media IT-SicherheitsForum informiert

Kritische Infrastruktur – Wie sicher sind unsere Lebensadern?

Die zunehmende Digitalisierung aller Lebensbereiche macht diese auch mehr und mehr verwundbar. Energieversorger und Krankenhäuser, Häfen, Geldinstitute, Versicherungsgesellschaften und nicht zuletzt auch die Wirtschaft sind zur Zielscheibe von Hackern geworden, die die Computernetzwerke aus kriminellen oder politischen Gründen lahmzulegen oder zu übernehmen versuchen.

Grund genug für das IT-SicherheitsForum des Vereins media Lahn-Dill, sich unter dem Titel „Kritische Infrastruktur – Wie sicher sind unsere Lebensadern?“ mit dem ebenso spannenden wie beunruhigenden Thema auseinanderzusetzen. Die Entscheidung dafür sei schon lange, bevor die Gießener Universität Ende vergangenen Jahres wochenlang durch einen Hackerangriff lahmgelegt war, getroffen worden, erklärte Christian Bernhard als Vorstandsvorsitzender des media Lahn-Dill e. V. in seiner Begrüßung: „Wir sind mit den richtigen Themen unterwegs und am Puls der Zeit“, sagte er. Auch Sabine Fremerey-Warnecke als Vizepräsidentin der IHK Lahn-Dill dankte den Organisatoren des SicherheitsForums in ihrem Grußwort dafür, sich des wichtigen Themas anzunehmen: Mitunter halte die Sicherheit nicht Schritt mit den Innovationen der Industrie- und Wirtschaftsbetriebe. „Sensibilisieren, aber keine Angst verbreiten“ - das sei, wie von Christian Bernhard als Prämisse ausgelobt, das richtige Vorgehen.

Dafür schuf media Lahn-Dill-Vorstandsmitglied Michael Wiesner in Vertretung des erkrankten Referenten mit einem informativen Überblick die Grundlagen, als er die neun Sektoren vorstellte, denen das besondere Augenmerk gilt. Allen voran seien der Energiesektor mit Strom-, Gas-, Kraftstoff-, Heizöl- und Fernwärmeversorgung sowie der Bereich IT, Cloud-Datenspeicherung und Kommunikation zu nennen, sagte der Informationssicherheitsbeauftragte. Weitere besonders schützenswerte Sektoren seien Trink- und Abwasser, Ernährung, das Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur. Auf die Bereiche Gesundheit und Transport/Verkehr ging Wiesner etwas ausführlicher ein: So gebe es in den Krankenhäusern zwar ein Notstromaggregat, aber wenn ein Trojaner das Computersystem lahmlege, komme das Personal weder an Krankenblätter noch an Arzneimittelpläne. Und ein Ausfall der Güter- und Personenbeförderung per Eisenbahn ziehe immensen volkswirtschaftlichen Schaden nach sich, machte Wiesner bewusst.

Mittlerweile sei wegen der immer komplexer werdenden Systeme auf der „Fallback“, das Zurückgreifen auf analoge Technik nicht mehr möglich. „Wir machen uns vollkommen abhängig von IT“, mahnte der Experte. In seiner beruflichen Praxis erlebe er Computersysteme, die ohne Wartungsintervalle sozusagen Tag und Nacht laufen, eben


Foto: Klaus Kordesch

Die richtigen Themen zur richtigen Zeit: IHK-Vizepräsidentin Sabine Fremerey-Warnecke dankte den Veranstaltern des SicherheitsForums in ihrem Grußwort für das Sensibilisieren in Sachen IT-Sicherheit.

wie das Verbinden klassischer Automatisierungstechnik mit dem Internet zum Beispiel für die Fernwartung, obwohl sie gar nicht dafür konstruiert worden sei: „Das bietet eine große Angriffsfläche und bedeutet einfache Angriffsmöglichkeiten mit einem enormen Schadenspotential!“, warnte Wiesner: „Da geht Funktionalität vor Sicherheit, das wird uns noch auf die Füße fallen!“ Die derzeitigen Angriffe auf die Infrastrukturen wertete der Experte größtenteils als Testläufe der Hacker, wenn es nicht um das Erpressen von Geld gehe. Zugleich bezeichnete er die vorhandenen Kapazitäten beispielsweise des Bundesamts für Sicherheit in der Informationstechnologie (BSI) als nicht ausreichend.

Dies vor allem für die Zivilbevölkerung zu ändern, ist eine der Aufgaben des Bundesamts Bevölkerungsschutz und Katastrophenhilfe (BBK) in Bonn. Referentin Nicola Rupp umriss die Inhalte des Integrierten Risikomanagements für den Schutz der Bevölkerung nach DIN SPEC 91390, das auf gründlichen Analysen kritischer Dienstleistungen, Prozesse und Anlagen sowie einem intensiven Austausch aller beteiligten Behörden und Unternehmen basiert. Die Zusammenarbeit sei vor allem zwischen den Betreibern Kritischer Infrastrukturen und Staatlichen Akteuren erforderlich, betonte Rupp. Sie empfahl, beim Erstellen der Notfallkonzepte praktisch zu denken: Beim

Das IT-SicherheitsForum des Vereins media Lahn-Dill beschäftigte sich Anfang März mit dem Thema „Kritische Infrastruktur – Wie sicher sind unsere Lebensadern?“ Christian Bernhard als Vorstandsvorsitzender des media Lahn-Dill e.V. begrüßte die Gäste in der Wetzlarer IHK-Geschäftsstelle.

Foto: Klaus Kordesch

Mit (v.l.) Marco Müller, Michael Wiesner und Nicola Rupp konnte Christian Bernhard als Vorstandsvorsitzender des media Lahn-Dill e.V. erneut hochkarätige Experten zum media IT-Sicherheitsforum begrüßen.

Ermitteln des Strombedarfs in einer mehrtägigen Krise beispielsweise seien so auch Kaffeemaschinen und Lademöglichkeiten für die Handys der Mitarbeiter zu berücksichtigen, regte sie an. Zudem sei es wichtig, die Szenarien auch regelmäßig zu üben und die für den Krisenfall vorgehaltenen Anlagen zu warten.

Was ein Energieversorger wie die EnergieNetz Mitte GmbH als Tochtergesellschaft der EAM tut, um die Stromversorgung zu gewährleisten, schilderte deren Prokurist Marco Müller. Nicht nur Cyberattacken, sondern auch Unwetterereignisse bedrohten das Netz, so dass heute schon mehr als 90 Prozent der Versorgungskabel unterirdisch verlegt seien, erläuterte Müller. Störungen in der Energieversorgung seien weniger durch externe Einflüsse verursacht, sondern durch den Umstand, dass die Höchst- und Hochspannungsnetze, die regionalen Mittelspannungsnetze und die lokalen Niederspannungs-Verteilnetze auf die Erzeuger „von gestern" hin geplant und eigentlich nicht für die Erzeugung „von unten" ausgelegt seien, also den von Photovoltaik, Biogasanlagen und Blockheizkraftwerken produzierten Strom: „Die Schwierigkeit ist, immer genau so viel Strom zu produzieren wie gerade verbraucht wird", machte Müller das Problem deutlich.

Eine zusätzliche technische Herausforderung stelle die wachsende E-Mobilität dar; zumal, wenn bis 2050 auf erneuerbare Energien umgestellt werde: „Dann brauchen wir eine `Flexibilisierung der Nachfrage´, das heißt, es kann nicht jeder sein Fahrzeug dann laden, wann er möchte", sagte Müller. Wenn am Nachmittag nach der Arbeit zuhause alle E-Fahrzeuge geladen werden sollten, könne das nicht funktionieren. Eine weitere Unwägbarkeit stelle das Internet dar, das schon heute – wäre es ein Staat – den sechstgrößten Stromverbrauch der Erde habe, vor allem für die Kühlung der Rechner. Und der Trend gehe hin zu sogenannten Hyperscale-Rechenzentren, die so groß wie mehrere Fußballfelder sein könnten: „Die Energiewende ist eine große Baustelle", fasste Müller zusammen.

Abschließend stellte Holger Cyriax der Runde das „Netzwerk IT-Sicherheit" des Vereins media Lahn-Dill vor und lud die IT-Verantwortlichen herzlich zu den Treffen eine Praxisplattform für die Praktiker" ein.

Klaus Kordesch

Ihr IHK-Ansprechpartner:
Christian Bernhard
Tel.: 06441 9448-1700
wz@media-ldk.de

Wie sicher ist unsere Stromversorgung? Diese Frage beantwortete beim SicherheitsForum Marco Müller als Prokurist der EnergieNetz Mitte GmbH, einer Tochtergesellschaft der EAM.

„Einfache Angriffsmöglichkeiten mit einem enormen Schadenspotential": Der Informationssicherheitsbeauftragte Michael Wiesner warnte vor veralteten und schlecht gewarteten Anlagen, die fast ungeschützt mit dem Internet verbunden sind.

Nicola Rupp vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) in Bonn riet zu einer engen Vernetzung von staatlichen Akteuren und Betreibern, welche etwa im Rahmen eines integrierten Risikomanagements nach DIN SPEC 91390 umsetzbar ist.