Bundesamt
für Sicherheit in der
Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn

Landtag Nordrhein-Westfalen

per E-Mail

LANDTAG
NORDRHEIN-WESTFALEN
16. WAHLPERIODE

STELLUNGNAHME
16/3960

A01, A09

Dirk Häger

HAUSANSCHRIFT
Bundesamt für Sicherheit in
der Informationstechnik
Godesberger Allee 185-189
53175 Bonn

POSTANSCHRIFT
Postfach 20 03 63
53133 Bonn

TEL +49 228 99 9582-5304
FAX +49 228 99 10 9582-5304

dirk.haeger@bsi.bund.de
https://www.bsi.bund.de

Betreff: Anhörung zur Drucksache 16/11216
hier: Stellungnahme BSI

Bezug: Ihr Schreiben vom 17. Mai 2016

Datum: 30. Mai 2016

Stellungnahme des BSI

Kritische Infrastrukturen sind für das moderne Leben, das Funktionieren unserer modernen Gesellschaft, notwendig. Bei ihrem Ausfall käme es zu nachhaltigen Versorgungsengpässen oder erheblichen Störungen der Öffentlichen Sicherheit. Ihrem Schutz kommt daher im Rahmen der Daseinsvorsorge von staatlicher Seite eine besondere Bedeutung zu.

Der Trend der zunehmenden Durchdringung mit IT sowie deren zunehmende Vernetzung trifft auch auf Kritische Infrastrukturen zu. IT ist für einen stetig wachsenden Teil der sogenannten kritischen Dienstleistungen, die von Kritischen Infrastrukturen erbracht werden (z. B. Stromversorgung, Wasserversorgung, medizinische Versorgung, Versorgung mit Lebensmitteln, …), essentiell. Ein Ausfall oder eine Beeinträchtigung dieser IT kann oft auch zu einem Ausfall oder einer Beeinträchtigung der jeweiligen kritischen Dienstleistung führen. Die Aufrechterhaltung eines hohen IT-Sicherheitsniveaus ist daher für Kritische Infrastrukturen von zentraler Bedeutung.

Schon seit mehreren Jahren besteht mit dem UP KRITIS eine öffentlich-private Kooperation, die sich intensiv dem Schutz Kritischer Infrastrukturen widmet. Die IT-Sicherheit in Krankenhäusern ist beispielsweise Hauptthema im Branchenarbeitskreis Gesundheitsversorgung, der sich regelmäßig zu präventiven Maßnahmen und IT-Sicherheitsvorfällen sowie deren Bewältigung austauscht.

Ergänzend zu den kooperativen Arbeiten im UP KRITIS wurde das IT-Sicherheitsgesetz erarbeitet, das am 25. Juli 2015 in Kraft trat und die wichtigsten Betreiber Kritischer Infrastrukturen zur Wahrung eines hohen IT-Sicherheitsniveaus nach dem Stand der Technik und zur Meldung von relevanten IT-Sicherheitsvorfällen verpflichtet.

Welche Unternehmen aus dem Bereich der Kritischen Infrastrukturen als besonders wichtig und damit als Betreiber Kritischer Infrastrukturen im Sinne des IT-Sicherheitsgesetzes angesehen werden, wird durch eine Rechtsverordnung des Bundesministerium des Innern in zwei Körben geregelt. Der erste Korb dieser Rechtsverordnung, der die Sektoren Energie, Wasser, Informationstechnik und Telekommunikation sowie Ernährung beinhaltet, ist am 3. Mai 2016 in Kraft getreten. Der zweite Korb, der die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr beinhaltet, soll Ende 2016 veröffentlicht werden.

Die zur Realisierung und Aufrechterhaltung eines hohen IT-Sicherheitsniveaus nach Stand der Technik notwendigen Maßnahmen lassen sich in technische, infrastrukturelle, organisatorische und personelle Maßnahmen unterteilen. Zu den wichtigen personellen Maßnahmen eines umfassenden IT-Sicherheitskonzepts gehört dabei auch die entsprechende Ausbildung und Schulung der Administratoren und Anwender der IT.

Das IT-Sicherheitsgesetz lädt die Branchen Kritischer Infrastrukturen dazu ein, den Stand der Technik in einem sog. Branchenspezifischen Sicherheitsstandard zu formulieren und diesen vom BSI anerkennen zu lassen. Das BSI verbindet mit diesem Vorgehen die Erwartung, dass nicht nur gesetzlich verpflichtete Betreiber die dann dokumentierten Maßnahmen umsetzen, sondern dass der Standard Ausstrahlwirkung auch auf viele weitere Krankenhäuser entfaltet. Die Erarbeitung der zuvor genannten Standards erfolgt typischerweise in den Branchenarbeitskreisen des UP KRITIS.

Die Umsetzung dieser aus Sicht des BSI wichtigen und notwendigen Maßnahmen zum Schutz Kritischer Infrastrukturen sind dabei für die Betreiber Kritischer Infrastrukturen mit Kosten verbunden. Die Höhe dieser Kosten hängt maßgeblich vom bisher bereits erreichten Stand der IT-Sicherheit ab.

Mit freundlichen Grüßen

Im Auftrag

Dr. Dirk Häger