gibt es nach unserer Erfahrung nicht, dafür sind die Möglichkeiten zu vielfältig. Bei einem erfolgreichen Angriff mit Wiper-Malware werden Daten gelöscht. Bei Ransomware-Angriffen werden Teile des IT-Systems verschlüsselt, wodurch das Unternehmen keinen Zugriff mehr auf dieses Teilsystem hat. In der Regel folgen Erpressungsversuche und das System wird erst durch Zahlen eines Geldbetrages wieder freigeschaltet.

Im Zuge dessen kann es auch zum Diebstahl persönlicher Daten kommen, die wiederum auf dem Schwarzmarkt verkauft werden können, beispielsweise Kundendaten. Damit kann ein erheblicher Imageschaden und Vertrauensverlust einhergehen. Ziemlich schnell werden auch die Datenschutzbehörden bei den betroffenen Unternehmen vor der Tür stehen, wodurch wir wieder beim Thema Haftung sind: Denn auch hier müssen Sie beweisen, dass Sie alles dafür getan haben, dass ein solcher Fall nicht eintritt. Erst dann sind Sie aus der Haftung raus.

**e|m|w:**
**Erkannt wird ein Angriff in der Regel erst, wenn es zu spät ist. Gibt es Dinge, die Versorger im Schadensfall unbedingt beherzigen sollten?**

**Zenke:**
Zunächst muss es immer darum gehen, alles zu tun, damit ein Schadensfall erst gar nicht eintritt. Aber wichtig ist, genau für den Schadensfall auch bereits alles gedanklich durchgespielt und vorbereitet zu haben. Es sollte für verschiedene Szenarien festgelegt werden, wer kontaktiert werden muss, welche Redundanzsysteme genutzt werden, wann die Öffentlichkeit beziehungsweise die Kunden informiert werden, was aus versicherungstechnischen Gründen gemacht werden muss und so weiter. Das BSI hält hier einige Handreichungen für die Unternehmen bereit. Und wir natürlich für unsere Mandanten auch. Wichtig ist zum Beispiel auch daran zu denken, dass man als Betreiber einer kritischen Infrastruktur, wie es viele EVU und alle Netzbetreiber letztlich sind, unverzüglich dem BSI Bescheid geben muss.

**e|m|w:**
**Gibt es Erfahrungswerte, wie lange die Wiederinstandsetzung nach einem erfolgreichen Angriff dauert – wovon hängt das ab?**

**Zenke:**
Das hängt stark davon ab, welche IT-Teilsysteme betroffen sind und wie groß das Ausmaß ist. Meine Kollegen von der BBH Consulting AG – ausgewiesene Experten und Exptertinnen für die technische Seite der Cybersicherheit und auch Softwareningenieure – sagen mir, dass die Wiederinstandsetzung bei einer gravierenden Infektion leicht 12 bis 24 Monate dauern kann. Insbesondere die Dekontaminierung der Daten, die nicht kritisch, aber Compliance-relevant sind, kann teuer und umfänglich sein. Dabei geht es zum Beispiel um Dateien aus dem Archivsystem wie Dokumente, Verträge, Belege und Ähnliches.

Als 2019 das Kammergericht Berlin nach einer Cyberattacke mit der Schadsoftware „Emotet" infiziert worden war, blieb das Gericht über mehrere Monate arbeitsunfähig und musste die IT-Infrastruktur komplett neu aufsetzen. Das lag, so war zu lesen, daran, dass die IT-Infrastruktur gar nicht in unterschiedliche Teilbereiche aufgeteilt war, so dass der Cyberangriff das gesamte System befallen konnte.

**e|m|w:**
**Welches sind die wirksamsten Schutzmaßnahmen – wie sieht eine gute Hackerprävention aus?**

**Zenke:**
Schon erwähnt, aber deswegen nicht weniger wichtig: Eine gute Hackerprävention begreift Cybersicherheit als Teil der Compliance im Unternehmen. In diesem Rahmen muss ein Regelsystem etabliert werden mit klaren Verantwortlichkeiten,

Kontrollen und Dokumentationen. Hier werden dann entsprechende Einzelmaßnahmen abgeleitet. Dazu sollten neben der gut ausgestatteten IT-Infrastruktur und moderner Software regelmäßige Schulungen für die Mitarbeitenden gehören, um eine möglichst effektive „human firewall" zu etablieren. Schon ein bewusst platzierter USB-Stick, den ein Mitarbeiter findet und mit dem PC verbindet, kann ein Einfallstor für eine Schadsoftware sein. Auch ein externer Dienstleister, der die Systeme überwacht, kann die IT-Sicherheit erhöhen, genauso wie die Teilnahme an Lernlaboren, in denen Krisensimulationen durchgespielt werden.

**e|m|w:**
**Gibt es Anlaufstellen, an die Stadtwerke sich wenden können, wenn sie ihre Strategie dazu aufsetzen?**

**Zenke:**
Ja. Eine Präventionsplattform zur Abwehr von Cyberangriffen ist beispielsweise „G4C" – das German Competence Centre against Cybercrime e. V. Der gemeinnützige Verein versteht sich als Kompetenzzentrum und Frühwarnsystem für Cyberkriminalität, dessen Ziel es ist, eine neue Qualität an Präventionsmöglichkeiten zu schaffen. Die Leute sind gut da. Und zu den Kooperationspartnern gehört neben dem Bundeskriminalamt und dem BSI auch BBH.

**e|m|w:**
**Wie steht es um die Aufklärung – wie erfolgreich sind Ermittlungsbehörden allgemein im Kampf gegen Cybercrime?**

**Zenke:**
Laut den Berichten des BKA gab es im Jahr 2020 108.000 Straftaten im Bereich Cyberkriminalität. Das sind circa acht Prozent mehr als im Vorjahr. Wir können davon ausgehen, dass sich dieser Trend für 2021 und 2022 fortsetzen wird. Wir müssen uns allerdings bewusst sein, dass wir es in diesem Bereich mit einer sehr hohen Dunkelziffer zu tun haben, weil das betroffene Unternehmen die Straftat entweder nicht bemerkt oder sich bewusst entschieden hat, die Straftat nicht zur Anzeige zu bringen – zum Beispiel, um einen Imageschaden zu vermeiden oder bei Erpressungsfällen.

Gehen wir von den offiziellen Zahlen aus, liegt die Aufklärungsquote im Bereich Cyberkriminalität in den letzten Jahren bei circa 32 Prozent – deutlich niedriger als die Gesamtaufklärungsquote bei Straftaten von 58 Prozent. Das liegt daran, dass die Täter im Prinzip von jedem Fleck der Erde einen Cyberangriff generieren können und die Spurensuche im digitalen Umfeld extrem schwierig ist. Das erschwert die Aufklärung enorm. Hinzu kommt, dass die Professionalisierung der Täter und die Komplexität der Angriffe steigen.

**e|m|w:**
**Frau Zenke, vielen Dank für das Interview.**

**PROF. DR. INES ZENKE**

**Jahrgang 1971**

- 1990–1995 Studium der Rechtswissenschaften, Humboldt-Universität zu Berlin
- seit 1995 bei Becker Büttner Held (BBH)
- seit 1999 Rechtsanwältin und seit 2011 Fachanwältin für Verwaltungsrecht
- seit 2002 Partnerin bei BBH
- ines.zenke@bbh-online.de