Fachforum 5

Kritische Infrastrukturen – Wie sichern wir unsere Versorgungsnetze?

„Kritische Infrastrukturen – wie sichern wir unsere Versorgungsnetze?“ Dieses Thema stand vor dem Hintergrund der zunehmenden Digitalisierung unserer Schlüsselinfrastrukturen, die gleichwohl große Chancen als auch ein großes Potential an kaum vorhersehbaren Risiken mit sich bringen, im Fokus der Diskussion des Fachforums 5 der diesjährigen „Denkfabrik Sachsen“.

Cyber-Sicherheit ist ein politischer Schwerpunkt im Freistaat Sachsen.

In Sachsen sei, so der Sächsische Innenminister **Markus Ulbig**, dass Bewusstsein für die Chancen und Risiken der „neuen Welt“ der Digitalisierung und der auch damit verbundenen Cyberkriminalität angekommen. Demografische Veränderungen und die Energiewende seien die Herausforderungen der Zukunft, bei denen die Digitalisierung auch weiterhin zunehmen werde.
Das Sächsische Innenministerium befasse sich im Rahmen entsprechender Arbeitskreise sowohl mit der damit verbundenen Kriminalitätsbekämpfung als auch mit der kontinuierlichen Sensibilisierung der kommunalen Ebene.
Zu diesem Zeitpunkt könne er festhalten, dass die Erkenntnis in ihm gereift sei, dass die öffentliche Hand dem nicht allein entgegen treten könne, sondern eine gezielte Gestaltung nur gemeinsam mit der Privatwirtschaft erreicht werden könne.

Die ganze Gesellschaft muss für das Thema sensibilisiert werden.

Die Leiterin der Research Group „IT-Security“ an der Rheinisch-Westfälischen Technischen Hochschule Aachen, **Prof. Dr. Ulrike Meyer**, beschäftigt sich, zusammen mit ihrem Team, mit den technischen Herausforderungen und Möglichkeiten der Digitalisierung und veranschaulichte ihre Forschung anhand von simulierten Hackerangriffen. Sie wies darauf hin, dass die mit der Digitalisierung einhergehenden Gefahren, bspw. in Form von Hackerangriffen, ein Problem der gesamten Gesellschaft, also der Politik, der Wirtschaft, aber auch der privaten Haushalte sei.

Der Gesetzgeber hat die Funktion eines Moderators und Kontrolleurs.

Dr. Markus Dürigvom Referat „IT-Sicherheit“ des Bundesministeriums des Innern (BMI) unterschied zwischen organisatorischen Maßnahmen einerseits und der politischen Handlungsebene andererseits.
So organisiere sich die Bundesrepublik im Cyber-Abwehrzentrum des Bundesamtes für Sicherheit in der Informationstechnik, dem auch Verbindungsbeamte der Nachrichtendienste, der Polizei sowie des Katastrophen- und des Bevölkerungsschutzes angehören, um so Informationen, sowohl national aber auch international, zusammenzubringen und daraus Empfehlungen ableiten zu können.
Die politische Handlungsebene setze sich unter der Leitung der Staatssekretärin im Bundesministerium des Innern, **Cornelia Rogall-Grothe**, aus sechs weiteren Staatssekretären der

entsprechenden Ressorts zusammen und diskutiere Gefahren und Lösungen.
Dabei werden auch Gespräche mit den acht Sektoren, die in Deutschland den kritischen Infrastrukturen angehören, geführt und über Maßnahmen zu den jeweils unterschiedlich entwickelten Sicherheitsniveaus der IT beraten.
Grundsätzlich wolle man noch in dieser Wahlperiode ein Gesetz zur IT-Sicherheit auf den Weg bringen, auf Grundlage dessen die Wirtschaft selbst branchenspezifische Standards entwickelt, die dann vom BMI anerkannt werden.
Zudem sollen alle Betroffenen etwaige Vorfälle melden, sodass es möglich wäre, ein einheitliches Lagebild zu generieren, mit dem alle Beteiligten die Themen entsprechend den Anforderungen weiterentwickeln könnten.
Der Staat, so Dürig weiter, wolle keine „Überwachungsbürokratie“, sondern konstruktive Bedingungen schaffen.

Mindeststandards bei der IT-Sicherheit sind wichtig – müssen aber auch angenommen werden.

Thomas Tschersich, Senior Vice President bei der Group „IT Security“ der Deutschen Telekom AG, bestätigte die Wichtigkeit eines Gesetzes zu Mindeststandards. Er gab aber zu bedenken, dass es wichtig sei, dass alle Marktteilnehmer mitmachen müssten, damit Probleme gelöst werden. So müssten sich die Unternehmen davon befreien, dass überwinden der internen Sicherheit als Tabu zu stigmatisieren. Nur durch die Analyse solcher Vorfälle könne man auch Lösungen finden.
Darüber hinaus müssten Unternehmen ihre Technologien vorher zu Ende denken, sich frühzeitig mit möglichen Problemen auseinander setzen und das Produkt nicht erst am Markt „reifen“ lassen.
Steffen Heyde, Principal Portfolio Manager im Geschäftsbereich „Business Security“ bei der secunet Security Networks AG, ergänzte, dass das, was dann über Mindeststandards hinaus gehe, auch als Chance im internationalen Wettbewerb genutzt werden und der Standort Deutschland so sein Know-how in Sachen IT-Sicherheit exportieren könne.

Das Problem „IT-Sicherheit“ ist allgegenwärtig – keiner kann behaupten, er hat es in Griff.

Kein Unternehmen lasse sich gern in die Karten schauen, bestätigte **Dr. Lothar Mackert**, Vice President des „Public Sector“ bei IBM. So könne man nur das bekämpfen, von dem man wisse und was man verstehe. Damit verbunden ist also eine Zusammenarbeit aller Beteiligten, eine Bündelung aller Kräfte sozusagen.
Für Einzelne sei es nicht in den Griff zu bekommen. Um pro aktiv zu sein, müsse man gemeinsam analysieren, investieren und die jeweiligen, speziellen Kenntnisse zusammen bringen, dann könnten wir auch reagieren bzw. idealerweise schon präventiv agieren.

IT-Sicherheit betrifft alle gesellschaftlichen Akteure und alle müssen ihren Beitrag leisten.

Das klare Fazit des Abends lautete: Alle Akteure haben noch viel für die IT-Sicherheit zu leisten.

Der Staat muss alle Beteiligten an einen Tisch bringen, da dieser die Gesellschaft vertritt und das Problem der sicheren (Versorgungs-)Netze auch im Interesse der gesamten Gesellschaft wahrzunehmen hat.
Zudem müsse er die nötige Infrastruktur für eine effektive Strafverfolgung im Bereich der Cyber-Kriminalität gewährleisten bzw. diese weiter ausbauen.

Die Technologieanbieter sollten sich die Nachfrage nach marktreifen Produkten zu Nutzen machen, Mindeststandards mitentwickeln und diese Technologien dann auch international anbieten.

Die Unternehmen sollten ihre Anforderungen an IT-Sicherheit überprüfen und bei möglichen Investitionen in ihre Schwerpunktbereiche die Kosten-Nutzen-Kallkulation vom potentiellen Schaden aus betrachten.

Auch die privaten Nutzer sollten sich (weiterhin) für die Fragen und Probleme der IT-Sicherheit sensibilisieren.

Audiomitschnitt der Diskussion

Quelle:
https://denkfabrik.cdu-sachsen.de/inhalte/1023185/kritische-infrastrukturen-wie-sichern-wir-unsere-versorgungsnetze-/index.html
Druckdatum:
18.09.2018 10:20