ZfK Zeitung für kommunale Wirtschaft

IT

ZfK+ "Cyberkriminalität hat sich zu einem lukrativen Geschäftsmodell entwickelt"

Nehmen Cyberangriffe auf Unternehmen der Daseinsvorsorge zu? Ist die Wasserwirtschaft gefährdeter als andere Branchen im KRITIS-Bereich? Ein Gespräch mit dem IT-Sicherheitsexperten Tim Philipp Schäfers von OEDIV Oetker Daten und Informationsverarbeitung.

07.02.2022

Tim Philipp Schäfers ist Whitehat-Hacker und IT-Sicherheitsexperte. Er berät Organisationen in den Bereichen IT- und Informationssicherheit und tritt in Funk/Fernsehen auf. Zudem ist er Mitgründer und Mitbetreiber des Webprojektes "Internetwache.org". Darüber hinaus ist Schäfers Dozent für IT-Security & Risikomanagement und Technical Security an der FHDW in Paderborn und Bielefeld. Schäfers konnte gravierende Sicherheitslücken bei Unternehmen wie PayPal, Facebook, Google, der deutschen Telekom und vielen weiteren Unternehmen verantwortlich aufdecken.

Bild: © Thomas Zajada/AdobeStock

Herr Schäfers, Sie sind ein sogenannter White-Hacker, also jemand der im Auftrag von Unternehmen Schwachstellen in der IT findet. Sie waren mit dabei, als sich 2018 IT-Sicherheitsexperten in die Prozessleitsysteme von sieben Wasserwerken hacken konnten. Sind Wasserwerke gefährderter als andere KRITIS-Infrastrukturen?

Tim Philipp Schäfers, Information Governance/Cyber Security Consultant der OEDIV Oetker Daten- und Informationsverarbeitung KG: Als ich 2018 gemeinsam mit meinem Freund Sebastian Neef dafür sensibilisieren konnte, wie einfach es ist, die digitalen Steuerungssysteme mehrerer deutscher Wasserwerke, Blockheizkraftwerke und Biogasanlagen nicht nur auszuspähen, sondern auch gezielt zu manipulieren, waren wir schockiert, wie problemlos kriminelle Hacker sie mit Standardmethoden hätten sabotieren können. Seitens der Betreiber war es schon gefährlicher Leichtsinn, dass ein Mausklick unsererseits ausgereicht hätte, um uns selbst zu Administratoren der gesamten Anlage zu machen. Glücklicherweise haben alle Beteiligten dieses deutliche Warnsignal verstanden und entsprechende Sicherheitsmaßnahmen verankert. Dennoch kann man nicht pauschal sagen, dass Wasserwerke und Kläranlagen gefährdeter sind, zumal sie zum Beispiel. durch regelmäßige Probenentnahmen und zusätzliche technische Kontrollen mehrfach abgesichert sind. Fakt ist allerdings auch, dass der Energiebereich einer stärkeren staatlichen Aufsicht unterliegt und damit per se mehr markterprobte Schutzmechanismen

etabliert hat. Brandgefährlich wird es, wenn Angriffe in größerem Umfang auf die KRITIS-Gesamtstruktur abzielen.

Auch die Steuerung von Windkraftanlagen ist schon übernommen worden. Ist das wirklich eine Gefahr für die Stromversorgung?
Das Beispiel Windkraftanlagen zeigt recht deutlich, wie wichtig ein effektives IT Asset Management (ITAM) für mehr Sicherheit, Transparenz und Produktivität ist. So haben etwa Windkraftanlagen mit 10 bis 15 Jahren eine deutlich höhere Lebensdauer als die zugrundeliegenden Betriebssysteme, die bereits nach acht bis zehn Jahren ihr End of Life erreichen. Diese Diskrepanz birgt gefährliche Sicherheitslücken in sich, die zunehmend auch den Gesetzgeber auf den Plan rufen werden. Ein IT Asset Management ist eine wichtige Grundlage, wenn man besser bewerten möchte, welche Komponenten im Einsatz sind, welchen Sicherheitsstand diese haben und wann diese ggfs. durch neue Komponenten abgelöst werden müssen.

Realistisch betrachtet, stellen Angriffe auf einzelne Anlagen jedoch noch keine ernst zu nehmende Bedrohung für das Gemeinwohl dar. Erst wenn großflächig strukturelle Sicherheitslücken ausgenutzt werden, die Reaktionsfähigkeit der Systeme nicht mehr gewährleistet ist oder wie kürzlich im Falle von Log4j zu viele Softwarekomponenten angegriffen werden, entwickelt sich ein kleines, noch beherrschbares Feuer zu einem unkontrollierbaren, nicht mehr zu löschenden Großbrand.

Stichwort Log4j: Wie betroffen war die Energie- und Wasserwirtschaft von dieser Schwachstelle? Gab es deswegen Ausfälle in der Branche?
Log4j war für uns im Dezember 2021 branchenübergreifend eine große Herausforderung, die glücklicherweise verhältnismäßig schnell ohne größere Systemausfälle in Griff bekommen wurde. Bei der Ursachenbekämpfung wurde die Verantwortung nicht selten zwischen den Herstellern der Systeme, deren Betreibern und den Systemintegratoren hin- und hergeschoben. Der Umgang mit Log4j hat gezeigt, wie wichtig es ist, die zu schützenden Bereiche und dazugehörigen Verantwortlichkeiten unmissverständlich vorab zu definieren und deren Umsetzung systematisch zu kontrollieren. Während viele Unternehmen durchaus vorbildlich im Bereich der Prävention dastehen – etwa durch Firewalls, Antivirusprogramme –, wird nicht selten der mindestens ebenso wichtige Bereich der Reaktion sträflich vernachlässigt. Ein krisensicheres Business Continuity Management ist daher dringlich erforderlich, damit der reguläre Betrieb nach störungsbedingter Unterbrechung in kürzestmöglicher Zeit wiederaufgenommen werden kann. So lassen sich Schäden reduzieren und existentielle Bedrohungen vermeiden, die beispielsweise durch unterbrochene Lieferketten schnell auch für weitere Unternehmen zu einem Flächenbrand werden können.

Wie bewerten Sie allgemein die IT-Sicherheit bei der Energie- und Wasserversorgung?
Betrachten wir die Kommunal-, Energie- und Wasserwirtschaft als Ganzes, bietet sich ein durchaus heterogenes Bild. Nur wenige, vorwiegend kleinere Strukturen verlassen sich auch heute noch mit vorhandener Alttechnik und einem von verschiedenen Abteilungen gehäkelten Flickenteppich darauf, dass ein Cyberangriff sie schon nicht treffen werde. Die Mehrzahl ist bereits stark sensibilisiert für die unterschiedlichen Facetten der Cyberkriminalität und entsprechend gut – sowohl personell als auch technologisch – aufgestellt. Jede erfolgreich getroffene Maßnahme bildet hier für sich genommen ein eigenes Schutzniveau. So ist im Optimalfall erst dann, wenn die Angreifer mehrere dieser Schutzwälle durchbrechen können, der Punkt erreicht, an dem die IT-Sicherheit nicht mehr gewährleistet werden kann.

Man hat das Gefühl, Angriffe auf Stadtwerke und Energieversorger nehmen zu. Sehen Sie das ähnlich und woran liegt das? Entdecken Hacker gerade die Unternehmen der Daseinsvorsorge für sich?
Grundsätzlich teile ich Ihre Einschätzung. Dennoch sollte man den Gesamtzusammenhang nicht aus dem Blick verlieren, da vermehrt alle Branchen, nicht nur die kritischen Infrastrukturen von Cyberangriffen betroffen sind. Laut Bitkom entsteht der deutschen Wirtschaft ganz allgemein durch Diebstahl, Spionage und Sabotage jährlich ein Gesamtschaden von 223 Mrd. EUR – Tendenz steigend. Neun von zehn Unternehmen sind 2020/2021 Opfer von Cyberattacken geworden. Es geht also längst nicht mehr darum, ob ein Cyberangriff stattfinden wird, sondern wann dies passiert und wie schnell dieser erkannt und erfolgreich abgewehrt werden kann.

Zunehmend nutzen die Angreifer Ransomware auch für neue Formen der Cyber-Erpressung und drohen ihren Opfern nicht nur mit der Vernichtung bzw. Verschlüsselung, sondern auch mit der Veröffentlichung und missbräuchlichen Nutzung von Identitätsdaten. Nicht selten wird die Höhe des Lösegeldes dabei ganz individuell an Unternehmensgröße und -bedeutung –

etwa im Rahmen der kritischen Infrastrukturen – festgemacht.

Dass nahezu alle Branchen zunehmend von Cyberkriminalität betroffen sind, hat grundsätzlich zwei Ursachen – die immer stärkere Digitalisierung unserer Gesellschaft – mit Einfallstoren wie Remote Working, Smart Home und Smart Governance – sowie die wachsende Professionalisierung der Tätergruppen – bis hin zu einer ausgeklügelten Arbeitsteilung und „Industrialisierung" in weltweit agierenden kriminellen Netzwerken, die es den Ermittlungsbehörden zunehmend schwermachen, personell und technologisch hinterherzukommen. Die Cyberkriminalität hat sich zu einem lukrativen Geschäftsmodell entwickelt, das gerade in Entwicklungs- und Schwellenländern topausgebildete IT-Spezialisten auf die dunkle Seite der Macht zieht.

Hinzu kommt auf internationaler Ebene ein weiterer gefährlicher Trend: Zwischen- und innerstaatliche Konflikte werden zunehmend auch auf den Schlachtfeldern des Cyberspace ausgetragen, wobei die Grenzen zwischen privaten und staatlichen Hackergruppen immer weiter verschwimmen. Das Spektrum hybrider Kriegsführung und staatlich gesteuerter Cyberangriffe reicht dabei von klassischer Spionage hin zu Sabotage und gezielter Aushöhlung demokratischer Strukturen durch Lieferengpässe, Desinformation, Aufstachelung und Verunsicherung einzelner Bevölkerungsgruppen. Hier werden die kritischen Infrastrukturen aufgrund ihrer besonderen Vulnerabilität als Rückgrat der Gesellschaft immer „attraktiver" für entsprechende, systematische Angriffe.

> *"Häufig lassen sich mit anderen Unternehmen Synergien in der Zusammenarbeit nutzen, etwa durch den Aufbau gemeinsamer IT-Sicherheitsstrukturen. Das spart eigene Personal-, Anschaffungs- und Administrationskosten."*
>
> **Tim Philipp Schäfers**
> OEDIV KG

Aktuell wird im Zusammenhang mit Corona viel von der Erstellung geeigneter Notfall- und Katastrophenpläne gesprochen? Welch Stellenwert wird in diesem Zusammenhang der ebenfalls vulnerablen IT-Infrastruktur beigemessen oder wird der Blickwinkel eher verkürzt auf krankheitsbedingte Personalausfälle etc. gerichtet?
Vor dem Hintergrund der Pandemie signalisieren viele kommunale Unternehmen, Wasser- und Energieversorger, dass sie geeignete Notfall- und Katastrophenpläne schon lange in der Schublade haben. Für Unternehmen der kritischen Infrastruktur ist es allerdings empfehlenswert, ihre Krisenmanagement-Planung nicht nur als schriftliche Dokumentation vorzuhalten, sondern sie kontinuierlich praxisnah zu erproben und mögliche Schwachstellen systematisch auszubessern. Auch hier ist wieder eine ganzheitliche Herangehensweise gefragt, da die Gesamtsicht beispielsweise auch Aspekte der internen und externen Kommunikation umfasst – bei der Information der MitarbeiterInnen, juristischen Bewertungen, der Beantwortung von Ad-hoc-Presseanfragen oder im Umgang mit Aufsichtsbehörden, Polizei und weiteren Stakeholdern. Es ist sinnvoll, diverse Krisenszenarien im Vorfeld ehrlich durchzuspielen und entsprechend abzusichern.

IT-Sicherheit ist Chefsache: Wie wichtig ist es, einen CISO im Unternehmen zu haben, und wie sollen sich das kleinere Unternehmen leisten können?
IT-Sicherheit sollte ganzheitlich betrachtet werden und grundsätzlich Chefsache sein. Oftmals kommt aber in kleinen Unternehmen die Entwicklung einer einheitlichen, konsolidierten IT- und IT-Sicherheitsstrategie einem Kraftakt gleich. Hier hat es sich in der Praxis bewährt, analog zum Datenschutz und unter klarer Definition der Verantwortlichkeiten einen externen IT-Informationssicherheitsbeauftragten (ISB) hinzuzuziehen – und das nicht erst im Rahmen einer geplanten Zertifizierung gemäß ISO 27001 und IT-Grundschutz. Auch lassen sich häufig mit anderen Unternehmen Synergien in der Zusammenarbeit nutzen, etwa durch den Aufbau gemeinsamer IT-Sicherheitsstrukturen. Das spart eigene Personal-, Anschaffungs- und Administrationskosten.

Der Faktor Mensch spielt auch immer eine große Rolle: Ist es nicht deprimierend, dass egal, wie gut die Technik ist, der Mensch immer dafür sorgen kann, dass Angreifer trotzdem ein Einfallstor finden?
Fakt ist, dass die Digitalisierung unserer Gesellschaft nicht mehr aufzuhalten ist. Unsere Lebens- und Arbeitswelten sind zunehmend smart und digital vernetzt. Ich empfinde es daher gar nicht als so deprimierend, dass die technischen Möglichkeiten und damit auch die Einfallstore für Angreifer größer werden. Vielmehr ist es doch eine spannende Herausforderung, eine lebendige, offene Unternehmenskultur zu schaffen, in der kontinuierlich hinzugelernt wird.

Ein unterschätzter Risikofaktor sind eigene MitarbeiterInnen, die zum Beispiel gekündigut wurden und auf Rache sinnen, oder die vielen kleinen Nachlässigkeiten im Arbeitsalltag, wenn es etwa um Passwörter geht. Wie kann man hier vorbeugen?

IT-Sicherheit ist ein kontinuierlicher Prozess, bei dem der Faktor Mensch den Unterschied macht. Kontinuierlich up to date zu bleiben und für Sicherheitslücken sensibilisiert zu sein ist daher auch, aber nicht nur, Aufgabe gezielter Awareness-Trainings. Dabei kommt die Bedrohung nicht immer nur von externen Angreifern, sondern auch von eigenen MitarbeiterInnen. Durch eine sorgfältige Personalauswahl, eine offene, wertschätzende Unternehmenskultur und die gezielte Nutzung effektiver Security-Information- und Event-Management-Systeme (SIEM) kann maliziösem Verhalten Einzelner erfolgreich entgegengesteuert werden.

Die Fragen stellten Anke Schäfer und Stephanie Gust

Quelle: Gust, Stefanie: "Cyberkriminalität hat sich zu einem lukrativen Geschäftsmodell entwickelt", in: ew-Magazin 3/2022, S. 64-67