Mitteilungsblatt 09.12.2022

Kritische Infrastrukturen werden meist über das Internet angegriffen

Noch letztes Jahr war das Thema eher ein theoretisches: Die Gas-Heizung sorgte fast sorgenfrei für wohlige Wärme und die Bahn kam zumindest irgendwann. Spätestens nach den Lecks in den beiden Northstream-Gas-Pipelines und der Sabotage an den Kommunikationskabeln der Deutschen Bahn stellen sich nun die Fragen: Wie ist es um die Sicherheit unserer kritischen Infrastruktur bestellt? Was sind überhaupt kritische Infrastrukturen? Welche Gefahren und Risiken bestehen und wie können die kritischen Infrastrukturen geschützt werden?
Diesen Fragen gingen Herr Prof. Dr. Dr. h. c. Günter Müller, Professor für Telematik an der Universität Freiburg, und Herr Patrick Klein, Cyber Security Governance Spezialist im Bereich kritischer Infrastrukturen, jüngst im Rahmen einer Liberalen Runde der FDP Hirschberg vor ca. 15 Zuhörern nach.

Klein erläuterte anhand der einschlägigen Rechtsgrundlagen, dass
Kritische Infrastrukturen (KRITIS) alle Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen sind, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. Unterteilt werden die kritischen Infrastrukturen in zehn Sektoren wie z.B. IT und TK, Energie, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen. Anhand von Beispielen machte Klein deutlich, dass etwa ein Zusammenbruch der Energieversorgung moderne Kommunikation unmöglich machen und längere Stromausfälle auch die medizinische Versorgung lahm legen würde.

Prof. Müller führte aus, dass das Internet eine zentrale Rolle spiele. So seien aktuell 94% aller Angriffe auf kritische Infrastrukturen in den USA extern über das Internet verübt worden. In Deutschland seien 2021 ca. 144 Mio. IT-Angriffe erfasst worden. Taiwan müsse gar mit 5 Mio. IT-Angriffen täglich zurecht kommen und die Dunkelziffer liege wohl auch in Deutschland erheblich höher. Laut dem Branchenverband Bitkom betrug der Schaden durch Angriffe auf kritische Infrastrukturen allein in Deutschland 2021 ca. 223 Mill. € – Tendenz steigend.

Als mögliche Lösungen griff Prof. Müller fünf Optionen auf. Eine Option, die den chinesischen Weg beschreibe, sei die (nicht nur digitale) Totalüberwachung. Das sei das Ende aller Freiheit. Option zwei wäre die Einrichtung von Redundanzen, also die doppelte Vorhaltung von kritischen Infrastrukturen, etwa durch Standy By, Backup oder Cloud, was enorme Kosten verursachen und Ressourcen binden würde. Eine dritte Variante wären Prognosen und Monitoring – quasi eine „Light-Überwachung“.

Einen vierten Ansatzpunkt stelle die an und für sich gute Idee der Reduzierung der Gewinne der Angreifer dar. Dies müsste über die Schließung des Darknets und die Einschränkung des Internets erfolgen und sein faktisch kaum möglich. Ferner dürfe man auch nicht vergessen, dass das Internet durchaus Wohlstand bringe. Schließlich bestehe eine Möglichkeit darin, kritische Infrastrukturen und Daten auch analog vorzuhalten und externe Vernetzungen – womit man wieder bei der Überwachung wäre – besser zu kontrollieren.

Einig waren sich Klein und Prof. Müller zum Schluss, dass man nicht alles zu jeder Zeit und an jedem Ort schützen könne. Ziel muss es daher im Sinne einer gesteigerten Resilienz sein, nach störenden Ereignissen die Funktionsfähigkeit kritischer Infrastrukturen zu erhalten und schnellstmöglich in den Ausgangszustand zurückkehren zu können.