Wie steht es um das IT-Sicherheitsniveau der deutschen Energieversorger

Interview mit Prof. Bretschneider und Prof. Lässig

Am 12. Mai 2017 hat mit der sogenannten WannaCry-Attacke ein Hackerangriff von bislang beispielslosem Ausmaß stattgefunden. Waren nach Ihren Kenntnissen davon auch Energieversorger in Deutschland betroffen?

Prof. Bretschneider: Ich habe direkt am Folgetag mit einigen Energieversorgern gesprochen, die nicht Opfer dieses Angriffs waren – weil insbesondere im Bereich der Netzleitstellen hohe Sicherheitsrichtlinien gelten und eingehalten werden.

Prof. Lässig: Wenn wir uns die Auswirkungen im britischen Gesundheitssystem anschauen, dann sind wir in Deutschland glimpflich davongekommen. Ähnliche Ransomware-Angriffe hatten wir ja in Deutschland in der Vergangenheit auch schon. Mittlerweile können wir davon ausgehen, dass zumindest aus diesem Angriff keine Folgeschäden mehr entstehen. Aber es ist zu erwarten, dass sich Attacken mit ähnlichem Muster wiederholen. Deshalb müssen wir WannaCry als Warnschuss verstehen.

Wie hoch ist das Gefahrenpotenzial, dass Kritische Infrastrukturen in Deutschland von einer solchen Cyberattacke lahmgelegt werden?

Prof. Bretschneider: Die Gefahr ist real. Deshalb gibt es das IT-Sicherheitsgesetz, das Unternehmen dazu anhält, diese Infrastrukturen mit hoher Priorität zu schützen. Energieversorger und Netzbetreiber sind für Cyberrisiken bereits seit einigen Jahren sensibilisiert. Allerdings steigt mit der Dezentralisierung der Energieversorgung der Vernetzungsbedarf, was wiederum die Zahl der Einfallstore für Cyberangriffe erhöht. Je komplexer die Netze werden, desto größer ist die Gefahr, dass Schwachstellen auftreten, die Cyberkriminelle ausnutzen. Insbesondere die zunehmende digitale Vernetzung von bislang getrennten Bereichen, zum Beispiel zum Einspeisemanagement Erneuerbarer Energien oder zur Kopplung virtueller Kraftwerke, erfordert eine hohe Awareness von allen Akteuren. Sonst besteht die Gefahr, dass sich ein Virus von einem einzigen Backoffice-PC unbemerkt im ganzen System ausbreitet. Das ist eine Problematik, die wir unter anderem mit unserem Lernlabor Cybersicherheit adressieren.

Prof. Lässig: Die Herausforderung besteht darin, dass IT-Sicherheit eine Querschnittseigenschaft ist, die von einer Vielzahl von Faktoren beeinflusst wird, von systeminternen Kriterien über die Anwender bis hin zur Gesetzeslage. Diese Kette ist nur so stark wie ihr schwächstes Glied. Eine Vielzahl an Maßnahmen kann daher trotzdem nutzlos sein, wenn es eine Schwachstelle gibt. Daher empfehlen wir einen prozessorientierten Ansatz, den wir in unserem Kursprogramm vermitteln, von der Einführung bis zur Umsetzung eines IT-Sicherheitsmanagements. Dabei geht es zum einen um grundlegende Normen und Standards, die umgesetzt werden müssen, aber auch um die Notwendigkeit, die eingeführten Maßnahmen kontinuierlich zu aktualisieren, um sich gegen neue Angriffsmuster zu wappnen.

Aktuelle Statistiken belegen, dass sich die Situation im Zuge der Digitalisierung erheblich verschärft hat. Das zeigen nicht nur erfolgreiche Angriffe etwa auf Energieanlagen in der Ukraine oder die Manipulation eines Hochofens in einem Stahlwerk in Deutschland, über die das BSI 2014 berichtet hat, sondern auch die Polizeiliche Kriminalstatistik (Beispiel

Sächsische PKS): Im Vergleich zu rund 2.800 Kfz-Diebstählen im Jahr 2016 ist die Cyberkriminalität mit über 10.000 Vorfällen hier absoluter Spitzenreiter – wobei die Dunkelziffer noch um ein Vielfaches höher ist. Ein interessanter Aspekt sind dabei die entstehenden Kosten. Für KMU entstehen bei einem erfolgreichen Angriff beispielsweise Kosten von durchschnittlich 36.000 Euro. Bezogen auf Kritische Infrastrukturen, kann man davon ausgehen, dass ein Stromausfall pro Person und Stunde in Deutschland circa 10 Euro kostet. Ein eintägiger Stromausfall summiert sich also auf 19 Milliarden Euro – das sind Größenordnungen, die die Relevanz sicherer Infrastrukturen verdeutlichen.

Warum setzt die Energiebranche auf die digitale Vernetzung und Smart Grids, wenn sie dadurch mehr Einfallstore für Cyberattacken öffnet?

Prof. Bretschneider: Laut BDI kann Europa bis 2025 durch eine vernetzte Produktion und digitale Geschäftsmodelle einen Zuwachs von 1,25 Billionen Euro an industrieller Bruttowertschöpfung erzielen [1]. Um dieses Potenzial zu erschließen, sind IT-Sicherheitslösungen wichtig.

Prof. Lässig: Kritische Infrastrukturen sind auch ein zentraler Treiber für die Weiterentwicklung aktueller Sicherheitsansätze, etwa der verstärkte Einsatz von datengetriebenen Methoden und Maschinellem Lernen, um Angriffe möglichst schnell zu erkennen und damit rechtzeitig Gegenmaßnahmen einleiten zu können, oder die Umsetzung von Konzepten wie Security by Design. Das IT-Sicherheitsgesetz hat hier durchaus positive Impulse gesetzt. Wichtig sind eine kontinuierliche Weiterentwicklung und Kalibrierung der Konzepte anhand aktueller Entwicklungen und Herausforderungen.

Wie schätzen Sie die Sicherheit der Energieversorger in Deutschland aktuell ein?

Prof. Bretschneider: Wir haben hierzulande eine sehr zuverlässige Energieversorgung und bewegen uns in puncto IT-Sicherheit auf äußerst hohem Niveau. Die niedrigen Ausfallzeiten belegen die hervorragende Arbeit der Unternehmen. In diesem Zusammenhang nehmen sie auch die Anforderungen des IT-Sicherheitsgesetzes äußerst ernst und sind bemüht, diese umfänglich zu erfüllen. Absoluter Schutz ist dennoch nicht gegeben, da sich die Angriffsmuster kontinuierlich verändern. Das IT-Sicherheitsmanagement muss daher ständig dynamisch angepasst werden.

Wo sehen Sie Handlungsbedarf, vor allem bezüglich Kompetenzaufbau, den Sie durch Ihre Schulungsangebote vorantreiben?

Prof. Bretschneider: Wir adressieren vom CEO über Planer und Operator von Energienetzen, um IT-Sicherheitsmanagement ganzheitlich in den Unternehmen zu verankern. Wir vermitteln aktuelles Know-how, das sich an den gegenwärtigen Anforderungen orientiert. Und wir untersuchen Fragestellungen, wo die Risiken liegen und welche Analyseinstrumente geeignet sind.

Prof. Lässig: Für die Etablierung wirksamer Sicherheitsarchitekturen ist eine Top-Down-Vorgehensweise anzuraten. Deshalb sprechen wir mit unseren Schulungen die Mitarbeiter aller Hierarchieebenen, wie schon zuvor skizziert, an, damit letztlich auch eine Unternehmenskultur entsteht, die IT-Sicherheit als festen Bestandteil beinhaltet. Ein Alleinstellungsmerkmal unserer Weiterbildung ist die Tatsache, dass die Kompetenzen aus den Bereichen Energie und Wasser, IT-Systeme sowie die Aus- und Weiterbildungskompetenz der Fraunhofer Academy zu Kursen kombiniert werden, die neben

der theoretischen Basis auch praktische Skills vermitteln, indem wir Angriffsszenarien und Verteidigungsstrategien in unseren Lernlaboren real nachbilden.