Es gilt das gesprochene Wort!

Hinweis: Diese Rede kann hier als Video abgerufen werden:

http://www.landtag.ltsh.de/aktuelles/mediathek

Kiel, 24. Januar 2019

TOP 25: Mündlicher Bericht zur Cybersicherheit (Drs. 19/1163)

Stefan Weber

„Ich danke Minister Albrecht für seinen Bericht, auch über seine Einschätzung das nicht nur die Quantität, sondern auch die Qualität von Häckerangriffen zunimmt.

Nach dem Bundeslagebericht 2017 des Bundeskriminalamtes zum Cybercrime deuten polizeiliche Ermittlungsergebnisse daraufhin, dass sich Täter im Bereich Cybercrime zunehmend professionalisieren, indem sie sehr flexibel auf aktuelle technische Rahmenbedingungen reagieren.

Cybercrime-Täter begehen heute nicht mehr ausschließlich Straftaten im digitalen Raum, sondern bieten auch die zur Begehung von Straftaten erforderliche Schadsoftware oder komplette technische Infrastrukturen in der im Internet bestehenden kriminellen Schattenwirtschaft an. Mit zunehmender Digitalisierung erhöht sich die Anfälligkeit digitaler Infrastrukturen bei Cyberattacken. Angreifern stehen immer leistungsfähigere Methoden zur Verfügung. Vereinfachte Prozesse ermöglichen Kriminellen, Angriffe auf digitale Systeme effektiv zu gestalten. Gut zu hören, dass unsere Verwaltung durch den länderübergreifenden Anbieter Dataport abgesichert ist. Aber wie sieht es mit anderen sensiblen Einrichtungen aus? Missbräuchliche Eingriffe z.B. in die Energieinfrastrukturen sind eine Bedrohung. Besonders gefährlich wird dies in Bereichen, deren Ausfall nachhaltige Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit zur Folge haben.

Herausgeber
SPD-Landtagsfraktion
Landeshaus
Postfach 7121, 24171 Kiel
Verantwortlich: Heimo Zwischenberger
Telefon Pressestelle 0431-988-13 05
Fax Pressestelle 0431-988-13 08
E-Mail pressestelle@spd.ltsh.de
Web spd.ltsh.de

Cyberangriffe gehen nicht immer direkt in das Stromnetz. Cyberangriffe benutzen häufig Umwege. Hacker greifen dann nicht unbedingt direkt Kraftwerke oder Stromnetze an, sondern schleichen sich über die Bürokommunikation ein – und arbeiten sich Schritt für Schritt zur kritischen Infrastruktur vor. Wie gut die Energiebranche geschützt ist, ist oft von Unternehmen zu Unternehmen unterschiedlich. Bei kleinen Stadtwerken ist der Schutz oft verbesserungswürdig. Da kann es vorkommen, dass sich der IT-Beauftragte häufig nur nebenbei um das Thema kümmert. Ja, da haben Sie Recht Herr Albrecht, hier aber auch in vielen Bereichen brauchen wir Spezialisten und sehr gut ausgebildetes Personal. Aber die Bedrohungen sind keineswegs nur theoretisch. Bereits 2015 gelang es einer Hackergruppe, das Stromnetz in Teilen der Ukraine lahmzulegen. Dabei nutzten die Angreifer Phishing-Emails mit fingierten Excel- und Word-Dokumenten, die an Mitarbeiter bei Netzbetreibern gerichtet waren. Beim Öffnen der Dateien installierte sich eine Malware, die wichtige IT-Systeme zur Netzsteuerung unter ihre Kontrolle brachte.

Mit dem Aufbau intelligenter Stromnetze wird die Gefahr von Hackerangriffen weiter steigen, denn immer mehr Einheiten sind in Smart Grids mit dem Internet verbunden. Damit wächst die Zahl möglicher Angriffspunkte. Smart-Grids, das sind intelligente Stromnetze, die Erzeugung, Speicherung und Verbrauch kombinieren können. Das bedeutet, dass in einem Smart-Grid nicht nur Energie, sondern auch Daten transportiert werden, sodass Netzbetreiber in kurzen Abständen Informationen zur Energieproduktion und -verbrauch erhalten.

Im September 2018 warnte der Präsident des Bundesamtes für Sicherheit in der Informationstechnik vor Hackerattacken auf die deutsche Energiebranche. Energieversorger registrieren täglich Attacken. Es wird bewusst versucht, die Systeme zu infiltrieren, um später vielleicht wirklich Kraftwerke oder Netze lahmzulegen. Bislang ist es Hackern noch nicht gelungen, Kraftwerke oder Stromnetze in Deutschland ernsthaft zu attackieren. Richtig ist, daher die Kompetenzen auszuweiten, für bessere Aufklärung zu sorgen und hochqualifiziertes Personal vorzuhalten, daran werden wir Sie und die Landesregierung messen. Hier müssen Taten folgen. Auch in der Gesundheitsversorgung gibt es Risiken im digitalen Bereich. Hier kann die Digitalisierung zwar zu einer qualitativ hochwertigen und finanzierbaren Gesundheitsversorgung beitragen, aber sie schafft mit zunehmender Technologisierung immer mehr Angriffspunkte. Gleiches gilt auch für Privatwirtschaft und in der Zivilgesellschaft.

Meine Damen und Herren. Wir brauchen nicht nur verbesserte Geräte mit eingebautem Datenschutz, wir brauchen in unseren Unternehmen der öffentlichen Daseinsvorsorge, sowie den Behörden des Landes, ein professionelles Sicherheitsmanagement, das gegen die täglichen Herausforderungen von Cyberangriffen gewappnet ist. Dies ist eine Aufgabe, der sich die

Beteiligten jeden Tag neu stellen müssen und nicht nur dann, wenn Personen des öffentlichen Lebens oder der Politik betroffen sind, sondern auch damit alle Bürgerinnen und Bürger Informations- und Datensicherheit genießen können.“